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

студентки *Мороз Лілії Василівни*

академічної групи *281м-21з-2 ІДУ*

спеціальності *281 Публічне управління та адміністрування*

на тему: *«Державна політика запобігання інформаційним загрозам в Україні»*

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

Рецензент:				

Нормоконтролер:	Вишневська О.В.			

Дніпро
2022

РЕФЕРАТ

Пояснювальна записка: 89 с., 2 рис., 1 табл., 63 використаних джерела.

ІНФОРМАЦІЙНА БЕЗПЕКА, ІНФОРМАЦІЙНІ ЗАГРОЗИ, НАЦІОНАЛЬНА БЕЗПЕКА, ІНФОРМАЦІЙНЕ СЕРЕДОВИЩЕ, ІНФОРМАЦІЙНА ПОЛІТИКА ДЕРЖАВИ, ДЕРЖАВНЕ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ СФЕРОЮ.

Об’єктом дослідження є суспільні відносини у сфері забезпечення інформаційної безпеки держави.

Предметом дослідження є державна політика запобігання інформаційним загрозам в Україні.

Мета магістерської роботи полягає у розробленні та обґрунтуванні засад державної політики запобігання інформаційним загрозам в Україні як складової національної безпеки України.

У першому розділі проаналізовано базові поняття інформаційної безпеки, проаналізовано стан дослідження інформаційної безпеки та інформаційних загроз у науці державного управління.

Другий розділ присвячено аналізу проблемних напрямів правового забезпечення інформаційної безпеки та державної політики запобігання інформаційним загрозам.

Третій розділ присвячено напрямам удосконалення державної політики інформбезпеки в умовах сучасних викликів і загроз.

Практичне значення кваліфікаційної роботи полягає у прогнозуванні і своєчасному виявленні загроз інформаційній безпеці, причин і факторів, що сприяють нанесенню шкоди національній безпеці; порушення нормального функціонування й розвитку інформаційних ресурсів.

Рекомендації та пропозиції, надані в роботі, можуть застосовуватись органами публічної влади для мінімізації впливу інформаційних ризиків та протидії деструктивному інформаційному впливу.

.

ABSTRACT

Explanatory: 89 p., 2 figures, 1 table, 63 used sources.

STATE ADMINISTRATION, INFORMATION SECURITY, NATIONAL SECURITY, INFORMATION ENVIRONMENT, STATE INFORMATION POLICY, STATE MANAGEMENT OF THE INFORMATION SPHERE.

The object of the study is public relations in the field of ensuring the information security of the state.

The subject of the study is the state policy of preventing informational threats in Ukraine.

The purpose of the master's thesis is to develop and substantiate the principles of the state policy of preventing information threats in Ukraine as a component of Ukraine's national security.

The first chapter analyzes the basic concepts of information security, analyzes the state of research on information security and information threats in the science of public administration.

The second chapter is devoted to the analysis of problematic areas of legal provision of information security and state policy for the prevention of information threats.

The third section is devoted to directions for improving the state policy of cyber security in the conditions of modern challenges and threats.

The practical significance of the qualification work consists in forecasting and timely detection of threats to information security, causes and factors contributing to damage to national security; violation of the normal functioning and development of information resources.

Recommendations and suggestions provided in the work can be used by public authorities to minimize the impact of information risks and counter destructive informational influence.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ЄС – Європейський Союз

ЗМІ – засоби масової інформації

ЗС України – Збройні Сили України

ІБ – інформаційна безпека;

ІКТ – інформаційно-комунікаційні технології;

ІЗ – інформаційна зброя;

ІПВ – інформаційно-психологічний вплив

ІТ – інформаційні технології

ІТС – інформаційно технологічні системи

КМУ – Кабінет Міністрів України

КУпАП – Кодекс України про адміністративні правопорушення

МВС України – Міністерство внутрішніх справ України

Міноборони – Міністерство оборони України

НАТО – Організація Північноатлантичного договору

НПУ – Національна поліція України

ОБСЄ – Організація з безпеки і співробітництва в Європі

ООН – Організація Об’єднаних націй

РЄ – Рада Європи

РНБОУ – Рада Національної безпеки України

СБУ Служба безпеки України

ст. – стаття

ВСТУП

Актуальність теми роботи обумовлена тим фактом, що однією зі складових суспільного розвитку України є стабільність і збалансованість у системі державного управління інформаційною безпекою в епоху турбулентності. Ефективність функціонування політичної системи держави у вирішенні складних соціально-політичних проблем сучасності безпосередньо пов'язане з роботою громадських об'єднань та окремих громадян. Найбільш яскраво ця залежність проявляється в умовах необхідності протидій загрозам національній безпеці. На даний час державна політика протидії інформаційним загрозам відіграє особливу роль в системі суспільного управління.

Інформаційна революція, що триває вже декілька десятиліть, викликала такі потужні цивілізаційні зрушення у всіх сферах суспільного буття, які важко порівняти з будь-якою іншою епохою. Інформація стала не просто засобом чи зручним способом дії, вона перетворилася для сучасної людини і суспільства на життєвий простір, що містить не тільки нові можливості, але й значні небезпеки. Вплив інформаційної технології і електронних обмінів справляє такий перетворюючий ефект, який не могла викликати навіть промислова революція. Інтернет став таким засобом комунікації, без якого вже не можуть обходитись працівники будь-якої сфери суспільної життєдіяльності.

Водночас у новій віртуальній реальності закладено безліч загроз – для індивіда, громади, держави, міжнародних організацій. Інформаційної агресії зазнають важливі основи сучасного суспільного життя – демократія і подальша демократизація, стабільні політичні системи і системи, що модернізуються, локальні культури та нові глобалізовані формати співробітництва та миру. Усе це потребує мобілізації теоретичних зусиль, які мають передувати практиці, визначати детермінанти, ресурси, технології та напрями реалізації цього непростого завдання.

Деструктивні та дестабілізуючі інформаційні впливи найперше загрожують вразливим елементам політичної системи. Водночас нерідко

цілеспрямовані та регулярні інформаційні атаки самі по собі формують сприятливе для поглинання середовище, коли дієві суб'єкти перетворюються у дезорієнтованих та безпорадних об'єктів політики.

Особливо актуальною проблематика інститутів інформаційної безпеки є для нашої країни, суспільство якої та кожен окремий громадянин всі роки незалежності знаходяться під агресивним впливом різних суб'єктів інформаційного простору, як внутрішнього, так і зовнішнього. Для України питання інформаційної безпеки особливо актуалізувалося у зв'язку із гібридною війною, яку розв'язала Росія в останні роки.

Розвиток новітніх інформаційних технологій обумовлює збільшення технологічного розриву між вимогами, які постійно ускладнюються до показників захищеності інформаційних ресурсів у суб'єктів державного управління і можливостей інформаційних технологій та програмно-апаратних засобів, що використовуються при забезпеченні протидії інформаційним загрозам. Зростає потреба в науково обґрунтованих методах і технологічних рішеннях для поновлення і вдосконалення системи забезпечення інформаційної безпеки не тільки держави, а й суспільства й особистості зокрема. Саме тому на сучасному етапі розвитку України, в умовах збройної агресії проти України надзвичайно актуальним є вирішення проблеми державного управління у сфері інформаційної безпеки.

Істотною причиною цього, із одного боку, є недосконалі механізми державного управління цією сферою, а з іншого – це зумовлюється недостатністю науково обґрунтованих методів і технологічних рішень для поновлення і вдосконалення системи забезпечення інформаційної безпеки України. Існуюча недосконалість діючої системи протидії інформаційним загрозам призводить до колосальних збитків для держави, суспільства й особистості. Таким чином, актуальності набирає потреба в перезавантаженні діючої системи інформаційної безпеки відповідно до сучасного суспільного запиту. Нагальними виступають удосконалення та структуризація нормативно-правового, технічного, інформаційно-організаційного, медико-психологічного й

превентивно-просвітницького функціоналу.

Безпосередньо питання державного управління у сфері інформаційної безпеки досліджували О. Власенко, В. Гурковський, Л. Євдоченко і З. Коваль. Окремі аспекти обраної проблематики з позицій державного управління розглядали В. Абрамов, Р. Войтович, В. Горбулін, Н. Грицяк, Карлова, В. Мандрагеля, Ю. Нестеряк, К. Павлюк, І. Пантелейчук, О. Пухкал, А. Савков, Г. Ситник, В. Смолянюк, І. Сурай, О. Твердохліб, С. Телешун. Нагальною проблемою, що потребує комплексного та системного вирішення виступає забезпечення протидії інформаційним загрозам щодо особистості, суспільства та держави, оскільки значно зросла роль накопичення, обробки й поширення інформації, збільшилася кількість суб'єктів інформаційних відносин і споживачів інформації.

Мета магістерської роботи полягає у розробленні та обґрунтуванні засад державної політики запобігання інформаційним загрозам в Україні як складової національної безпеки України. На реалізацію мети спрямовані такі завдання роботи:

- дослідити засади державного управління інформаційною безпекою в умовах зовнішнього впливу;

- дослідити сучасний стан нормативно-правового регулювання інформаційної безпеки;

- обґрунтувати комплексний підхід до визначення стратегії розвитку державної політики запобігання інформаційним загрозам в Україні в умовах глобалізації;

- розробити можливі варіанти вирішення проблем реалізації напрямів державної політики запобігання інформаційним загрозам в Україні;

- дослідити необхідність запровадження нової сучасної концепції розвитку державного управління у сфері забезпечення інформаційної безпеки;

- систематизувати принципи державного управління у сфері забезпечення інформаційної безпеки громадян;

- обґрунтувати засади державного управління у сфері інформаційної

безпеки при реагуванні виклики і загрози національній безпеці.

Об’єктом дослідження є суспільні відносини у сфері забезпечення інформаційної безпеки держави.

Предметом дослідження є державна політика запобігання інформаційним загрозам в Україні.

Методологічною основою дослідження є інституційний метод – представлений комплексом загальних, загальнонаукових та спеціальних методів наукового пізнання, який дозволив провести аналіз діяльності органів державної влади, що складають систему забезпечення інформаційної безпеки держави; порівняльно- ретроспективний аналіз й абстрагування – для встановлення змісту та етапності розвитку державного управління та державної політики протидії загрозам у сфері інформаційної безпеки.

Новизна одержаних результатів роботи полягає в комплексному науковому дослідженні засад формування державної політики протидії загрозам інформаційної безпеки. Основними напрямами формування такої політики визначено: удосконалення нормативно-правової бази щодо забезпечення інформаційної безпеки; концентрацію діяльності органів державної влади й ресурсів держави на пріоритетних завданнях розвитку інформаційного суспільства та забезпечення інформаційної безпеки; підвищення рівня координації діяльності органів державної влади щодо виявлення, оцінки та прогнозування загроз інформаційної безпеки, запобігання таким загрозам та забезпечення ліквідації їх наслідків, здійснення ефективного міжнародного співробітництва з цих питань; цілеспрямоване впровадження позитивних результатів і урахування недоліків зарубіжного досвіду щодо організації та проведення інформаційних операцій, форм, методів, засобів запобігання кібератакам.

Основні теоретичні положення, висновки та рекомендації роботи мають практичне спрямування та можуть бути застосовані для вдосконалення практики реалізації державної політики запобігання інформаційним загрозам в Україні.

РОЗДІЛ 1
ЗАСАДИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В СУЧАСНИХ УМОВАХ ДЕРЖАВОТВОРЕННЯ

1.1. Поняття «інформаційна безпека» в системі національної безпеки

У сучасному світі все більше зростає роль інформаційної сфери життя суспільства, що розглядається як сукупність інформації, інформаційної інфраструктури, суб'єктів інформаційних правовідносин та системи регулювання суспільних відносин, що виникають при цьому. Зі свого боку, інформаційна сфера має дуже істотний вплив на стан політичної, економічної, оборонної та інших складових безпеки держави. Тобто, національна безпека залежить від забезпечення інформаційної безпеки, і з подальшим розвитком у сфері інформаційних технологій ця взаємозалежність буде тільки зростати та набувати більшого значення для держави та суспільства в цілому. Так, у ст.17 Конституції України зазначено, що інформаційна безпека є найважливішою функцією держави, справою Українського народу [1]. Із розвитком інформаційних технологій і інформаційного суспільства, в умовах глобалізації виникло ціле коло невирішених питань і проблем, істотно змінилась характеристика викликів і загроз цивілізації. Головні цінності, для захисту яких держави прагнуть сформувати ефективні механізми протидії викликам і загрозам, – світ, безпека, права людини і стійкий розвиток держави [2].

У своїх працях науковці розглядають їх шляхом комплексного підходу відносно світового та вітчизняного досвіду її забезпечення. Б. Кормич, визначає інформаційну безпеку як стан захищеності параметрів інформаційних процесів, відносин і норм, які встановлені законодавством. Це забезпечує необхідні умови існування суспільства, держави, людини як суб'єктів таких процесів та відносин [3]. В. Лопатін стверджує, що інформаційна безпека – це стан захищеності життєво важливих інтересів держави, суспільства та особи на

збалансованій основі, тобто національних інтересів країни, від внутрішніх і зовнішніх загроз в інформаційній сфері [4].

О. Баранов визнає інформаційну безпеку як стан захищеності національних інтересів країни в інформаційному середовищі. За таких умов зводиться до мінімуму чи не допускається взагалі заподіяння шкоди державі, суспільству чи особі через несанкціоноване поширення інформації, її недостовірність, несвоєчасність, через негативні наслідки функціонування інформаційних технологій чи негативний інформаційний вплив [15]. Як показує аналіз наукової літератури, інформаційна безпека є складовою частиною національної безпеки держави, а процес забезпечення інформаційної безпеки необхідно розуміти як одне з глобальних і пріоритетних завдань органів державного управління, вирішенню якого мають бути підпорядковані політична, економічна, воєнна, культурна та інші види діяльності системи державного управління.

Згідно із Законом України «Про Концепцію Національної програми інформатизації», інформаційна безпека є невід'ємною складовою оборонної, економічної, політичної, а також інших складових національної безпеки [4], вона є станом захищеності життєво важливих інтересів особи, суспільства й держави від внутрішніх і зовнішніх загроз. Отже, національна безпека залежна від змісту національно-державних інтересів та характеризує положення країни, при якому їй не загрожує небезпека війни або інших посягань на суверенний розвиток.

Національна безпека України – це захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів України від реальних та потенційних загроз [5]. Основними компонентами національної безпеки є військова, економічна, соціальна, екологічна, інформаційна безпека (рис. 1.1). Сама по собі національна безпека представляє геополітичний аспект безпеки взагалі, увесь комплекс питань фізичного виживання держави, захисту і збереження його

суверенітету й територіальної цілісності, що охоплює. На сьогодні проблема інформаційної безпеки є дуже важливою, оскільки значно зросла роль накопичення, обробки й поширення інформації, зокрема, в ухваленні стратегічних рішень, збільшилася кількість суб'єктів інформаційних відносин і споживачів інформації. Інформація грає все більшу роль у процесі життєдіяльності людини. Загалом, модель державної політики протидії загрозам інформаційної безпеки в Україні варто показати таким чином (рис. 1.1).

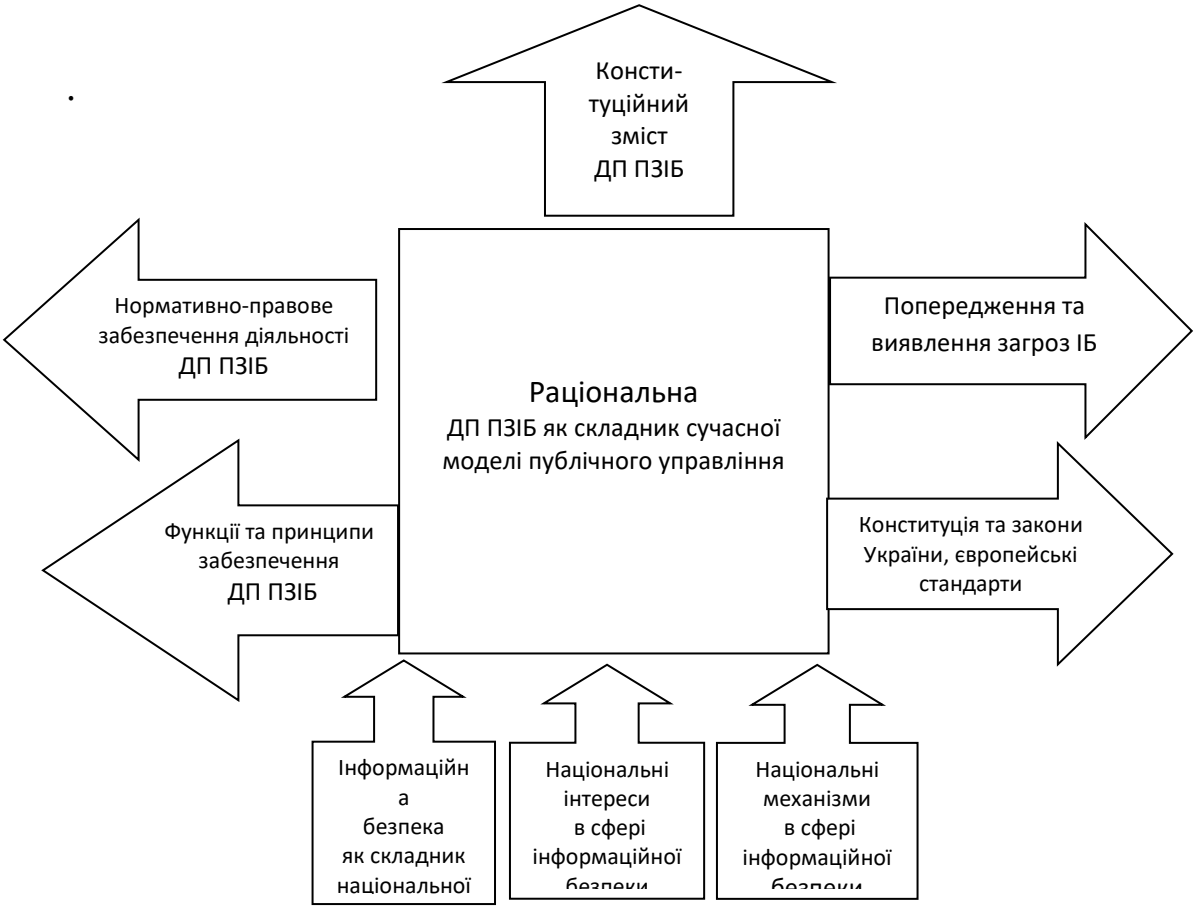

Рис. 1.1. Забезпечення функціонування раціональної моделі державної політики запобігання інформаційним загрозам

На рис. ДП ПЗІБ – державна політика протидії загрозам інформаційної безпеки

Питання протидії гібридним загрозам в інформаційній сфері, зокрема, у кіберпросторі, достатньо широко та комплексно охоплює проблеми національної безпеки. Зазначене, перш за все, потребує суттєвого аналізу ситуації, дослідження тих факторів, що спричинюють неспроможність ефективного реагування на протидію гібридним загрозам, зокрема щодо прав та свобод громадян та інтересів суспільства і держави. Поряд з цим, об'єктивність та обґрунтованість результатів дослідження потребує відповідної методологічної бази, прийнятності даних, що використовуються в аналізі, та джерел, з яких вони надходять

Глобалізація суспільних відносин та прискорення технологічного прогресу визначають чітке усвідомлення того, що сучасне інформаційне суспільство охоплює всі сфери життєдіяльності людини і держави, а кіберсфера стала важливим економічним, політичним і соціальним ресурсом [6, с. 28]. Технологічний розвиток інформаційних відносин сформував нові можливості соціального прогресу, проте паралельно також створив нові можливості для зловживаннь, а з розвитком Інтернет технологій виникла надзвичайно специфічна група загроз системі національної безпеки.

Зростання залежності людини, суспільства та національних інфраструктур (енергетичної, транспортної, телекомунікаційної) від належної роботи інформаційно-телекомунікаційних систем зумовлює їх уразливість від кіберзагроз, що, у свою чергу, підвищує ризик виникнення надзвичайних ситуацій, створює реальні загрози життєдіяльності людини, суспільства, держави, подальшому соціально-економічному розвитку та національній безпеці України.

Стратегія забезпечення кібербезпеки України визначає, що побудова інформаційного суспільства в різних країнах світу, глобалізація інформаційних процесів, суттєве зростання ролі інформаційної інфраструктури в різних сферах суспільного життя з одного боку створюють підґрунтя для ефективного соціально-економічного розвитку держав, задоволення конституційного права особи на інформацію, побудови ефективної системи державного управління. З

іншого, – сучасні інформаційні технології, перетворюють інформаційні системи урядового, оборонного, виробничого, кредитно-банківського, комунального та інших секторів на надзвичайно вразливі для реалізації інформзагроз об’єкти.

Проте, всього кілька злочинців можуть суттєво вплинути на безпеку тисячі користувачів. Технологічні можливості формують низку якостей, що спрощують, забезпечують анонімність та доступність для людей, але, у той же час, приваблюють злочинців для вчинення протиправних дій. Наслідком зростаючого використання інформаційних технологій є одночасне зростання та поширення інформзагроз, зокрема, і у форму кіберзлочинів.

У сучасному світі прогрес неможливий без цифрового інфраструктурного базису – ключового компоненту економічного розвитку. Реальною є сучасна залежність людини та суспільства, у цілому, від кіберпростору, що охоплює прилади, обладнання, програмне забезпечення, комп’ютерну техніку, телефонію, які є невід’ємною складовою сучасної повсякденної життєдіяльності. Це телекомунікаційні мережі урядової, виробничої та соціальної сфер, секретні військові та розвідувальні мережі, відкритий Інтернет, локальні мережі окремих суб’єктів інші масові мережі, які пов’язали людей, громади, підприємства та суспільства. Саме реальність кіберпростору і робить реальними ризики, які виникли разом із ним [7, с. 61].

Потрібно зазначити, що США, як одна з найбільш інформаційно розвинених країн, одна з перших зіткнулися з проблемою забезпечення недоторканості приватного життя та економічної безпеки держави й громадян. За даними дослідження, тільки за два роки кіберзлочинність вартувала американцям 8 млрд. доларів. За оцінками фахівців, лише упродовж року, у глобальному вимірі, кіберзлочини завдають збитків на суму до $ 1 трлн власникам інтелектуальної власності. Зрозумілим стає, що економічне зростання будь-якого суспільства в XXI сторіччі залежатиме від кібербезпеки.

Але не лише США, а й більшість країн Заходу, зіткнулися з необхідністю забезпечення інформаційної безпеки особи, суспільства та держави, зокрема, і

за допомогою адміністративно-правових засобів, що спричинено технічним прогресом у сфері телекомунікацій та інформаційних технологій, який призвів до виникнення низки абсолютно нових неврегульованих правом суспільних відносин.

З метою інституційного забезпечення, у травні 2009 року при федеральному уряді США була створена Єдина Рада з національної безпеки, однією з основних функцій якої є моніторинг реалізації політики кібербезпеки. У Білому Домі створено також новий відділ, яким керує Координатор з кібербезпеки, який підпорядковується безпосередньо Президенту. У межах своїх повноважень Координатор є відповідальним за інтеграцію і злагоджену роботу усіх складових державного управління у сфері кібербезпеки, за співпрацю офісу адміністрації Президента та за координацію дій у випадку настання надзвичайної події, або кібератаки.

Виступаючи 29 травня 2009 року, Президент Обама визначив п’ять головних напрямів діяльності, зокрема [8]:

1) розробка нової стратегії забезпечення безпеки інформаційно- телекомунікаційних мереж Америки;

2) налагодження взаємодії державних та місцевих органів влади з метою забезпечення організованої відповіді на кібератаки;

3) зміцнення співробітництва державного та приватного секторів, оскільки переважна кількість найважливіших інформаційних інфраструктур у США перебуває у власності або управляються приватним сектором;

4) запровадження національної пропагандистської кампанії з метою поширення серед населення інформованості і грамотності у сфері цифрових технологій.

На 55-й і 56-й Генеральних Асамблеях ООН були прийняті резолюції 55/63 і 56/121, що спрямовувались на боротьбу з кримінальним використанням інформаційної інфраструктури. Зазначалося, що вразливості інформаційної інфраструктури збільшують можливість кібератак, і суспільство має бути

готовим до цих технологічних викликів, а також, що це питання як стратегічної важливості, так і політичної волі, економічної та соціальної відповідальності. Запобігання цим загрозам потребує узгоджених дій між націями та міжнародними об’єднаннями, а також між державним і приватним секторами.

Україну, зазначене явище звісно ніяким чином не оминає, забезпечення національної безпеки, економічний розвиток та розширення соціальних благ повною мірою залежать від доступності, цілісності та конфіденційності інформаційних ресурсів, що забезпечуються інформаційними та телекомунікаційними технологіями, або в більш широкому розумінні – інформпростором. Водночас, зростання залежності від інформаційно-телекомунікаційних технологій робить сучасне українське суспільство більш уразливим перед можливими негативними наслідками протиправного використання інформпростору.

До головних тенденцій поширення інформзагроз відносять:

1) зростання кількості інформатак, багато з яких призводять до великих втрат;

2) зростання складності інформатак, які можуть включати кілька етапів і застосовувати спеціальні методи захисту від можливих методів протидії;

3) вплив практично на всі електронні (цифрові) пристрої, в числі яких останнім часом все більшу значимість набувають мобільні пристрої, а вони найбільшою мірою схильні до ризиків в сфері інформбезпеки;

4) усе частіші випадки нападу на інформаційну інфраструктуру великих корпорацій, найважливіших промислових об’єктів і навіть державних структур;

5) застосування найбільш розвиненими в області комп’ютерних технологій країнами засобів і методів інформнападів на інші держави.

За оцінками Інтерполу, кількість інформзлочинів зростає пропорційно кількості комп'ютерних мереж, а темпи зростання правопорушень та злочинів у інформпросторі є найшвидшими на планеті [9]. Проблема правового забезпечення інформбезпеки має безпосереднє відношення до обігу інформації, інформаційних відносин та своєчасного та повного обміну інформацією, а крім того до недопущення несанкціонованого використання і поширення інформації, порушення її цілісності та конфіденційності.

Сучасний еволюційний та прогресивний розвиток технологій дозволяє вирішувати широку низку завдань та проблем глобального світу. Поряд з цим, науково-технічний прогрес одночасно породжує й нові виклики та загрози в суспільстві, загалом, й у сфері інформбезпеки, зокрема. З-поміж іншого, серед дослідників поширено підхід інформзагрози долучати до сфери інформаційної безпеки. Однак, на нашу думку, доречним є відокремлення інформбезпеки від інформаційної, не дивлячись на цілком логічне узагальнення.

За оцінками Інтерполу, кількість інформзлочинів зростає пропорційно кількості комп'ютерних мереж, а темпи зростання правопорушень та злочинів у інформпросторі є найшвидшими на планеті [9]. Проблема правового забезпечення інформбезпеки має безпосереднє відношення до обігу інформації, інформаційних відносин та своєчасного та повного обміну інформацією, а крім того до недопущення несанкціонованого використання і поширення інформації, порушення її цілісності та конфіденційності.

Змістове наповнення поняття «інформаційна безпека» трьома складовими: задоволенням інформаційних потреб суб'єктів в інформаційному середовищі, безпекою інформації, захистом суб'єктів інформаційних відносин від негативного інформаційного впливу. *Перша* – задоволення інформаційних потреб суб'єктів в інформаційному середовищі. Очевидно, що без наявності у суб'єкта потрібної інформації неможливо забезпечення інформаційної безпеки. Інформаційні потреби різних суб'єктів не однакові, однак у жодному випадку відсутність необхідної інформації може нести негативні наслідки.

Друга – безпека інформації. Вимоги своєчасності, достовірності та

повноти інформації повинні дотримуватися протягом усього часу обертання інформації, оскільки їх порушення може призвести до сумнівних рішень або взагалі до неможливості прийняття його, як і недотримання статусу конфіденційності може знецінити інформацію. Тому інформація мусить бути захищена від впливів, порушуючих її статус.

Третя – захист суб'єктів інформаційних відносин від негативного інформаційного впливу. До прийняття неправильних рішень може призвести не тільки відсутність необхідної інформації, але й наявність шкідливої, загрозливої для суб'єкта інформації, яка найчастіше свідомо нав'язується [10].

При такому підході можна сформулювати наступне визначення: інформаційна безпека – стан інформаційного середовища, який забезпечує задоволення інформаційних потреб суб'єктів інформаційних відносин, безпеку інформації та захист суб'єктів від негативного інформаційного впливу. У даному визначенні суб'єктами інформаційних відносин можуть бути держава, суспільсво і громадяни. У контексті національної безпеки більш повним визначенням інформаційної безпеки можна вважати наступне: «інформаційна безпека – це стан захищеності життєво важливих інтересів особистості, суспільства й держави, при якому зводиться до мінімуму завдання шкоди через неповноту, невчасність та невірогідність інформації, негативний інформаційний вплив, негативні наслідки функціонування інформаційних технологій, а також через несанкціоноване поширення інформації» [11].

Спираючись на вищезазначені визначення, можна виділити три основні напрямки забезпечення інформаційної безпеки:

- захист інформаційних прав і свобод людини і громадянина;
- захист інформаційних ресурсів, у тому числі й інформації з обмеженим доступом, від неправомірного доступу;
- захист суспільства від некорисної і недоброякісної інформації.

Зі свого боку, небезпечні інформаційні дії зазвичай розділяють на два види. Перший пов'язаний зі втратою цінної інформації, що або знижує

ефективність власної діяльності, або підвищує ефективність діяльності супротивника, конкурента. Якщо об'єктом такої дії є свідомість людей, то йдеться про розголошування державних таємниць, вербування агентів, спеціальні заходи й засоби для прослуховування, використання детекторів брехні, медикаментозних, біологічних та хімічних впливів на психіку людини.

Безпеку від інформаційної дії цього виду забезпечують органи цензури, військової контррозвідки й інші суб'єкти інформаційної безпеки. Якщо ж джерелом інформації служать технічні системи, то йдеться вже про технічну розвідку, або шпигунство (прослуховування та перехоплення телефонних розмов, радіограм, сигналів інших систем комунікації), проникнення до комп'ютерних мереж, баз даних.

Другий вид інформаційної дії тісно пов'язаний зі впровадженням негативної інформації, що не лише призводить до небезпечних помилкових рішень, але і змушує шкідливо діяти, що підводить суспільство до катастрофи. Інформаційну безпеку даного виду зобов'язані забезпечувати спеціальні структури інформаційно-технічної боротьби. Вони нейтралізують акції дезінформації, ослаблюють маніпулювання громадською думкою, ліквідовують наслідки комп'ютерних атак. Розвиток і впровадження нових інформаційних технологій у різні сфери життєдіяльності суспільства, як і будь-яких інших науково-технічних досягнень, не лише забезпечують комфортність, але й іноді несуть небезпеку.

Визначимо найбільш значні *групи інформаційно-технічних небезпек. Перша* група пов'язана з швидким розвитком нового класу зброї – інформаційної, що здатна ефективно впливати і на психіку, свідомість людей, і на інформаційно-технічну інфраструктуру суспільства. У відносно мирних умовах інформаційно-психологічні технології можуть застосовуватися в якості спеціальних механізмів управління кризами і провокації жорстокості на території супротивника. *Друга* група інформаційно-технічних небезпек для особи, суспільства й держави – це новий клас соціальних злочинів, що ґрунтуються на

застосуванні сучасних інформаційних технологій (махінації з електронними грошима, комп'ютерне хуліганство та ін.). Питання забезпечення інформаційної безпеки як однієї із важливих складових національної безпеки держави особливо гостро постає в контексті появи транснаціональної трансграничної комп'ютерної злочинності й кібертероризма. *Третя* група інформаційних небезпек – використання нових інформаційних технологій у політичних цілях.

Складності у сфері державного регулювання інформаційною безпекою: на сьогодні відсутня чітко виражена організована система вироблення та реалізації єдиної державної політики у сфері забезпечення інформаційної безпеки, що займається визначенням пріоритетів розвитку єдиного інформаційного простору. Спираючись на це, необхідно визначити причини, що зумовлюють незадовільний стан у сфері забезпечення інформаційної безпеки, серед яких:

– безсистемний розвиток законодавства, що регулює інформаційну сферу;

– низький рівень правової та інформаційної культури громадян і суспільства в цілому;

– незадовільне фінансування діяльності забезпечення інформаційної безпеки;

– недостатній розвиток інформаційних і комунікаційних технологій у сфері державного управління, неготовність органів державної влади до застосування ефективних технологій управління й організації взаємодії з громадянами і господарюючими суб'єктами;

– недостатній рівень підготовки кадрів у сфері створення і використання інформаційних і комунікаційних технологій.

Державне врегулювання безпеки, а саме регламентація основних принципів і зміст діяльності щодо її забезпечення приведені в Законі України «Про національну безпеку» від 21.06.2018 року № 2469-УШ. Цим законом

визначається та розмежовуються повноваження державних органів у сферах національної безпеки й оборони, створюється основа для інтеграції політики та процедур органів державної влади, інших державних органів, функції яких стосуються національної безпеки й оборони, сил безпеки і сил оборони, визначається система командування, контролю та координації операцій сил безпеки і сил оборони, запроваджується всеосяжний підхід до планування у сферах національної безпеки й оборони, забезпечуючи в такий спосіб демократичний цивільний контроль над органами та формуваннями сектору безпеки й оборони [12].

Основні принципи забезпечення безпеки: дотримання й захист прав і свобод людини і громадянина; законність; системність і комплексність застосування публічними органами влади політичних, організаційних, соціально-економічних, інформаційних, правових та інших заходів забезпечення безпеки; пріоритет запобіжних заходів у цілях забезпечення безпеки; взаємодія органів державної влади із громадськими об’єднаннями, міжнародними організаціями і громадянами в цілях забезпечення безпеки.

Діяльність держави щодо забезпечення безпеки включає:

1) прогнозування, виявлення, аналіз і оцінку загроз безпеки;

2) визначення основних напрямків державної політики і стратегічне планування в області забезпечення безпеки;

3) правове регулювання в області забезпечення безпеки;

4) розробку й застосування комплексу оперативних і довготривалих заходів з виявлення, попередження і усунення загроз безпеки, локалізації і нейтралізації наслідків їх прояву;

5) застосування спеціальних економічних заходів у цілях забезпечення безпеки;

6) розробку, виробництво і впровадження сучасного вигляду озброєння, військової і спеціальної техніки, а також техніки подвійного й цивільного призначення в цілях забезпечення безпеки;

7) організацію наукової діяльності в області забезпечення безпеки;

8) координацію діяльності регіональних органів державної влади, органів державної влади суб'єктів України, органів місцевого самоврядування в області забезпечення безпеки;

9) фінансування витрат на забезпечення безпеки, контроль за цільовим витрачанням виділених засобів;

10) міжнародна співпраця в цілях забезпечення безпеки;

11) здійснення інших заходів в області забезпечення безпеки відповідно до законодавства України [13].

Так, у Законі України «Про національну програму інформатизації» визначається, що головною метою Національної програми інформатизації є створення необхідних умов для забезпечення громадян та суспільства своєчасною, достовірною та повною інформацією шляхом широкого використання інформаційних технологій, забезпечення інформаційної безпеки держави [14].

Таким чином, із вищезазначеного можна зробити висновок, що «безпека» розглядається як поняття, що відображає стан об'єкта в системі його зв'язків із точки зору здатності самовиживання в умовах внутрішніх та зовнішніх загроз, а також в умовах дій непередбачених та тяжко прогнозованих факторів. Національна безпека України складається із сукупності складових, які повинні забезпечувати збалансовані інтереси особи, суспільства й держави. До цих складових відносяться безпека в міжнародній економічній, військовій, внутрішньополітичній, інформаційній, соціальній, екологічній і інших сферах. При цьому одна з основних ролей у системі забезпечення національної безпеки відводиться економічній та інформаційній складовим.

1.2. Аналіз інформаційних загроз для України

Базовим документом, що визначає зміст національних інтересів України в інформаційній сфері, є Доктрина інформаційної безпеки України. Правовою

основою Доктрини є Конституція України, закони України, Стратегія національної безпеки України, затверджена Указом Президента України від 25 лютого 2017 року № 47/2017 «Про рішення Ради національної безпеки й оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України», а також міжнародні договори, згода на обов'язковість яких надана Верховною Радою України. Стратегія національної безпеки України є обов'язковим для виконання документом і основою для розробки конкретних програм за складовими державної політики національної безпеки [15].

У Доктрині інформаційної безпеки закріплені наступні актуальні загрози національним інтересам та національній безпеці України в інформаційній сфері:

- здійснення спеціальних інформаційних операцій, спрямованих на підрив обороноздатності, деморалізацію особового складу Збройних Сил України та інших військових формувань, провокування екстремістських проявів, підживлення панічних настроїв, загострення й дестабілізація суспільно-політичної та соціально-економічної ситуації, розпалювання міжетнічних і міжконфесійних конфліктів в Україні;

- проведення державою-агресором спеціальних інформаційних операцій в інших державах із метою створення негативного іміджу України у світі;

- інформаційна експансія держави-агресора та контрольованих нею структур, зокрема шляхом розширення власної інформаційної інфраструктури на території України та в інших державах;

- інформаційне домінування держави-агресора на тимчасово окупованих територіях;

- недостатня розвиненість національної інформаційної інфраструктури, що обмежує можливості України ефективно протидіяти інформаційній агресії та проактивно діяти в інформаційній сфері для реалізації національних інтересів України;

- неефективність державної інформаційної політики, недосконалість

законодавства стосовно регулювання суспільних відносин в інформаційній сфері, невизначеність стратегічного наративу, недостатній рівень медіакультури суспільства;

- поширення закликів до радикальних дій, пропаганда ізоляціоністських та автономістських концепцій співіснування регіонів в Україні [16].

Національна безпека нерозривно пов'язана з діяльністю держави. Тільки вона, спираючись на свій апарат, владні органи, діяльність яких поставлена в жорсткі рамки і підкріплюється відповідними правовими актами, може забезпечити спокій громадян, створити сприятливі умови для їхнього життя та діяльності. Ніякі інші соціальні сили не зможуть виконати цього завдання. Забезпечення власної безпеки та своїх громадян є одним із основних завдань будь-якої держави. Успішний розвиток і саме існування України як суверенної держави неможливі без забезпечення її національної інформаційної безпеки.

У світі розвитку інформатизації і глобалізації роль інформаційної безпеки особи, суспільства, держави збільшується, і її забезпечення повинно зайняти належне місце в політиці держави. Виходячи з цього, зазначимо основні завдання, що вимагають вирішення в забезпеченні інформаційної безпеки як складової національної безпеки держави:

1) необхідність нормативно-правового регулювання щодо протидії використання інформаційних технологій, які загрожують інтересам держави;

2) необхідність створення економічних передумов для розвитку національних інформаційних ресурсів та інфраструктури, впровадження новітніх технологій в інформаційну сферу;

3) необхідність удосконалення виробництва вітчизняних інформаційних технологій, що розробляються, впровадження вітчизняних розробок, підвищення ефективності наукових досліджень та якості освіти у сфері інформаційних технологій.

Інформація стала одним із чинників, що спроможний призвести до

великомасштабних аварій, військових конфліктів і дезорганізації державного управління. І чим вищий рівень інтелектуалізації й інформатизації суспільства, тим надійніша його інформаційна безпека. Тому Україні необхідно приділяти своїй національній інформаційній безпеці особливу увагу, оскільки вона є основою визначення найважливіших напрямків і принципів державної політики країни, життєво важливих інтересів особи, держави і суспільства. Традиційно загрози, що виникають в інформаційному просторі класифікують за характером спрямованості: на внутрішні, джерелом походження яких є вітчизняний інформаційний простір, або національний сегмент глобальної інформаційно-телекомунікаційної мережі, та зовнішні, поширення яких, пов'язане з характером глобальності мережі Інтернет. Поряд з тим, екстериторіальність Інтернету, значно ускладнює визначення конкретного джерела загрози, так як може ідентифікуватися за доменом в одній країні, а поширювати інформацію в іншій, не розкриваючи його, за допомогою використання пошукової системи, посилання тощо.

За таких умов, достатньо складним є завдання встановлення суб'єкта поширення шкідливої інформації. Зокрема, цей фактор є надзвичайно важливим з огляду на те, що необхідним є врахування сучасного стану інформбезпеки України, який характеризується як справжній театр бойових дій. За сучасних умов низка стратегічно важливих об'єктів економічного, інфраструктурного та оборонного секторів, зокрема, підприємства енергетичної й атомної галузі, транспортування газу та нафти, обслуговування ліній електромереж, що використовують інформаційно-телекомунікаційні системи, є потенційно об'єктами високого ризику через наслідки та їх рівень уразливості від зовнішнього вторгнення. Зазначене підтверджується проведеним працівниками Державного науково-дослідного інституту МВС України дослідженням, за яким рівень загрози атаки на об'єкти атомної енергетики оцінюється як надзвичайний, але, перш за все, не за рахунок ймовірності такої атаки, яка є середньою, а за рахунок катастрофічних наслідків, що спричинює

надзвичайна ситуація на цих об’єктах [17].

Щодо внутрішніх загроз потрібно акцентувати увагу на певній дискусійності серед дослідників. Зокрема, у дослідженні [17, с. 29-30] до внутрішніх загроз віднесено:

– технічна залежність інформаційної інфраструктури України від іноземних технологій, включаючи безпосередньо мережу Інтернет;

– низький рівень захищеності інформаційно-телекомунікаційних систем від несанкціонованого доступу (під цим мається на увазі і вразливість програмно-апаратного обладнання, і наявність людського фактора, що виражається у витоку важливої інформації про паролі та коди доступу);

– низька якість нормативно-правових актів, що розробляються та їх невідповідність нинішній ситуації в інформаційній сфері й в цілому відсутність послідовної державної політики в галузі забезпечення інформбезпеки;

– низький рівень комп’ютерної грамотності у населення та знань у сфері інформаційно-комунікаційних технологій;

– відсутність кваліфікованих фахівців, що володіють необхідними професійними якостями, відповідних організаційно-функціональних структур, здатних на підставі ввірених державою повноважень здійснювати ефективну протидію розміщенню в інформпросторі незаконної і небажаної (шкідливої) інформації;

– відсутність механізмів контролю та відповідальності учасників медіаспівтовариства мережі Інтернет, реєстраторів доменних імен, провайдерів, що функціонують в Інтернеті засобів масової інформації.

На наше глибоке переконання, враховуючи навіть загальні методологічні підходи до оцінювання ризиків поширення загроз, зазначені фактори, перш за

все, є не загрозами, а факторами внутрішнього характеру, що сприяють поширенню інформзагроз і можуть характеризуватися як спроможність системи протидіяти поширенню цих загроз, або як вразливість суспільства.

Окремої уваги заслуговує інформзагроза, яка може містити як екстериторіальні, так і внутрішні характеристики – інформзлочинність. Це явище є характерним не лише для України, а й для всього світового соціуму. У Європейській конвенції про інформзлочинність зроблено спробу нормативно закріпити і систематизувати правопорушення в інформпросторі за такими видами: фальсифікація з використанням комп'ютерних технологій; шахрайство з використанням комп'ютерних технологій; правопорушення, пов'язані з дитячою порнографією; правопорушення, пов'язані з порушенням авторських та суміжних прав.

Враховуючи те, що Конвенція про інформзлочинність достатньо узагальнено підійшла до класифікації інформзлочинності, певним чином поза її увагою залишились діяння у інформпросторі, які вочевидь заподіюють в тій чи іншій мірі значні збитки суб'єктам інформаційних відносин. До них відносять:

– інформсквотерство (придбання доменних імен з метою їх подальшого перепродажу або розміщення реклами); розсилку спаму;

– створення спеціальних наборів та інструментів для проведення хакерських атак, пошуку і використання вразливостей в інформаційних системах (при цьому більшість таких засобів не є шкідливим програмним забезпеченням);

– інформдифамація (від латинського diffamatio – паплюжити), тобто поширення за допомогою засобів масової інформації в мережі Інтернет неправдивих відомостей, що ганьблять честь, гідність, ділову репутацію, добре ім'я [18, с. 31].

Важливою обставиною, яка ускладнює проблему інформзлочинності, обмежує спектр її поширення на протиправні діяння, є використання цього

поняття лише стосовно сфери функціонування комп'ютерів і не враховування в якості інформзлочину правопорушень, вчинених з використанням, наприклад, мобільних засобів зв'язку, зокрема, щодо поширення дитячої порнографії за допомогою стільникового зв'язку і шахрайства з оплатою послуг зв'язку. Більш обґрунтованим є підхід, який поділяє думку тих вчених та фахівців, які вважають, що інформзлочини включають в себе «не тільки діяння, вчинені в глобальній мережі Інтернет, але і в інформаційно-телекомунікаційній сфері, де інформація, інформаційні ресурси, техніка можуть виступати предметом злочинних посягань, середовищем, в якому вчинено правопорушення, і засобом або знаряддям злочину» [19].

Інформзлочинність не обмежується межами злочинів, вчинених у глобальній мережі Інтернет. Вона поширюється на всі види злочинів, вчинених в інформаційно-телекомунікаційній сфері, де інформація, інформаційні ресурси, інформаційна техніка можуть бути предметом (метою) злочинних посягань, середовищем, в якому скоюються правопорушення, і засобом чи знаряддям злочину. Такий підхід є більш вдалим та більш обґрунтованим щодо сутності інформпростору, що формується за рахунок усіх можливих локальних та глобальних інформаційно-телекомунікаційних мереж, хоча мережа Інтернет серед них є переважаючою.

Загалом, за певними характеристиками та ознаками щодо сфери поширення та впливу, інформзлочини можуть характеризуватися як правопорушення економічного, політичного та дискримінаційного характеру, що проявляється у різних формах, зокрема, у формі незаконної політичної боротьби, вчинення шахрайства щодо фінансових операцій, тощо; у формі інформації, поширення якої потенційно є шкідливим так як стосується, наприклад, незаконної торгівлі зброєю, вибуховими речовинами, вибуховими пристроями, їх виготовлення, торгівлі людьми, людськими органами, наркотичними засобами, психотропними сильнодіючими речовинами, рецептами щодо їх виробництва тощо [20, с. 33].

На нашу думку, особливим видом інформзагрози у сучасних умовах є поширення інформтероризму. Президент США Обама зазначив, що «інформзагрози можуть нашкодити навіть міжнародному миру і безпеці, оскільки традиційні форми конфлікту розширюються вже і на Інтернет» [21].

Важливою особливістю сучасного тероризму є ієрархічна структурованість та сувора організаційна структура; жорстка конспірація; потужне технічне оснащення, що може конкурувати із забезпеченістю урядових підрозділів. Інформтероризм однаковою мірою загрожує інформаційним системам, розташованим практично у будь-якому місці світу. Виявити і нейтралізувати віртуального терориста дуже складно через занадто малу спроможність та складність фіксації слідів, на відміну від фізичного світу, де сліди є більш прагматичною та реальною можливістю для фіксації.

Наступне поняття – Інформтероризм – суспільно небезпечна діяльність, що здійснюється в інформпросторі (або з використанням його технічних можливостей) із терористичною метою і полягає у свідомому, цілеспрямованому залякуванні населення та органів влади або вчиненні інших посягань на життя і здоров’я людей. Інформтероризм як новий тип тероризму значно відрізняється від інших типів: діє в інформпросторі і породжує новий різновид насильства. Саме тому глобальний характер технічної бази інформтероризму та її доступність визначили особливі риси цього виду тероризму: висока ефективність інформатак, наслідки яких можуть мати глобальний характер; невизначеність джерела інформатаки у просторі; тимчасова невизначеність у часі як самої інформатаки, так і процесу її підготовки; можливість організації складних інформатак одночасно на різні об’єкти із різних напрямів; анонімність злочинця (для здійснення терористичного акту зловмиснику немає необхідності перетинати межі держав і знаходитися безпосередньо на місці злочину); зниження рівня морально-психологічного тиску на суб’єкт інформатаки, пов’язане з просторово-часовою віддаленістю від об’єкта інформатаки (усі дії для суб’єктів інформатаки

відбувається у віртуальному інформпросторі) [22].

Розмаїття прояву інформтероризму досить широке, від незаконного впливу на прийняття невиправданих рішень, поширення паніки і безладу, до проникнення в канали і системи супутникового зв'язку, навігації, управління енергетикою, транспортом, банківським сектором тощо. На відміну від звичайного терориста, який для досягнення своїх цілей використовує вибухівку або стрілецьку зброю, інформтерорист використовує для досягнення своїх цілей сучасні інформаційні технології, комп'ютерні системи і мережі, спеціальне програмне забезпечення, призначене для несанкціонованого проникнення в комп'ютерні системи й організації дистанційної атаки на інформаційні ресурси об'єкта нападу [23, с. 35].

Під загрозою злочинців є закриті інформаційні ресурси державних органів. Інформтерористи можуть отримати доступ до чутливої інформації: даних щодо розташування підземних комунікацій, місць знаходження техногенно небезпечних об'єктів, можливої їх охорони тощо. Водночас злочинці можуть дістати доступ до особистих даних багатьох користувачів мережі, починаючи від адреси, номера телефону і завершуючи індивідуальною інформацією щодо особи, включаючи її хобі та розпорядок життя.

Вирішення проблеми протидії інформтероризму ґрунтується на комплексному підході та має такі складові [24]:

– *правову* – пов'язана з розробленням нормативно-правових актів, які регламентують відносини в інформаційній сфері, і нормативно-методичних документів із питань забезпечення інформаційної безпеки;

– *організаційну* – полягає в удосконаленні організаційної структури державних і комерційних підприємств, сертифікації і стандартизації засобів захисту інформації та ліцензуванні діяльності у сфері захисту інформації;

– *психологічну* – передбачає формування морально-етичних норм у співробітників, які працюють з інформаційними

системами, що забезпечують критичну інфраструктуру держави;

– *технічну* – ґрунтується на створенні і постійному вдосконаленні системи забезпечення інформаційної безпеки на об’єктах інформатизації та попередження нападу.

Із врахуванням предмету нашого дослідження, ключовою проблемою залишається правова регламентація використання інформпростору. Правовим регулюванням держава має сприяти підвищенню відповідальності провайдерів і власників сайтів щодо розміщення недостовірної та завідомо шкідливої інформації, а також закріплювати механізм впливу на недобросовісних суб’єктів інформаційних правовідносин в інформпросторі. Крім того, необхідною умовою також є уникнення правових колізій та прогалин в законодавстві, наслідком чого є несвоєчасне і неадекватне реагування правоохоронних органів на факти заподіяння шкоди інформації, інформаційно-телекомунікаційним мережам, репутації громадян тощо [25, с. 31]. Забезпечення інформбезпеки все частіше розглядається, у якості стратегічного завдання держави, що охоплює увесь спектр правового регулювання.

Характерними особливостями гібридних війн є: агресія без офіційного оголошення війни; приховування країною-агресором своєї участі в конфлікті; широке використання нерегулярних збройних формувань (у т. ч. під прикриттям мирного населення); нехтування агресором міжнародними нормами ведення бойових дій і чинними угодами й досягненими домовленостями; взаємні заходи політичного та економічного тиску (за формального збереження зв’язків між двома країнами); широка пропаганда й контрпропаганда із застосуванням «брудних» інформаційних технологій; протистояння в інформнетичному просторі [26].

У «гібридній війні» особливого значення набувають засоби інтернет-комунікації, які можуть використовуватися терористами для пошуку спільників по всій території нашої держави, пропаганди власних поглядів та ідеологічного обґрунтування своїх дій, здобуття розвідданих та засобів вчинення

терористичного акту. Терористична діяльність із використанням сучасних інформаційно-комунікаційних технологій проявляється у порушенні штатних режимів роботи автоматизованих систем керування технологічними процесами на об’єктах критичної інфраструктури, цілеспрямованих атаках на урядові та приватні веб-сайти, розсиланні шкідливого програмного забезпечення з метою подальшого отримання віддаленого доступу до автоматизованих систем обробки даних органів влади та управління. В умовах гібридної війни бойові дії є другорядними, а на перший план виходять інформаційні операції та інші важелі впливу» [27, с. 27].

У свою чергу, інформвійна – це військові дії, що здійснюються в електронному просторі в електронному вигляді. Зброя в інформвійні – це інформація, інструменти – комп’ютери, театр військових дій – інтернет. Мережа інтернет стає потужною зброєю, яка суттєво підсилюється технологіями штучного інтелекту. Інформзброя представляє собою широкий спектр технічних і програмних інструментів, які найчастіше спрямовані саме на використання вразливих місць у систем передачі даних. Підсумовуючи думки експертів з питань «гібридної війни» можна говорити, що гібридна війна, яка ведеться через традиційні військові засоби та невійськові методи (інформаційна, економічна війна інші протиправні діяння), ведеться країною-агресором з метою дестабілізації обстановки в державі: встановлення напруженої атмосфери серед населення через пропаганду, залякування, внутрішні протиріччя; погіршення економічного стану та підриву політичної системи країни.

Однією з типових особливостей інформзлочинності є її глобальний міжнародний характер – інформатака може плануватися в одній країні, поширюватися з декількох інших, а жертвами можуть стати як громадяни, так і приватні й державні установи на різних континентах світу. Дедалі частіше об’єктами інформатак та інформзлочинів стають інформаційні ресурси фінансових установ, підприємств транспорту та енергозабезпечення, державних

органів, які гарантують безпеку, оборону, захист від надзвичайних ситуацій. Новітні технології застосовуються не лише для скоєння традиційних видів злочинів, але і для скоєння принципово нових видів злочинів, притаманних суспільству з високим рівнем інформатизації.

РОЗДІЛ 2
ІНСТРУМЕНТИ І ЗАСОБИ ПРОТИДІЇ ІНФОРМАЦІЙНИМ ЗАГРОЗАМ

2.1. Правова основа протидії інформаційним загрозам

Головною метою правового забезпечення інформаційної безпеки є протидія загрозам безпеці об’єктів національних інтересів в інформаційній сфері правовими засобами. Ця протидія передбачає ліквідацію загроз безпеці об’єктів національних інтересів в інформаційній сфері та мінімізацію шкоди від їхніх проявів, що досягається за допомогою попередження, припинення й мінімізації наслідків реалізації цих загроз.

Ліквідація загроз як мета функціонування правового механізму забезпечення інформаційної безпеки полягає у створенні таких умов взаємодії особистості, суспільства і держави із джерелами загроз, за яких ця взаємодія зі стадії дисгармонії чи конфлікту переходить у стадію гармонії. Ця мета може досягатися шляхом:

– правового впливу, спрямованого на зміну інтересів суб’єктів, які є джерелами або засобами реалізації загроз;

– ліквідація наявних засобів здійснення загроз;

– забезпечення невідворотного обмеження інтересів суб’єктів загроз у разі виявлення ознак підготовки до їх реалізації.

Зрозуміло, не завжди є можливість ліквідувати численні загрози безпеці об’єктів національних інтересів в інформаційній сфері через брак необхідних для цього соціальних, політичних, економічних та інших ресурсів. У цих випадках мета функціонування правових механізмів протидії загрозам може полягати в запобіганні та припиненні проявів цих загроз, а також мінімізації

їхніх наслідків.

Запобігання проявам загроз об’єктам національних інтересів в інформаційній сфері полягає у створенні умов, за яких імовірність прояву цих загроз істотно знижується. Це досягається тоді, коли істотно мінімізується очікуваний від реалізації загроз політичний, економічний, соціальний чи інший ефект. Зниження загроз можна досягнути:

– по-перше, застосувавши до суб’єктів, через дії котрих реалізуються загрози об’єктам національних інтересів, достатньої міри юридичної відповідальності;

– по-друге, підвищивши захищеність об’єктів загроз. Приміром, загроза знищення документів, що мають важливе значення для збереження й розвитку нації, може бути значною мірою попереджена шляхом встановлення для даних документів особливого правового режиму, котрий регламентує порядок їх зберігання та доступу до них, а також можливості застосування достатньої міри юридичної відповідальності до осіб, що порушують цей режим.

Припинення проявів загроз спрямоване на виявлення фактів прояву загроз та вжиття заходів щодо припинення негативного впливу на об’єкт національних інтересів в інформаційній сфері. Припинення проявів загрози здійснення комп’ютерних злочинів як мета правового забезпечення інформаційної безпеки полягає у створенні умов, за яких надійно й оперативно можна встановити факт початку протиправного діяння, конкретного суб’єкта, що здійснює його, а також зафіксувати ознаки об’єктивних та суб’єктивних складників злочину у необхідній для подання в судові органи формі, тобто вжити заходів для припинення протиправного діяння.

Мінімізація наслідків проявів загроз полягає у створенні правових умов для зменшення завданої об’єктам національних інтересів в інформаційній сфері шкоди, а також для ліквідації, якщо це можливо, наслідків реалізації загроз.

Цього можна досягти шляхом правого закріплення вимог до захищеності даних об’єктів, а також встановлення порядку відшкодування суб’єктами, котрі завдали шкоди, коштів, витрачених на ліквідацію наслідків проявів загроз. Так, мінімізувати наслідки реалізації загроз безпеці функціонування критично важливих об’єктів національної інформаційної інфраструктури можна досягти правовим закріпленням регламентів, що встановлюють вимоги до сертифікації технічного і програмного забезпечення цих об’єктів, організації системи управління безпекою, а також процедури контролю рівня їх реальної захищеності й відповідальності посадових осіб за дотримання регламентів і приписів контрольних органів.

Правове забезпечення інформаційної безпеки утворюється сукупністю інститутів і норм інформаційного, конституційного, цивільного, адміністративного та кримінального права, що регулюють відносини у сфері протидії загрозам безпеці об’єктів національних інтересів в інформаційній сфері. У зв’язку з цим уважаємо за доцільне розглядати правове забезпечення інформаційної безпеки самостійним комплексним напрямом правового регулювання, що здійснюється в межах реалізації державної політики в галузі забезпечення інформаційної безпеки держави.

У цьому контексті правильним убачається твердження О.Баранова, що з-поміж проблем забезпечення інформаційної безпеки особливе місце посідає правова. Недосконаліть правового регулювання різноманіття інформаційних відносин гальмує як розвиток і вдосконалення політичних, економічних, матеріальних та інших відносин в суспільстві, так і власне сам процес забезпечення інформаційної безпеки. Тому це, особливо в сучасних умовах життя нашого суспільства, зумовлює потребу невідкладного вирішення правових проблем регулювання інформаційних відносин [28, с. 34].

Основною метою правового забезпечення інформаційної безпеки є створення законодавчих засад для попередження, припинення й ліквідації загроз безпеці основних об’єктів національних інтересів в інформаційній сфері, а також мінімізації наслідків проявів цих загроз.

У цьому ракурсі доцільним убачається виокремити два пріоритетних, на нашу думку, напрями вдосконалення правового забезпечення інформаційної безпеки держави на сучасному етапі:

1) підвищення структурної впорядкованості нормативних правових актів, що закріплюють правові норми розглянутого правового забезпечення;

2) удосконалення нормативного правового забезпечення інформаційної безпеки, власне, – усунення законодавчих прогалин, що перешкоджають організації ефективної протидії загрозам національним інтересам України в інформаційній сфері.

Доцільним убачається виділити такі основні групи інформаційних відносин *(табл. 2.1).*

Групи інформаційних відносин в системі запобігання інформаційним загрозам

Таблиця 2.1

.

Група відносин	**Форма представлення інформації**	**Функція інформації**
Товарно-грошові відносини	Повідомлення	Товар, послуга або об’єкт прав інтелектуальної власності
Духовні відносини	Відомості	Засіб впливу на психічний стан суб’єктів
Відносини у сфері соціального та державного управління	Відомості та повідомлення	Засіб ідентифікації суб’єктів, регулювання їх діяльності
Відносини в галузі управління технічними й технологічними системами	Повідомлення	Засіб забезпечення узгодженого функціонування окремих складових систем
Відносини, пов’язані з повсякденним міжособистісним спілкуванням	Відомості	Засіб самовдосконалення суб’єктів, їхнього інформаційного збагачення

Інформаційні правовідносини – це регульовані правом суспільні відносини, що виникають у процесі взаємодії суб'єктів, що має на меті задоволення їхніх інтересів у володінні необхідною інформацією, в передаванні частини наявної інформації іншим суб'єктам, а також у збереженні інформації.

Аналогічні взаємодії, які здійснюються з метою реалізації інтересів, пов'язаних із володінням речами, регулюються з використанням детально розроблених правових засобів цивільного права. Однак можливості застосовувати їх для регулювання відносин, об'єктом яких є інформація, досить обмежені, оскільки, існуючи у формі повідомлень матеріального характеру, інформація позбавлена властивостей речі: її не можна зберегти без закріплення на матеріальному носії; вона не має ознак одиничності, адже копіюється в необмежених кількостях, не амортизується в процесі використання тощо.

Умовою реалізації інтересів суб'єктів суспільних відносин, об'єктом яких є інформація, є стійке й безпечне функціонування інформаційної інфраструктури суспільства. Склад цієї інфраструктури і зміст суспільних відносин, що виникають у зв'язку з її використанням, зумовлюються рівнем розвитку суспільства, його економічними можливостями, здатністю до впровадження результатів науково-технічного прогресу.

У складі сучасної інформаційної інфраструктури виділяють такі складові частини:

– *організаційно-керуюча:* органи і служби, що забезпечують

– стале функціонування технологічних та інформаційних елементів інфраструктури; засоби масової інформації; організації, які надають інформаційні послуги;

– *технологічна*: мережі та об'єкти зв'язку, телекомунікації; засоби автоматизації управління соціальними й технологічними процесами, автоматизації обробки даних, комп'ютерні мережі та системи;

– *інформаційна:* інформаційні системи, в т. ч. у вигляді бібліотечних, архівних і музейних фондів.

До факторів, що сприяли певним чином у формуванні в Україні несприятливого середовища для проведення інформатак РФ, можна віднести наступні:

– використання переважною більшістю українських державних організацій неліцензійного програмного забезпечення, що знизило їхню захищеність;

– використання неліцензійного антивірусного забезпечення або програмних продуктів російського походження;

– низький рівень безпеки внутрішніх інформаційно-комунікаційних мереж на підприємствах та в організаціях, що належать до об'єктів критичної інфраструктури.

Отже, сучасний розвиток демократичної, соціальної, правової держави, зростання громадянського суспільства відчутно залежить від використання інформаційних ресурсів повною мірою, від закріплення загальних основ та детальних механізмів державної інформаційної політики, від розбудови ефективної та адекватної часу системи національної інформаційної безпеки, від інформаційної культури окремих громадян та соціальних груп. Інформаційна безпека держави, суспільства, громадянина, людини сьогодні є чинником міжцивілізаційного зближення, конкурентоспроможних комунікацій, правової культури, національної довіри, демократизаційних зрушень. Вона має локальні, національні, регіональні, міждержавні та глобальні виміри, але у всіх них потребує фахового концептуального розуміння та стратегічного консультування.

Інформаційна безпека є феноменом, що одночасно належить до сфери правової регламентації державної інформаційної політики та сфери нормативного регулювання політики в галузі безпеки держави. Цілком виправданим видається і правове розуміння державної інформаційної політики України – на засадах правової держави, демократичного устрою, розробки та,

реалізації відповідних національних доктрин, стратегій, концепцій та програм згідно із чинним законодавством.

Тому інформаційна безпека як об'єкт правового регулювання та охорони конституційних прав і законних інтересів зазначених суб'єктів спрямована на одночасне забезпечення: конституційних прав і свобод людини, громадянина, єдності їх прав і обов'язків; і на захист духовних, морально-етичних, культурних, історичних, інтелектуальних та матеріальних цінностей суспільства, його інформаційного і природного середовища; конституційного ладу, суверенітету, територіальної цілісності держави; політичної, економічної, соціокультурної, науково-технологічної, оборонної і державної безпеки, екологічної, власне інформаційної сфер тощо складових національної безпеки. Загалом кожен із вказаних напрямків потребує і організованої системи протидії інформаційним загрозам, і напрацювання системи власного інформаційного простору, і відповідної інфраструктури, тобто широких інформаційних ресурсів, доступних для держави, суспільства, громадян.

Необхідність забезпечення інформаційної безпеки справедливо пов'язується з: 1) потребою забезпечення національної безпеки України як цілісності, що передбачає й інформаційну складову; 2) існуванням таких загроз інформаційній сфері країни, які можуть завдавати значної шкоди загальним національним інтересам; 3) врахуванням того, що за допомогою інформації можна впливати на зміну свідомості людей, їх поведінкові моделі.

Забезпечення інформаційної безпеки визначене нормами ч. 1 ст. 17 Конституції України як «найважливіша функція держави» і саме остання виступає головним суб'єктом політики інформаційної безпеки [1]. Згідно зі ст. 2 Закону України «Про національну безпеку України», правову основу в сфері національної безпеки, окрім Конституції, визначають і «закони України, міжнародні договори, згода на обов'язковість яких надана ВРУ України» [29], а також видані на виконання Конституції та законів України інші нормативно-правові акти.

Серед міжнародних договорів варто навести такі приклади, які

увиразнюють інформаційну складову навіть у складних міжнародних програмах співробітництва: Договір про безпеку і співробітництво у Європі (засновує структуру ОБСЄ, що опікується питаннями безпеки і співробітництва держав- учасників у галузі економіки, науки, технологій, довкілля, в гуманітарній сфері, а також питаннях прав людини, інформації, культури, освіти тощо); Угода про партнерство та співробітництво між Європейським співтовариством і Україною (започатковує таке партнерство, в тому числі з огляду на спільне бажання встановити культурне співробітництво, розширити доступ до інформації); Договір «Відкрите небо» (надає можливість сторонам здійснювати спостережні польоти над територіями одна одної для більшої відкритості у військовій діяльності, розширення миротворчих можливостей тощо), Додатковий протокол до Європейської конвенції про інформацію щодо іноземного законодавства (у якому сторони зобов'язуються обмінюватися інформацією щодо матеріального процесуального права та організації кримінального судочинства).

Ці та ряд інших договорів зобов'язують сучасні демократичні держави обмінюватися різноплановою інформацією, напрацьовувати дійові механізми її зберігання, спільно працювати у сфері сприяння загальній культурі споживання інформації людьми. Однак вони конкретизуються і в низці інших міжнародних документів. Наприклад, у прагненні об'єднати зусилля для боротьби з кіберзлочинністю і захисту законних інтересів у ході використання і розвитку інформаційних технологій країни-учасники підготували «Конвенцію Ради Європи про кіберзлочинність» [30].

Основні правила щодо здійснення діяльності в інформаційній сфері, тобто «створення, отримання, використання, поширення та зберігання інформації і захисту прав суб'єктів інформаційних відносин», містяться у 32 і 34, а також низці інших (10, 15, 17, 23. 28, 29, 31, 32, 40, 50, 53, 54, 55, 57) статей Конституції України. Крім того, основу галузевого законодавства складають більш ніж п'ятнадцять базових законів і значний корпус пов'язаних нормативних актів. За підрахунками фахівців, кількість тільки Законів України,

яких регулюються суспільні інформаційні відносини, досягла більш ніж 300.

Серед найважливіших з них: «Про інформацію», «Про доступ до публічної інформації», «Про захист персональних даних, «Про друковані засоби масової інформації (пресу) в Україні», «Про телебачення і радіомовлення», «Про звернення громадян», «Про державну таємницю», «Про засади запобігання і протидії корупції» та деяких інших. Крім того, ціла низка нормативних актів у тій чи іншій частині розглядають питання конкретних дій при інформаційній діяльності в зазначеній сфері, наприклад, Податковий та Митний кодекси України, розглядають питання створення, збору, використання специфічної податкової, митної інформації, процеси окремі нюанси розповсюдження інформації та забезпечення безпеки регулюють адміністративне, карне та цивільне кодифіковане законодавство тощо. Важливим правовим підґрунтям інформаційної безпеки виступають концептуальні державні документи – Концепції, Стратегії, Доктрини. Зокрема була розроблена Стратегія національної безпеки України, Доктрина інформаційної безпеки, Концепція розвитку інформаційного суспільства в Україні. В таких актах зазначаються базові пріоритети розвитку певної сфери, вони є підґрунтям для прийняття нових норм та усунення колій в існуючих.

Аналіз діючого вітчизняного законодавства, дозволяє зазначити, що в українській практиці часто складалась зворотна ситуація – спочатку розроблялись нормативні акти, які регулювали окремі дискретні сфери інформаційних та безпекових відносин (частіше, навіть, на рівні Постанов Уряду та Указів Президента, відомчих актів та інструкцій), а потім деякі з них змінювались законодавцем при актуалізації потреби у розробці та втіленні державної доктрини.

Фактично за великим рахунком лише закон України «Про інформацію» на початковому етапі існування української державності охоплював «глибокі пласти інформаційних відносин, регламентуючи їх на загальному, надгалузевому рівні» [31], та фактично регламентуючи і сферу інформаційних відносин, і сферу інформаційної безпеки. Закон був прийнятий 2 жовтня 1992 р.

й відтоді є певним орієнтиром для розуміння основ у питаннях створення, збирання, одержання, зберігання, використання, поширення, охорони та захисту інформації, тобто одним із перших важливих політико-правових рішень в організації безпечного інформаційного простору. Вітчизняні науковці високо оцінюють це тогочасне рішення, що вперше на вищому законодавчому рівні визначило ключові поняття інформації та її видів, державної інформаційної політики, режимів доступу до інформації, охорони інформації, гарантій інформаційного суверенітету України та багато інших [32, с. 65]. Зрештою Закон закріпив забезпечення інформаційної безпеки України серед головних напрямів державної інформаційної політики.

В ст. 14 Закону України «Про інформацію» безпосередньо визначені та розкриті види інформаційної діяльності, «а державна діяльність, що відповідає цим видам, згідно зі ст. 6 цього ж закону, складає основу державної інформаційної політики» [33]. За видами інформаційної діяльності у безпековому контексті виділяють: а) забезпечення одержання інформації у встановленому порядку; б) забезпечення можливостей використання інформації; в) забезпечення законного поширення інформації; г) забезпечення належного зберігання інформації; д) захист інформації [34].

Нова редакція Закону 2011 р. була покликана забезпечити оновлене правове підґрунтя для формування та реалізації державної інформаційної політики та зміцнення інформаційної безпеки. Після подій 2014 р. Закон знову зазнає часткових змін, пов’язаних передусім з уже згаданою гуманітарною складовою (питання мови інформації, історичних оцінок в ЗМІ, доступу до архівних документів тощо).

Зі здобуттям незалежності в Україні приймалися норми, що регулювали переважно питання технічного захисту інформації, структурні, організаційні відносини у сфері інформатизації, однак вже у процесі формування інформаційного суспільства, з розширенням гуманістичної візії на цю проблематику інформаційне законодавство також стало більше концентруватися на питаннях інформаційної безпеки.

2.2. Аналіз міжнародних норм та практика забезпечення інформаційної безпеки в публічному управлінні

Сьогодні основні для розуміння забезпечення міжнародної інформаційної безпеки міжнародно-правові норми закріплені у Статуті ООН, а також інших міжнародних нормативно-правових актах, що формують правовий базис для розв'язання збройних конфліктів, визначають засади міжнародного гуманітарного права, а також регулюють процес упередження та боротьби з міжнародним тероризмом.

Таким чином, серед основних правових принципів, що пов'язані з міжнародними інформаційними відносинами в частині гарантування інформаційної безпеки називають такі:

1) «принцип суверенної рівності держав у сфері використання інформаційних ресурсів, забезпечення інформаційного суверенітету держави та рівноправної участі в переговорних процесах щодо встановлення і кодифікації міжнародно-правових документів у сфері інформаційної безпеки»;

2) «принцип невтручання у внутрішні справи інших держав, неприпустимість інформаційної інтервенції з метою проведення спеціальних інформаційних кампаній, ворожої пропаганди та поширення деструктивної чи спеціально спрямованої інформації»;

3) «принцип заборони застосування сили або загрози силою, який забороняє використання інструментів інформаційного впливу проти територіальної цілісності чи політичної незалежності будь-якої держави»;

4) «принцип мирного врегулювання міжнародних спорів, який зобов’язує держави до превентивної дипломатії або переведення збройного конфлікту на переговорний рівень за допомогою інструментів інформаційного впливу»;

5) «принцип територіальної цілісності та непорушності кордонів, який стосується визначення меж національного інформаційного простору та заходів захисту від несанкціонованого втручання ззовні»;

6) «принцип дотримання фундаментальних прав і свобод людини, який визначає конституційні та спеціальні норми, а також норми міжнародних договорів щодо свободи слова та вільного обігу інформації, незалежності і плюралізму міжнародних мас-медіа, свободи вираження, заборони цензури та захисту конфіденційності інформаційних ресурсів»;

7) «принцип самовизначення народів і націй, який встановлює права національних меншин на культурну самобутність та інформаційну діяльність;

8) принцип міжнародного співробітництва, який зобов’язує держави співпрацювати задля зміцнення миру та міжнародного взаєморозуміння, розвитку глобальної інфраструктури з метою досягнення інтересів людства».

Отже, це комплекс політичних, економічних і соціокультурних принципів, важливих для міжнародного порозуміння.

Відповідна тенденція закріпилася і у резолюціях Генеральної асамблеї ООН, а саме Резолюція ГА ООН 53/576 (1998 р.) «Роль науки і техніки в контексті міжнародної безпеки, роззброєння та інших, пов'язаних з цим сфер»; Резолюція ГА ООН 54/49 (1999 р.) «Досягнення у сфері інформатизації і телекомунікації в контексті міжнародної безпеки»; Резолюція ГА ООН 55/28 (2000 р.) «Досягнення у сфері інформатизації і телекомунікацій в контексті міжнародної безпеки»; Резолюція ГА ООН 60/45 (2005 р.) «Досягнення у сфері інформатизації і телекомунікацій у контексті міжнародної безпеки» та багато інших [35, с. 11].

В резолюції 1989 р. № 44/21 Генеральна Асамблея ООН звернулась до всіх держав із закликом сприяти міжнародній співпраці «в усіх напрямах забезпечення міжнародної безпеки, підтвердила дієвість і значення Статуту ООН, необхідність дотримання основних його принципів, висловилась за співробітництво в рамках Організації та її основних структур» [36] з метою

знайти різноманітні «підходи до зміцнення принципів і систем міжнародної безпеки на основі нормативних документів ООН» [36].

У 1999 році на 54-ій сесії ГА ООН було прийнято оновлений проект резолюції (A/RES/54/49) «Досягнення у сфері інформатизації і телекомунікацій в контексті міжнародної безпеки», який вперше вказав на загрози міжнародної інформаційної безпеки відносно не тільки до цивільної, але і до військової сфер. Поряд із зазначеним, за результатами роботи сесії було опубліковано проект «Принципів, що стосуються міжнародної інформаційної безпеки» (A/55/140У). Принципи є свого роду робочим варіантом кодексу поведінки держав в інформаційному просторі, створюючи для них відповідні моральні зобов'язання, що також закладають основу для широких міжнародних переговорів під егідою ООН і інших міжнародних організацій з проблем міжнародної інформаційної безпеки (МІБ). У них міститься необхідна понятійна база з предмету МІБ, наводяться основні визначення: міжнародної

інформаційної безпеки, погроз інформаційній безпеці, інформаційної зброї, інформаційної війни, міжнародного інформаційного тероризму та злочинності.

Фактично на рівні цих резолюцій йдеться про незастосування сили, але одночасно й небезпеки нового покоління інформаційної зброї, коли вкрай необхідна якісна система міжнародного контролю за інформаційними озброєннями. Передбачалося узгодити позиції світового співтовариства щодо проблеми потенційного воєнного використання інформаційно-комунікаційних технологій, вдосконалення існуючих і нових систем озброєнь. У таких резолюціях помітно, як міжнародна спільнота шукає і нових методів для гарантій невтручання у внутрішні справи держав, що ускладнюється з розвитком власне інформаційних впливів. Тому розглядаються усі доступні можливості для створення міжнародної системи моніторингу інформаційних загроз, для забезпечення фундаментальних прав і свобод в інформаційній сфері, але й попередження випадків використання високих технологій з протиправною метою. Цей специфічний міжнародно-правовий режим інформаційної безпеки відтак мусить передбачити оновлене міжнародно-правове регулювання інформаційної безпеки. Безпосередньо на рівні ООН це також кодифікація спеціальних принципів і норм, які склалися на основі Статуту ООН, а також оновлення існуючих і укладання нових угод у сфері інформаційної безпеки.

Упорядкування і стабілізація міжнародного співробітництва держав в інформаційній сфері – складне та багатогранне питання, що потребує окремого дослідження. Сучасні технології мають транскордонний характер, відтак і злочини стосуються міжнародної безпеки та стабільності в цілому, а не лише окремих систем права. І. Забара, наприклад, констатує функціонування двох провідних напрямів міжнародно-правового регулювання використання інформаційно-комунікаційних технологій: інформаційний («змістовний») та комунікаційний («технічний»). У міжнародно-правовій проблематиці інформаційної безпеки вони розглядаються з позицій протидії використанню

ІКТ, що спрямовані на шкоду 1) основним правам і свободам людини та 2) критично важливим структурам держав.

Інформаційний напрям передбачає протидію транскордонному поширенню за допомогою інформаційно-комунікаційних технологій матеріалів, що суперечить принципам і нормам міжнародного права, розпалюють міжнаціональну, міжрасову, міжконфесійну ворожнечу, поширюють расистські, ксенофобські ідеї. Це письмові матеріали чи зображення або будь- яка демонстрація положень, які підбурюють до ненависті, дискримінації, насилля проти будь-якої особи або групи осіб. Такі дії, як слушно зауважують фахівці, можуть відбуватися і через використання інформаційної інфраструктури для пропаганди насильства, залякування, пригнічення, нав'язування певних моделей поведінки; для екстремістських та терористичних актів; повалення державного ладу тощо. Комунікаційний напрям передусім орієнтований на боротьбу зі зловмисним використанням комунікаційних систем та інформаційних ресурсів, що має негативний вплив на політичну, фінансову, соціально-економічну та інші сфери життя сучасного людства.

Відтак вчені і практики нині звертають увагу на охоронні та забезпечувальні норми як частину міжнародного інформаційного права, що розвиваю сучасну кібер-стабільність і кібер-мир (зокрема, окремі норми в Резолюціях ГА ООН «Створення глобальної культури кібербезпеки і захист найважливіших інформаційних структур» №57/239 (2002), № 58/199 (2003), № 64/211 (2009), Декларації Еріче про принципи кібер-стабільності та кібер-миру (2009), Глобальній програмі кібербезпеки Міжнародного союзу електрозв'язку (2007) тощо. Безумовно проблематика потребує більш системного підходу.

Відтак, усвідомлюючи ті зміни суспільно-політичного життя, що спричиняє сучасне цифрове середовище, високі технології у сукупності з глобалізаційними процесами, Радою Європи підготовлено Конвенцію про кіберзлочинність. Вона відкрита до підписання у листопаді 2001 року, набула чинності 1 липня 2004 року, підписана Україною у квітні 2005 року та

ратифікована у грудні 2006 року. Через цей документ міжнародна спільнота наголошує, що держави мають вжити усіх заходів, «для встановлення кримінальної відповідальності відповідно до їх внутрішнього законодавства за навмисний доступ до цілої комп'ютерної системи або її частини без права на це» (ст. 2). Зокрема йдеться про кримінальну відповідальність за правопорушення, пов'язані з незаконним доступом, нелегальним перехопленням і втручанням у комп'ютерні дані чи систему; також кіберзлочинами названо зловживання пристроями, підробку та шахрайство, пов'язані з комп'ютерами, дитяча порнографія, порушення авторських прав та деякі інші.

Відзначимо, що зрештою сьогодні співзвучна цим проблемам і нормотворчість в Україні. Вітчизняним законодавством визнано і достатньо точно визначено сутність таких небезпек як кіберзлочин (суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України); кібератака (навмисні дії, які здійснюються за допомогою засобів електронних комунікацій та спрямовані на порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки і режиму функціонування комунікаційних і технологічних систем тощо); кібершпигунство (шпигунство, що здійснюється у кіберпросторі або з його використанням); кібертероризм; кіберзагроза та багато інших пов'язаних явищ.

У міжнародній площині, не лише ООН та Рада Європи займаються питаннями правового забезпечення інформаційної безпеки. До проблематики активно долучається все більше число міжнародних організацій. Наприклад, з ініціативи так званої «Великої вісімки» (на той час G8) у 2000 р. ухвалено «Окінавську хартію глобального інформаційного суспільства». У документі передусім сформульовано прагнення солідарними зусиллями (в державному і

приватному секторах) ліквідувати міжнародний розрив в галузі інформації і знань, наблизити прогрес, «раціональний розвиток інформаційного суспільства» через політичне співробітництво. Хартія містить змістовні розділи щодо 1) використання можливостей цифрових технологій; 2) подолання електронно-цифрового розриву; 3) сприяння загальній участі у використанні сучасних технологій для досягнення взаємодоповнюючих цілей зі стійкого економічного зростання, підвищення суспільного добробуту, стимулювання соціальної злагоди, зміцнення демократії, транспарентного і відповідального управління, прав людини, розвитку культурного різноманіття, зміцнення міжнародного миру; 4) подальшому розвитку зі створення безпечного і вільного від злочинності кіберпростору.

Глави держав і урядів 56 держав-учасниць ОБСЄ на саміті 2010 р. також приділили певну увагу проблемам інформаційного суспільства. Зокрема заради розвитку вільного, демократичного, загального і неподільного євроатлантичного і євразійського співтовариства безпеки, вони вкотре задекларували актуальність низи транснаціональних загроз. Відтак серед таких проблем як – тероризм, організована злочинність, нелегальна міграція, поширення зброї масового ураження, незаконний оборот легкої і стрілецької зброї, наркотиків і торгівля людьми – на рівні виокремлено і кіберзагрози. Для протистояння їм, так само як і іншим небезпекам в військово-політичній, економіко-екологічній сферах, у галузі прав людини і основних свобод, необхідна все більша міжнародна єдність цілей і дій [37].

Водночас багато держав у розбудові власної систем інформаційної безпеки враховують не лише спільні орієнтири глобального розвитку, але також (а іноді й передусім): національні інтереси; накопичений досвід інформаційних протистоянь і захисту інформаційного суверенітету; реальні та потенційні загрози для конкретного суспільства, національної безпеки та безпеки держави; національні культурні й духовні цінності, традиції тощо. Не варто забувати й про об’єктивні фактори, які також унеможливлюють однакові підходи до

проблеми у всіх країнах світу. Такими зокрема є рівень інформаційного розвитку країни, її технологічні потужності, підготовка до інформаційних викликів широких верств, суспільства, державних службовців, комунікаційні можливості тощо. Попередні застереження, висловленні світовими лідерами галузі про цифрову нерівність тут як ніколи доречні.

Демократичні держави, і тут ми цілком погоджуємося з дослідниками, справді володіють ширшими можливостями, розвинутішими правовими механізмами реалізації національних інтересів, в тому числі й в інформаційній сфері. На думку вчених, такі країни вигідно відрізняє: 1) чітке визначення пріоритетів національних інтересів в інформаційній сфері, 2) гарантування інформаційного суверенітету держави, 3) регламентація порядку використання національних інформаційних ресурсів, 4) створення загальної системи охорони та захисту інформації з обмеженим доступом, 5) поширення духовних та культурних цінностей на населення інших країн, 6) обмеження спроб зовнішньої інформаційної та духовної експансії. [38, с. 92].

Стратегії та тактики інформаційної політики та інформаційної безпеки держав у політико-правовому полі можуть відрізнятися. Часто науковці, як приклад у цьому зв’язку, наводять сучасний досвід Великій Британії.

Продумана, деталізована система забезпечення інформаційної безпеки цієї держави реалізується через дієві механізми захисту прав та свобод громадян у інформаційній сфері, гарантії діяльності медіа, громадських організацій. Водночас пріоритет національної безпеки тут також дуже виразний, тому в національних інтересах згадані вище суб’єкти за законом мають і чітко окреслені межі діяльності. Законодавчо регулюються питання захисту інформації, збереження державної таємниці, мереж і телекомунікацій, окремий Кодекс визначає практики доступу до урядової інформації [39].

Спільний європейський простір зобов’язує країни адаптувати нормативно-правові положення до спільних вимог, які встановлені і в інформаційній сфері, а також готовність співпрацювати над розробкою

спільних, в тому числі й ширших міжнародних стратегій (документів, інституцій, механізмів), які б зміцнювали довіру, прозорість й безпечність глобального інформаційного простору, узгоджували діяльність держав у спільному кіберпросторі. Україна також орієнтується на ці високі стандарти інформаційної безпеки.

Прикладом для наслідування в окремих аспектах інформаційної політики може слугувати й досвід ФРН. Тут ще у 2011 р. прийнята Стратегія кібербезпеки, створено Центр кіберреагування, узгоджена інформаційно-безпекова політика уряду та державного секретаріату, а також інших органів влади, активно розвиваються механізми захисту інфраструктури стратегічного значення, налагоджується двостороння співпраця державного сектору з приватним у боротьбі проти кіберзлочинності. Комплексний підхід, на думку фахівців, дозволяє федеративному уряду ФРН забезпечити оперативне виявлення, реагування та локалізацію інформаційних атак, системно захищати суспільство від деструктивних кібервпливів та небезпечних інцидентів, запроваджувати кращі інформаційні технології у всіх сферах суспільного життя, зокрема й розвивати електронну демократію тощо [40].

Нерідко у контексті осмислення різних досвідів становлення політико – правових відносин в інформаційній сфері вчені з пострадянського простору наводять і приклад Франції. У цій країні велика відповідальність щодо регулювання відповідних проблем покладається на узгоджену діяльність Міністерства внутрішніх справ та Міністерства оборони, тобто є комплексна візія внутрішніх та зовнішніх інформаційних загроз, розуміння їх взаємозв’язаності. Політико правові механізми закладені в основу достатньо дієвої системи безпеки інформації та попередження комп’ютерних злочинів. Законодавчо окремо врегульовано питання про електронні комунікації, зокрема нормами забезпечується контроль за передачею інформації в радіочастотному просторі. Вчені загалом вирізняють два головні акценти у правовому забезпеченні інформаційної безпеки Франції: 1) захист національного

інформаційного простору, в тому числі й обмеження іноземної присутності в інформаційній сфері; 2) культурна дипломатія інформаційними засобами, зокрема поширення національних інтересів у франкомовних країнах Африки, Азії та Латинської Америки.

Сполучені Штати Америки спрямовують свою інформаційну політику на впорядкування інформаційних потоків у політичній, економічній та військовій галузях задля забезпечення збалансованості між державним контролем і свободою інформаційної діяльності. Сформовано законодавчу базу забезпечення інформаційної безпеки. Зокрема, йдеться про регламентацію основ такого забезпечення (закони «Про удосконалення інформаційної безпеки», «Про комп'ютерну безпеку», «Про комп'ютерне шахрайство і зловживання»); регулювання інформаційних відносин та порядок доступу до закритої інформації (закони «Про свободу інформації», «Про таємницю», «Про право на фінансову таємницю», «Про охорону особистих таємниць» «Про висвітлення діяльності уряду»). Наведені вище закони формують правову основу для прийняття підзаконних нормативно-правових актів, націлених на реалізацію єдиної державної політики у сфері інформаційної безпеки.

Важливим інститутом забезпечення спільного стратегічного бачення у цій сфері є Департамент внутрішньої безпеки США (Department of Homeland Security), що в цілому реалізує координацію діяльності державних органів, громадських і всіх приватних структур, які покликані до захисту інформаційного простору федерації та поширення цінностей інформаційної політики цієї наддержави за її межами. Особливо слід наголосити на позиції Сполучених Штатів стосовно ворожих дій в кіберсередовищі. Це – право використовувати будь-які засоби: дипломатичні, політичні, воєнні та економічні, які є адекватними і не суперечать міжнародному законодавству для захисту країни, союзників, партнерів та інтересів США.

Отже, говорячи про формування правових основ і гарантій міжнародної інформаційної безпеки, слід визнати, що наразі можна засвідчити різні позиції

провідних держав сучасності щодо розуміння потенційних загроз в інформаційних озброєннях та їх використанні проти критично важливих сфер життєдіяльності суспільства. Зважаючи на це, на 54-й сесії Генеральної Асамблеї ООН було ухвалено оновлену резолюцію 54/49 «Досягнення у сфері інформатизації і телекомунікацій в контексті міжнародної безпеки», на підставі якої концепція світової інформаційної безпеки набула визнання як глобальна проблема сучасності. Мотивацією для прийняття резолюції стало усвідомлення принципово нових потенційних загроз для міжнародного миру під впливом науково-технологічного прогресу та глобальної взаємозалежності усіх сфер життєдіяльності міжнародного співтовариства. У цій резолюції державам-членам було запропоновано висловитися щодо проблем інформаційної безпеки, дослідити технології загроз у цій сфері, у тому числі протиправне застосування інформаційних і комунікаційних систем та ресурсів, розробити загальноприйнятні принципи, спрямовані на зміцнення безпеки та посилення боротьби з інформаційним тероризмом і злочинністю [41].

Втім питання на цьому вочевидь не було вичерпаним, а в нових інформаційних реаліях ще гостріше постало перед світовою спільнотою. Уніфіковані норми щодо правового регулювання міжнародної інформаційної безпеки стають необхідністю нашого часу, що характеризується всеохоплюючою глобалізацією і потужними антиглобалізаційними рухами, зростанням гострих протистоянь між ними, в тому числі й в інформаційному просторі; порушенням територіальної цілісності і інформаційного суверенітету держав, поєднанням конвенційних і не конвенційних засобів сучасної війни; зрештою дрібними кіберзлочинами та масштабними хакерськими атаками, масованим інтелектуальним піратством тощо Тому вже 69-а сесія Генеральної Асамблеї ООН 2014 р. «вітає початок роботи» Групи урядових експертів з досягнень в сфері інформатизації і телекомунікацій в контексті міжнародної безпеки, але також закликає усі держави-члени приймати до уваги її оцінки і рекомендації; вчасно інформувати про загальну ситуацію у сфері інформаційної

безпеки, національні зусилля для її зміцнення, усіляко сприяти збереженню вільного потоку інформації, відповідально ставитися до використання інформаційно-комунікаційних технологій в конфліктах, політичних взаємодіях тощо [42].

РОЗДІЛ 3
ШЛЯХИ РАЦІОНАЛІЗАЦІЇ ДЕРЖАВНОЇ ПОЛІТИКИ ЗАПОБІГАННЯ ІНФОРМАЦІЙНИМ ЗАГРОЗАМ

3.1. Формування інституціональних характеристик державної політики запобігання інформаційним загрозам

В Україні контрольованість інформаційних обмінів відчутною *мірою залежить від успішності демократизаційних перетворень,* від встановлення та збереження таких політичних інститутів, механізмів і соціально-політичних відносин, які характерні для правової держави, від громадянської ініціативності та партнерства, від солідаристських прагнень та численних діалогічних платформ. Реалістична, дієва, адекватна викликам сучасності та потребам суспільства стратегія інформаційної безпеки у будь-якому разі повинна захищати однаково як державний суверенітет, так і права громадян. Ці змісти не можуть бути лише декларативними, вони взаємодоповнюють один одного на практиці, передбачають людські та інституційні виміри.

Тут варто знову повернутися до завдання сучасної держави захищати права і свободи своїх громадян. Вочевидь це завдання прямо чи опосередковано пов’язане і зі суверенітетом, і з державною незалежністю, і з дієвою стратегією міжнародного позиціонування. Адже сучасні загрозливі інформаційні впливи передусім спрямовані на свідомість та психічне здоров’я конкретного індивіда, при чому сучасні технології таргетування цільових аудиторій аж до конкретної людини дозволяють відносно легко та недорого маніпулювати навіть освіченими людьми. Неконтрольовані інформаційні потоки є часто причиною неконтрольованих дій людей, їх поганого самопочуття, безініціативності, репресивності, байдужості до суспільно-політичного життя. Однак через багатоаспектність цього чинника відповідні причино-наслідкові зв’язки оперативно довести досить складно.

У цьому контексті привертають увагу сучасні дослідження проблем

інформаційного насильства, тобто цілеспрямованого впливу на (під)свідомість людини, зокрема через застосування інформаційних атак, розповсюдження вигадок, неправди, напівправди, пліток, дестабілізуючої інформації. Це часто повторювані дії, тобто шокуючі інформаційні впливи, що мають багаторазовий ефект – в момент первинного споживання інформації, пізніше через її активне обговорення, численні інтерпретації, масові дискусії.. Звичайно, ці продукти сертифіковані, але небезпечний не сам продукт, а реклама. Вона створює імідж, образ, стереотип мислення. Ми купуємо не певний продукт, а шматочок «іншого життя». Реклама не є логічною, і саме ця алогічність і створює маніпулятивний ефект, що загрожує нашому психологічному здоров'ю» [43, с. 73]. Зауважимо лише, що сучасні маркетингові прийоми все активніше використовують у політичних цілях, а інформаційне насилля стало буденним інструментом політики окремих урядів та політичних сил. Контроль держави над подібними інформаційними обмінами є безумовним пріоритетом національної безпеки.

Національна стратегія інформаційної безпеки України вочевидь мусить враховувати ці зовнішні фактори, їх гнучкість та періодичне оновлення. Модернізація у цьому сенсі означає постійний моніторинг та звірення проголошених орієнтирів з реальністю, це також збереження та нарощування засобів інформаційного впливу всередині суспільства і за його межами, це ефективне регулювання інформаційної сфери з використанням кращих інструментів і останніх доведених практикою дієвих технологій. Політична модернізація інформаційної сфери мусить не лише наздоганяти визнані й зразкові світові моделі, але й паралельно випереджати загрозливі інформаційні атаки, що часто потужніші у своєму технологічному потенціалі за наявні в перехідному суспільстві ресурси політики.

В умовах зовнішньої агресії нерідко навіть продукування українського інформаційного продукту може перебувати під активним впливом закордонних чинників, що вносить стихійність у модернізаційні плани та стратегії розробки державної політики.

Можливість протистояти подібним загрозам передбачає потужні ресурсні витрати, ефективну систему менеджменту, найновіші технології. Серед країн-лідерів у цій сфері складно змагатися, водночас вибудовування національних систем інформаційної безпеки є беззаперечною цінністю демократичного транзиту. Визначаючись з пріоритетами та перспективами, навіть молодим демократіям сьогодні варто особливо вкладатися у цю галузь, що має довгострокові орієнтири.

Поряд із цим чимало дослідників наполягають, що сучасні реалії фактично зобов'язують українське суспільство максимально переорієнтуватися лише на боротьбу з деструктивними впливами, зовнішніми інформаційними загрозами, і саме у такий оборонний спосіб вибудовувати стратегію національної системи інформаційної безпеки. За умов глобальної інтеграції та жорсткої міжнародної конкуренції головною ареною зіткнень і боротьби різновекторних національних інтересів держав стає інформаційний простір [44, с. 28]. Водночас незайвим тут також буде додати, про чий саме інформаційний простір йдеться, адже найчастіше навіть великі геополітичні протистояння ведуться не на полі головних супротивників, а у просторі вразливих суспільств та нестабільних держав. Неспроможність давати адекватні інформаційні відповіді для багатьох сусідніх держав ідентифікується як знак до інформаційної експансії та поступового поглинання, навіть без очевидного застосування воєнної сили. В умовах жорсткої інформаційної конкуренції, посилення глобалізаційних тенденцій дуже важливо реалізувати власні національні інтереси, використовувати сучасні інформаційні технології, формувати власний порядок денний інформаційної політики. Чіткі стратегічні пріоритети у системі інформаційної безпеки, серед низки зовнішніх інформаційних загроз, дозволять державі не тільки втримати позиції на міжнародній арені та зберегти власну інституційну спроможність, але й ефективніше вибудовувати комунікації зі суспільством, та й загалом розширити можливості громадян до саморозвитку, професійного, культурного зростання тощо.

Сучасна цивілізація фактично визнала інформаційний ресурс головною зброєю міждержавного, міжнаціонального, міжрегіонального протистояння. Інформаційне маніпулювання та деструктивні впливи застосовуються і щодо великих соціальних спільнот, держав, народів, націй, і стосовно конкретних людей, їх цінностей, норм, установок тощо. Руйнацій, миттєвих чи сповільнених, можуть зазнавати суб'єкти і об'єкти політики різного рівня, однак часто через саме інформаційні канали, що складно відстежити у звичних для безпекової справи способи.

Серед науковців чимало критичних оцінок процесу медіа-комерціалізації, яку характеризують навіть як «несанкціонований доступ до свідомості», адже через панування принципу «рекламної паузи» на телебаченні є вплив на психіку мільйонів людей. Тому в сучасний період інформаційні ресурси та інформаційні системи відносяться до числа основних елементів об'єктів безпеки в усіх сферах життєдіяльності держав [45, с. 54]. Число споживачів медіа-інформації постійно зростає, а її виробники нерідко зловживають цим ресурсом вже як інструментом політичного впливу, боротьби за владу, зовнішньої агресії. Через ЗМІ та мережеві інформаційні засоби досяжність вразливих об'єктів та цілей фактично зводиться до мінімуму, тобто завдати шкоди інформаційній безпеці окремої особистості чи цілого суспільства стає простіше. Глобальний характер сучасного інформаційного суспільства одночасно скоротив відстань між нападником та жертвою навіть міжнародних протистоянь, не кажучи про регіональні чи локальні.

У світі глобальних інформаційних потоків інформаційні впливи можуть проникати та залишати свій слід у всіх сферах життєдіяльності суспільства. Тобто зовнішні й внутрішні загрози не тільки легко переносяться з однієї в іншу площину, але й цілком можуть своїм деструктивним впливом пронизувати усі аспекти функціонування державних інститутів, громадських структур, людських спільнот і окремого індивіда. Ця всеохопність і тотальність інформаційних впливів часто нагадує тоталітарні практики, що викликає у

політологів стійкі аналогії окремих проявів сучасного інформаційного суспільства з найжорстокішими практиками державного управління або колоніалізму в історії людства. Тож, ще задовго до фактичної анексії та проявленої інформаційної агресії проти України з боку РФ, вітчизняні політологи, зокрема О. Морозов, застерігали про існуючі загрози інформаційній безпеці та навіть вирізняли специфічні види таких загроз, зокрема: «1) загрози конституційним правам і свободам людини і громадянина у сфері духовного життя й інформаційної діяльності, індивідуальній, груповій і суспільній свідомості, духовному відродженню України; 2) загрози інформаційному забезпеченню державної політики України; 3) загрози розвиткові вітчизняної індустрії інформації, включаючи індустрію засобів інформатизації, телекомунікації і зв'язку; 4) загрози безпеці інформаційно-телекомунікаційних систем на території України, як діючих, так і тих, що створюються» [46, с. 24].

Перелічені деструктивні впливи і загрози достатньо тісно зв'язані між собою. Наприклад, порушення прав громадян, в тому числі й інформаційних, навіть виключно зовнішніми агентами, як наслідок знижує довіру до державних інституцій, покликаних гарантувати відповідні права. Взаємна недовіра лише поглиблюватиметься засобами масової інформації, для яких така тематика викликає особливий інтерес. Усе це лише посилюватиме вразливість системи до геополітичних загроз та гальмуватиме розвиток сучасних державницьких і громадянських структур, динаміку демократизаційних процесів тощо. З іншого боку, якщо інформаційних атак зазнає державний апарат, це не може також не відобразитися на конкретних можливостях громадян та на загальній атмосфері у суспільстві. Соціально-економічний прогрес країни та її культурний розвиток напряму залежить від спроможності спільними політичними зусиллями держави і громадян, медіа та технічної інфраструктури формувати безпечне інформаційне середовище, конкурентне, насичене, суспільно корисне, яке інтегроване у глобальне, але захищене від його негативних проявів. Політичні домовленості, партнерство, широкі дискусії та консенсусні рішення, взаємний

контроль та моніторингові заходи – усе це ті сучасні методики політики, що відрізняють демократичні починання у розбудові безпечного інформаційного простору.

Відрізнити ознаки та вчасно розв'язати початки інформаційно-психологічного протиборства односторонніми зусиллями досить складно. Тут українські позиції могли би посилити зарубіжні партнери, а аргументацією збагатити самі цілі глобального розвитку. Адже на умовному ідеологічно-цивілізаційному та інформаційному «фронті» велика кількість суб'єктів глобальної політики, які керуються власними стратегіями та ситуативними інтересами. Чимало з таких інтересів пов'язанні з Україною, відтак наше суспільство зазнає багатосторонніх інтенсивних впливів, в тому числі й агресивних інформаційно-психологічних, яким можливо протиставити лише масштабніші, технологічно потужніші та спільні дії. Ця політика мала би приваблювати не лише своїм консолідуючим характером, але й ціннісним потенціалом, коли хоча й вразливі, але все ж правові й демократичні за своєю сутністю інститути та відносини знаходять потужну підтримку міжнародної спільноти у боротьбі з інформаційними нападами агресорів.

На шляху вибудовування такого не тільки декларативного, але й дієвого, ефективного, адекватного часу міжнародного партнерства, державі ще й варто розробляти чіткі механізми ідентифікації різних форм інформаційно-психологічного та інформаційно-технологічного впливу. Часто труднощі при налагодженні глобальних мереж комунікації щодо питань безпеки викликає саме невміння означувати та класифікувати існуючі загрози.

Варто розглянути класифікацію деструктивних інформаційних впливів за ознаками інтенсивності й масштабності:

1) інформаційна експансія (діяльність з досягнення конкретних інтересів методом безконфліктного проникнення в інформаційну сферу);

2) інформаційна агресія (незаконні дії однієї зі сторін в інформаційній сфері, обмежене і локальне застосування сили, для завдання супротивнику відчутної шкоди в окремих областях його діяльності);

3) інформаційна війна (вищий ступінь інформаційного протиборства, інформаційне насильство над державами, народами, націями, класами, соціальними групами, спрямоване на розв'язання суспільних, політичних, ідеологічних, національних, територіальних та інших конфліктів через широкомасштабне застосування інформаційної зброї).

У межах названих вище трьох форм вчені розрізняють безліч технологій і методів інформаційної агресії/насильства/експансії, кожен з яких потребує адекватних основ інформаційного захисту, відображення у стратегії і тактиці безпеки. Нерідко один і той самий суб'єкт політики (держава чи їх співдружність, політична партія чи партійна система загалом, передвиборчий штаб чи поле виборчої кампанії в цілому, правозахисна організація чи громадянське суспільство, соціальна група, окремий індивід тощо) може зазнавати багатосторонніх і багаторівневих інформаційних агресій. Глобальність сучасного світу сприяє цьому. Стратегічне бачення Україною інформаційних загроз сьогодні залежить і від наукових, фундаментальних визначень пріоритетів у цій політиці, і від фактичних дій та практик, які застосовує держава в умовах ведення справжньої інформаційної війни, в якій постійно перебуває. Те саме стосується й інших суб'єктів політики, які окремо поза державною стратегією інформаційної безпеки ризикують втратити і власну суб'єктність у політичному житті суспільства, і навіть цілковито увесь цей простір незалежного функціонування.

Глобалізація інформаційного середовища стосується не лише держави, адже цей всеохопний процес привносить та змінює більшість суб'єктів і об'єктів сучасної політики, серед яких важливу рол відіграють засоби масової інформації.

Загалом, теоретико-правове осмислення функції сучасної держави щодо забезпечення інформбезпеки характеризується двома напрямами розвитку:

1) теоретико-правові аспекти розуміння функцій держави та особливостей їх трансформації в сучасних умовах;

2) проблематика інформаційної та безпесередньо інформбезпеки в

межах теоретико-правових, галузевих і прикладних правових, спеціально-правових та інших соціально-гуманітарних наук.

Ураховуючи складність реальних проблем щодо боротьби з інформзлочинністю на національному і міждержавному рівні однією з перших міжнародних угод з юридичних і процедурних аспектів розслідування інформзлочинів стало прийняття Радою Європи 23 листопада 2001 р. Конвенції Ради Європи про інформзлочинність (далі – Конвенція про інформзлочинність) [47]. Варто зазначити, що нормами Конвенція про інформзлочинність передбачено координацію дій на національному та міждержавному рівнях щодо припинення несанкціонованого втручання в роботу комп'ютерних систем, незаконного перехоплення даних і втручання в комп'ютерні системи. Зокрема, важливим є те, що, на сьогодні на структурі зазначеного документа ґрунтується найбільш поширена класифікація інформзлочинів, яка є «еталоном» для наявних міжнародних та регіональних нормативно-правових актів, а також наукової практики. Відповідно інформзлочини поділено на п'ять груп:

1) інформзлочини проти конфіденційності, цілісності та доступності комп'ютерних даних і систем, такі як незаконний доступ, незаконне перехоплення, втручання в дані, втручання в систему;

2) інформзлочини, пов'язані з використанням комп'ютера, як засобу скоєння злочинів – а саме, як засіб маніпуляцій з інформацією (наприклад, комп'ютерне шахрайство та комп'ютерне підроблення);

3) інформзлочини, пов'язані з контентом (змістом даних), тобто з вмістом даних, розміщених в комп'ютерних мережах (наприклад, інформзлочини, пов'язані з дитячою порнографією);

4) злочини, пов'язані з порушенням авторського права і суміжних прав, при цьому встановлення таких правопорушень віднесено документом до компетенції національних законодавств держав;

5) інформзлочини як акти расизму та ксенофобії, вчинені за допомогою комп'ютерних мереж, входять до п'ятої групи інформзлочинів зафіксовано в

окремому протоколі [48, с. 4-5].

Варто звернути увагу на те, що деякі інформзлочини нормами Конвенції про інформзлочинність не виділено в окремі групи. В наукових колах ведуться дискусії щодо даних інформзлочинів, які до цього часу викликають суперечки щодо необхідності гармонізації законодавства на міжнародному рівні з точки зору техніки їх криміналізації. Це «інформтероризм» та використання інформпростору в терористичних цілях. Державами та міжнародними організаціями вживаються зусилля щодо боротьби з терористичними організаціями, які використовують інформпростір. Як приклад, можна навести проект Clean IT, який існує на рівні Європейського Союзу та метою якого є боротьба з інформтероризмом. Але, у зв'язку з відсутність узгодженого визначення тероризму на міжнародному рівні, у даному напрямі ускладняється, хоча і не заважає, боротьба з інформтероризмом. Тому, нагальною та необхідною для всього міжнародного співтовариства є криміналізація інформтероризму як явища.

Не можна поза увагою залишити ще одну категорію інформзлочинів, а саме – крадіжка, передача і використання персональних даних з метою вчинення злочинів (identity theft), яка, хоча і не включена окремо в Конвенцію про інформзлочинність, але отримала поширення після прийняття міжнадордного документа. Деякі країни виділяють ці злочини в окрему категорію, інші вважають, що дані діяння підпадають під кілька статей кримінального законодавства, що, у свою чергу, спонукає до виділення даного злочину в окрему групу та гармонізації міжнародного законодавства у цій сфері.

Небезпека зовнішніх деструктивних інформаційних впливів відтак походить не лише від офіційних державних агентів з закордону, але й від окремих медіа- корпорацій, комерційних структур, неформалізованих об'єднань, що активно функціонують у всесвітній мережі, добре вивчили закономірності функціонування інформаційного суспільства та готові

використовувати його вразливості на власну користь. Увесь масив інформаційних потоків контролювати за допомогою державних інструментів досить складно, тому таким важливим є налагодження міжнародного співробітництва зі залученням громадського сектору, наукової та освітянської спільноти, експертного середовища, професійних спілок тощо. Боротьба з інформаційними маніпулюваннями суспільною свідомістю найефективніша, коли відбувається на різних рівнях, з розвитком багатосторонніх каналів комунікації та загалом зі встановленням довірливих відносин між партнерами.

Суб'єкт-об'єктний вимір інформаційної безпеки заслуговує окремої уваги, але у контексті глобалізації варто також акцентувати на політичних процесах, що відбуваються одночасно та не можуть власне повноцінно відбутися без один одного. В українських реаліях йдеться передусім про щонайменше такі паралельні у політичному житті суспільства процеси як 1) налагодження та розвиток міжкультурних і міжнародних комунікацій, 2) модернізація і зміцнення демократичних інститутів 3) розбудова інфраструктури інформаційного суспільства як рушійної сили прогресивних державно-політичних змін. Для ворожої інформаційної агресії кожен із цих важливих напрямків національного розвитку є потенційною ціллю для дестабілізації.

В часі інтенсивних інформаційних протистоянь, фактичних інформаційно- психологічних і мережевих воєн відповідна стратегія є необхідністю, що визначає здатність держави зберігати та утверджувати суб'єктність у глобальному світі. Тут принагідним є досвід США, який детально аналізують і вітчизняні дослідники. Зокрема утверджується необхідність дослідження, напрацювання та перманентного оновлення підходів до врегулювання інформаційно-психологічної складової діяльності держави – «інформаційне забезпечення тих чи інших дій влади». Підкреслюється, що сучасні збройні конфлікти містять дуже виразні ознаки їх інформаційного та психологічного забезпечення. Відтак таке забезпечення мусить бути

пролонговане у часі, тобто це далеко не разовий захід, а складний їх комплекс до, під час та після початку розгортання бойових дій.

У даному аспекті уявляється корисним звернення до канадської Стратегії забезпечення інформбезпеки. У Стратегії акцентується увага на тому, що рівень інформбезпеки має бути визначено в залежності від шкоди, яку може бути завдано інформатакою, а інформатаки, безпосередньо, включають ненавмисний або несанкціонований доступ, використання, маніпуляції, переривання або знищення (через електронні засоби) електронної інформації та/або електронної та фізичної інфраструктури, що використовується для обробки, зв'язку, та/або баз даних [49]. Як приклад, наведемо, виявлену програму у 2009-2010 рр. Stuxnet. Stuxnet розроблена великою і добре скоординованою групою інформзлочинців, яка була направлена на атаки та для погіршення роботи промислового обладнання ядерного об'єкта, а також програма була здатна атакувати локальні мережі, не підключені до Інтернету. Згодом було виявлено такі програми з розвідувальними функціями як DuQu, Flamer, Red Octoder та інші [50]. Як було з'ясовано, деякі з масштабних розвідувальних операцій у інформпросторі проводились протягом майже 10 років, їх цілями були США, Західна Європа (джерело атак – Китай), Близький Схід (ймовірне джерело – США), Росія, Казахстан, Білорусь, Україна (джерело атак невідоме) [51].

Крім того, існують програми або окремі функції програм, які приховано впроваджуються у комп'ютерну систему та, які протягом тривалого часу функціонують у системі, при цьому порушують політику безпеки – програмні закладки. Це ще один із видів інформзагроз, який все частіше зустрічається та упроваджується вірусом, троянським конем, черв'яком або безпосередньо користувачем-зловмисником. До особливого виду програмних закладок відносять так звані руткіти (rootkit), мета яких приховати сліди присутності зловмисника чи зловмисної програми у системі. А також програмні закладки здійснюють такі функції: перехоплення і передавання інформації (Spyware); порушення функціонування систем («логічні бомби»); утиліти віддаленого

адміністрування (люки, backdoor); несанкціонована робота з мережею (Інтернет- клікери; проксі-сервера; організація DoS і DdoS атак); психологічний тиск на користувача (реклама (Adware); злі жарти і містифікації [52, с. 44]/

Викликає зацікавленість звіт щодо комп'ютерної безпеки і проблеми інформзлочинів. Звіт складено за даними американського Інституту Комп'ютерної Безпеки (Computer Security Insitute) на підставі дослідження, яке проведено за ініціативи Міжнародної Групи з Комп'ютерних Злочинів (International Computer Crime Squads) ФБР США [52, с. 112]. У документі наведено найбільш поширені методи атак і порушень, а саме:

- метод грубої сили (brute-force) – 13,9 %. Підбір паролів, ключів і іншої ідентифікаційної або аутентифікаційної інформації;
- підміна IP-адресу (IP-spoofing) – 12,4 %. Метод атаки, при якому зловмисник змінює IP-адреси пакетів, переданих по Internet таким чином, щоб вони виглядали «внутрішніми» для мережі, де кожний вузол довіряє адресній інформації іншого;
- ініціювання відмови в обслуговуванні (denial of service) – 16,3 %. Вплив на мережу або окремі її частини з метою порушення порядку штатного функціонування;
- аналіз трафіка (sniffer) – 11,2 %. Перегляд і розшифровування переданих даних із метою збору паролів, ключів і іншої ідентифікаційної або аутентифікаційної інформації;
- сканування (scanner) – 15,9 %. Метод атаки з використанням програм, що послідовно перебирають можливі точки входу в систему (наприклад, номера TCP-портів або телефонні номера) із метою встановлення шляхів і можливостей проникнення;
- підміна, нав'язування, знищення, переупорядкування даних або заміна вмісту повідомлень, переданих по мережі (data diddling) – 15,6 % [53].

Останнім часом набувають великого значення проблеми розробки систем захисту та збереження державної, службової та комерційної таємниці.

3.2. Шляхи удосконалення державної політики запобігання інформзагрозам

Основними принципами державного регулювання у сфері запоінформ загрозам є орієнтація на державно-правовий механізм забезпечення інформаційної безпеки та реалізація національних інтересів і цілей. Ефективність механізму забезпечення інформаційної безпеки визначається передусім його здатністю сприяти збереженню єдності нації, стабільності суспільних відносин, відтворенню національно-культурних цінностей, подоланню політичних, військових, економічних, соціальних криз, створенню передумов стабільного розвитку, а також здатністю ефективно протидіяти загрозам інформаційній безпеці. Останнє, у свою чергу, викликає до життя власне механізми протидії інформаційним загрозам, які на сучасному етапі характеризуються підвищеною небезпечністю, адже інформаційне протиборство нарощує свої можливості в результаті стрімкого зростання обсягу та значення інформації в сучасному світі.

Відтак, безпека сучасної держави безпосередньо залежить від стану її інформаційного простору. Комплексний характер актуальних загроз національній безпеці в інформаційній сфері потребує визначення інноваційних підходів до формування системи захисту та розвитку інформаційного простору в умовах глобалізації та вільного обігу інформації [54].

У теорії національної безпеки механізм протидії загрозам національній безпеці зазвичай розглядають у широкому або у вузькому сенсі. У вузькому

сенсі він виступає як складова частина державного механізму і становить систему державних організацій, органів, установ, а також недержавних інституцій, спеціально створюваних для забезпечення національної безпеки або таких, що наділяються окремими функціями щодо забезпечення національної безпеки, у їхній взаємодії та практичному функціонуванні (сили забезпечення національної безпеки).

У широкому сенсі механізм протидії загрозам національній безпеці включає не лише сили, але й систему засобів, за допомогою яких здійснюється протидія відповідним загрозам з метою захисту життєво важливих інтересів суспільства й держави. Такими засобами виступають технології, а також технічні, програмні, лінгвістичні, правові, організаційні засоби, включаючи телекомунікаційні канали, що використовуються з метою збирання, формування, обробки, передачі або приймання інформації щодо стану національної безпеки та стосовно заходів, спрямованих на її зміцнення, а також власне методи, способи і прийоми, використовувані суб’єктами забезпечення національної безпеки для вирішення завдань щодо протидії загрозам національній безпеці.

Механізм забезпечення національної безпеки – це динамічна система, у межах якої можна виділити такі стадії: формулювання інтересів, захист яких забезпечуватиметься; виявлення та прогнозування внутрішніх і зовнішніх загроз життєво важливим інтересам; вироблення системи заходів щодо протидії загрозам; нейтралізація загроз; здійснення заходів щодо відновлення нормального функціонування об’єктів безпеки. Численність засобів протидії інформаційним загрозам та варіативність їх комбінацій залежно від специфіки загроз дають змогу вести мову у множині – про механізми протидії інформаційним загрозам національній безпеці.

В умовах стрімкого розвитку інформаційного суспільства, який також зумовлює вдосконалення методів ведення інформаційних воєн, звичні технології та механізми протидії зовнішнім загрозам національній безпеці застаріли, і на передній план виходять нові способи стримування розгортання

загроз та мінімізації зумовлених ними ризиків. Методи протидії інформаційним загрозам від зовнішніх джерел можна умовно поділити на дві групи:

- профілактичні, або превентивні, – які застосовуються для недопущення розгортання відповідних загроз або для запобігання подальшим ризикам на початковому етапі розгортання таких загроз;
- оперативні методи, які використовуються безпосередньо у відповідь на агресивні кроки, що виходять від зовнішніх джерел інформаційних загроз та пов'язані з їх розгортанням та реалізацією.

З-поміж заходів превентивної протидії інформаційним загрозам від зовнішніх джерел вирізняють чотири основні групи: нормативно-правові, адміністративні, інформаційні й економічні.

Оперативна протидія має здійснюватися тільки після виявлення достовірної інформації щодо структур, груп або осіб, котрі є рушійними силами, а також оцінки ступеня загрози й наявних ресурсів для її нейтралізації. Лише після ефективної роботи з інформацією можна обрати оптимальний оперативний метод протидії, який відповідає наявним ресурсам і є достатнім для нейтралізації загрози відповідного ступеня.

В умовах, у яких нині опинилася Україна через збройну агресію РФ, особливої актуальності набуває протидія поширенню шкідливої для психіки людини інформації, яку без перебільшення можна вважати інформаційною зброєю, а також розвиток відповідного законодавства. У цьому контексті інформаційно-психологічну безпеку можна визначити як стан захищеності від окремих осіб та/або певних груп, а також відповідних життєво важливих інтересів людини, суспільства й держави в інформаційній сфері.

Під негативним інформаційно-психологічним впливом ми розуміємо такий вплив на особу чи групу осіб, який здійснюється на їх психіку, зокрема й усупереч їхній волі, із застосуванням спеціальних засобів і методів, що призводить до шкідливих для людини, суспільства та держави наслідків. Усю глибину загрози подібних постійних, цілеспрямованих, продуманих і щедро фінансованих впливів з боку РФ для національної безпеки Україна повною

мірою відчула під час анексії Криму та воєнних дій на сході. Убачається, що всі питання, пов'язані із зазначеними впливами, слід передбачити в межах спеціального закону стосовно забезпечення інформаційної безпеки.

Інша проблема, яка потребує законодавчого визначення та врегулювання, – відсутність систематизації законодавства з питань протидії екстремізму в інформаційній сфері. Внаслідок цього матеріали подібного змісту часто розповсюджуються практично безперешкодно, позаяк діяльність із запобігання й припинення різних видів екстремізму здійснюється компетентними державними органами безсистемно й нерідко формально.

При цьому важливо пам'ятати, що реальна протидія екстремістським чи іншим негативним проявами в інформаційній сфері не повинна перетворюватися на зведення особистих рахунків з «незручними» журналістами, тиск на опозиційні засоби масової інформації та придушення свободи слова. Масова інформатизація всіх сфер життєдіяльності суспільства не оминула й державні інституції. Тому вельми нагальним убачається забезпечення прозорості в діяльності всіх гілок державної влади, кожного держслужбовця. Це, своєю чергою, безпосередньо впливає на дієвість інституту відповідальності для кожного із суб'єктів цієї діяльності, на стан інформаційної безпеки, а також на загальний стан державної та національної безпеки.

Попри всі декларації й певні кроки української влади підвищити рівень доступу до офіційної інформації та ступінь довіри до електронного уряду, на даний момент до світових стандартів нам ще далеко. Такий висновок можна зробити на підставі дослідження, представленого Департаментом економічного й соціального розвитку ООН (The Unted Nations Department of Economic and Social Affairs), фахівці якого вважають, що електронний уряд є інструментом підвищення ефективності керування, трансформації процесів державного керування за рахунок підвищення ступені залучення до нього широкого кола громадськості на всіх рівнях – мікро, мезо, макро. Тож наразі стає актуальним і особливо затребуваним інститут доступу до офіційної інформації. Цьому сприяють швидкий розвиток інформаційних технологій, зростання добробуту й

рівня освіченості населення.

Задля реалізації державної політики у сфері забезпечення інформаційної безпеки відповідно до наведених вище принципів, завдань і функцій має бути створена ефективна державна система. Крім уповноважених державних органів, її мають складати науково- дослідницькі, науково-технічні установи, проектні, конструкторські та інші організації, котрі провадять наукові дослідження й розробляють технічні засоби, а також освітні заклади, які займаються підготовкою, перепідготовкою та підвищенням кваліфікації відповідних кадрів. Узгоджені дії вказаних суб'єктів забезпечуються шляхом ліцензійної, сертифікаційної, експертної та контрольної діяльності уповноважених на це органів у сфері забезпечення інформаційної безпеки, формування державних замовлень на відповідні наукові дослідження, освітні та інші послуги тощо.

Комплекс засобів, що їх застосовує державна система інформаційної безпеки, має гарантувати належний її рівень, у тому числі убезпечити суспільство від шкідливих інформаційно-психологічних впливів. Не останню роль у цьому має відіграти згадуване вище ліцензування, основні аспекти якого, зокрема умови отримання ліцензії, слід, на нашу думку, передбачити в базовому законі. Так, необхідною умовою отримання ліцензії вбачається сертифікація методів і засобів, які застосовуються під час проведення діяльності, пов'язаної з інформаційною безпекою.

Що стосується шкідливих інформаційних впливів, то достеменно виявити їх можна лише шляхом спеціальної експертизи. Остання проводиться для виявлення загроз інформаційній безпеці за державними стандартами й за дорученням відповідно уповноважених державних органів. Зростання залежності сучасного суспільства від стійкого функціонування інформаційної інфраструктури робить реалізацію національних інтересів України в інформаційній сфері важливим чинником національної безпеки. Тож для України сьогодні необхідним кроком на шляху до інформаційного майбутнього є розробка цілісної гнучкої динамічної державної політики у сфері забезпечення інформаційної безпеки, яка враховуватиме багатоаспектність

цього явища, перспективні тенденції змін інформаційного простору, особливості геополітичного становища, економічного стану країни і знайде своє відображення у суспільній свідомості, а також на правовому концептуально-доктринальному рівні та в ефективному інформаційному законодавстві [55, с. 178]. Досліджуючи проблеми формування та реалізації державної політики у сфері запобігання інформаційним загрозам в Україні на сучасному етапі, передусім слід з'ясувати, що ж таке «державна політика у сфері забезпечення інформаційної безпеки», і як зміст цього формулювання співвідноситься з поняттям «інформаційна політика держави».

Адже інформаційна політика держави в сучасному політичному процесі розглядається як окремий вид політичної діяльності. Основні підходи до проблеми становлення державної інформаційної політики сформувалися ще в XIX ст. і отримали новий імпульс до розвитку в 1960-х роках у зв'язку із входженням розвинених країн у стадію інформаційного, коли ЗМІ з інструменту відображення реальності перетворилися на засіб її творення [56, с. 74].

Інформаційна політика – «це особлива сфера життєдіяльності, пов'язана з відтворенням і поширенням інформації, котра задовольняє інтереси держави й громадянського суспільства і спрямована на забезпечення конструктивного діалогу між ними та їхніми представниками» [57, с. 38].

Своєю чергою С. Бондаренко під державною інформаційною політикою розуміє цілеспрямовану діяльність центральних органів влади з формування політико-релевантного знання про державу, його поширення та управління в інформаційному просторі з метою досягнення політичних цілей і захисту національних інтересів [58, с. 113]. Інформаційну політику держави розглядають також як діяльність останньої в інформаційній сфері, спрямовану на задоволення інформаційних потреб людини і громадянина через формування відкритого інформаційного суспільства на основі розвитку єдиного інформаційного простору цілісної держави та його інтеграції у світовий інформаційний простір з урахуванням національних особливостей та інтересів

при забезпеченні інформаційної безпеки на внутрішньодержавному та міжнародному рівні.

Виходячи із цього, основною метою державної інформаційної політики України є забезпечення: захисту інформаційного суверенітету держави (особливо захист національного інформаційного простору з інформаційним ресурсом і систем формування масового суспільної свідомості) в сучасних умовах глобалізації та інтернаціоналізації процесів в інформаційній сфері; рівня інформаційної достатності для прийняття рішень державними органами, підприємствами та громадянами; реалізації конституційних прав і свобод громадян, суспільства і держави на інформацію. Головною ж метою державної політики у сфері забезпечення інформаційної безпеки при цьому є управління реальними та потенційними загрозами, спрямоване на створення необхідних умов для задоволення інформаційних потреб людини та громадянина, а також реалізації національних інтересів. Відтак, державна політика у сфері забезпечення інформаційної безпеки України – це діяльність державно-правових інституцій щодо управління реальними та потенційними загрозами й небезпеками з метою задоволення інформаційних потреб людини та громадянина, а також реалізації національних інтересів, тож державна інформаційна політика та державна політика у сфері забезпечення інформаційної безпеки співвідносяться як ціле та частина. Державна політика у сфері забезпечення інформаційної безпеки України є невід'ємною складовою державної політики національної безпеки України і становить офіційно прийняту систему поглядів та практичну діяльність органів державної влади й управління, спрямовану на забезпечення такого стану соціальних суб'єктів, за якого дія будь-якої інформаційної загрози не призводить до зниження рівня їх інформаційної безпеки нижче мінімально припустимого.

Отже, інформаційна безпека забезпечується проведенням єдиної державної політики в інформаційній сфері, системою заходів економічного, політичного й організаційного характеру, які є адекватними загрозам національній безпеці, а також можливостям держави щодо управління

відповідними ризиками. Система забезпечення інформаційної безпеки є інструментом реалізації державної політики у сфері забезпечення інформаційної безпеки. Її головне призначення полягає в досягненні мети національної безпеки в інформаційній сфері, а відтак її основною функцією є забезпечення збалансованого існування інтересів особи, суспільства й держави в інформаційній сфері.

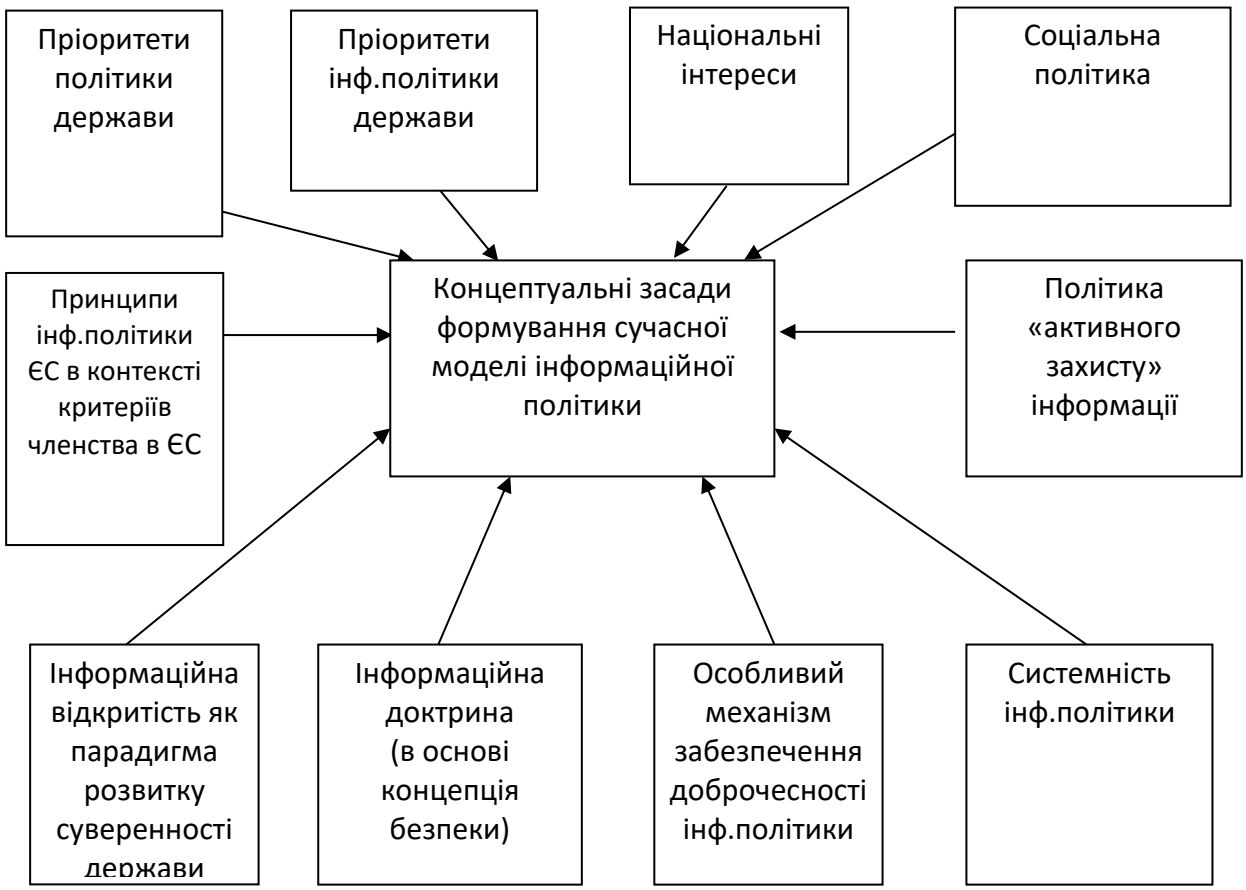

Рис.3.1. Складники державної політики запобігання інформаційним загрозам

У теперішній час у сфері державної політики в інформаційній галузі функціонують такі керівні документи:

1) Доктрина інформаційної безпеки України;
2) Концепція розвитку електронного урядування в Україні;

3) Концепція розвитку телекомунікацій в Україні

4) Концепція формування системи національних електронних інформаційних ресурсів;

5) Концепція технічного захисту інформації в Україні;

6) Концепція створення Національного громадського телебачення і радіомовлення;

7) Основні засади державної комунікативної політики;

8) Національна програма інформатизації;

9) Державна цільова науково-технічна програма «Образний комп'ютер»;

10) Програма «Українська книга».

На жаль, при забезпеченні безпеки в інформаційно-психологічній сфері розглядається здебільшого технічна сторона, а психологічна – практично залишається поза увагою. Це призводить до посилення інформаційної агресії з боку РФ, яка з метою просування своїх інтересів використовує соціально-політичну ситуацію в Україні, залучаючи до цього в тому числі й наших співвітчизників [59].

Відкритість національного інформаційного простору породжує реальну загрозу шкідливого інформаційно-психологічного впливу на суспільну свідомість населення, що становить особливу соціальну небезпеку. Безконтрольність електронних мас-медіа та соціальних мереж, які використовуються як майданчик для вербування в екстремістські організації, злочинні угруповання, незаконні збройні формування тощо, негативно впливає на користувачів мережі Інтернет, якими переважно є молодь і освічені люди з активною життєвою позицією. Слід також враховувати, що в українське суспільство сьогодні розколоте за ставленням до таких фундаментальних цінностей, як демократія, незалежність, приватна власність, ринок тощо. Є розбіжності щодо уявлень про форму державного устрою та правління, про кількість мов офіційного спілкування та навчання, напрямки децентралізації, функції та завдання місцевого самоврядування тощо. Існує ціла низка міжрегіональних, міжетнічних, міжконфесійних суперечностей, різні шкали

цінностей і пріоритетів, а тому наразі важко говорити про єдність інформаційного простору та про спільні ціннісні орієнтації , що також є джерелом різнопланових внутрішніх загроз [60].

Нині в Україні на законодавчому рівні відсутні достатні гарантії захисту населення від негативних інформаційно-психологічних впливів, результатом яких може стати руйнування єдиного інформаційного й духовного простору. У цьому зв'язку виникає необхідність формування державної системи забезпечення інформаційно-психологічної безпеки, яка має будуватися на основі щільної взаємодії всіх владних інститутів, а також громадських організацій. У ході реалізації державної політики у безпековій сфері варто, на наш погляд, звернути увагу на такі аспекти: розробку й реалізацію комплексних заходів щодо запобігання, нейтралізації й випередження негативних інформаційно-психологічних впливів на суспільство й державу; підготовку суспільства до активної інформаційної протидії; входження національного інформаційного поля у світовий інформаційний простір; удосконалення системи масової інформації й комунікації; формування системи підготовки кадрів для інформаційно-психологічної протидії; духовну консолідацію суспільства й віднаходження всіма верствами населення нової соціальної ідентичності.

За сучасних умов інформаційна безпека має визнаватися основою інформаційної складової усіх сфер забезпечення національної безпеки. До головних завдань системи забезпечення інформаційної безпеки належить: прогнозування ризиків реалізації державної внутрішньої та зовнішньої політики, міждержавних та державних програм і проектів; виявлення внутрішніх і зовнішніх потенційних і реальних загроз; розробка та впровадження адекватних заходів і засобів реагування на виклики, як історичного походження, так і сучасного цивілізаційного розвитку; нейтралізація або послаблення дії проявів гібридної війни та інших загроз національній безпеці України. Системний і комплексний підхід до вирішення

цих завдань має відповідним чином визначати спрямування державної політики у сфері забезпеченні інформаційної безпеки нашої країни.

Державна інформаційна політика на сучасному етапі має передбачати й вирішувати завдання щодо гармонійного забезпечення інформаційної безпеки особи, суспільства й держави з одночасним виокремленням нагальних пріоритетів. До останніх слід віднести створення або відновлення основних позицій захисту системи національної безпеки в інформаційній сфері, формування ефективної системи інформаційної безпеки держави, виявлення потенційних інформаційних загроз, усунення наявних із визначенням ступеня можливих наслідків та рівня їх інтенсивності. Головним підґрунтям державної інформаційної політики вбачається: забезпечення права на достовірну, повну та своєчасну інформацію, свободи слова та інформаційної діяльності в національному інформаційному просторі, недопущення втручання у зміст та внутрішню організацію інформаційних процесів, крім випадків, передбачених законодавством; збереження та вдосконалення вітчизняного національного інформаційного продукту й технологій, національно-духовних і культурних цінностей; забезпечення інформаційної та національно- культурної ідентифікації України у світовому інформаційному просторі; гарантування державної підтримки та розвитку ресурсів науково-технічної продукції та інформаційних технологій. Відповідно, державна політика у сфері забезпечення інформаційної безпеки має спрямовуватися передовсім на реалізацію комплексу системних превентивних заходів із наданням гарантій захисту життєво важливих інтересів особи, суспільства, держави та спроможності нейтралізувати чи послабити дію внутрішніх і зовнішніх потенційних і реальних загроз національній безпеці України.

Спираючись на такі міркування та з огляду на сучасний стан загроз інформаційній безпеці, доцільно, на нашу думку, виділити такі пріоритетні напрями державної політики у сфері забезпечення інформаційної безпеки:

1. **Захист життєво важливих інтересів особи, суспільства й держави від внутрішніх**

і зовнішніх загроз. Виходячи із сучасних загроз національній безпеці України, цей напрям має концентруватися передусім на протидії загрозам, пов'язаним із застосуванням інформаційних технологій у військово-політичних цілях, у тому числі для здійснення ворожих дій і актів агресії, спрямованих на підрив суверенітету, порушення територіальної цілісності нашої держави. Відтак, першочерговими вбачаються такі заходи:

1.1. удосконалення діючої системи забезпечення інформаційної безпеки Збройних сил України, військових формувань і органів, що включає в себе сили і засоби інформаційного протиборства;

1.2. розробка та впровадження дієвих механізмів прогнозування, виявлення та оцінки інформаційних загроз;

1.3. нейтралізація інформаційно-психологічного впливу, в тому числі спрямованого на підрив історичної спадщини, її спотворення чи викривлення фактів;

1.4. поширення національного інформаційного продукту на тимчасово окупованих територіях; розробка та впровадження щодо них цілісної державної інформаційної політики;

1.5. розвиток інформаційної культури молоді, а також культури особистої інформаційної безпеки, профілактика правопорушень в інформаційній сфері.

2 блок – Захист суверенітету, підтримання політичної та соціальної стабільності, територіальної цілісності України**. Невідкладними заходами цього напряму мають стати:**

2.1. протидія використанню інформаційних технологій з метою пропаганди екстремістської ідеології, поширення ксенофобії, ідей національної ворожнечі, в тому числі й на міжнародному рівні;

2.2. забезпечення захисту державної таємниці, іншої інформації обмеженого доступу, насамперед комерційної таємниці підприємств військово-промислового комплексу та інших, які мають особливе значення для економіки

держави;

2.3. нейтралізація інформаційного впливу, спрямованого на розмивання традиційних духовно-моральних цінностей українського народу;

2.4. підготовка спеціалістів з протидії інформаційним загрозам на рівні державних освітніх програм.

3 блок – захист критичної інформаційної інфраструктури**.**

3-поміж основних заходів цього напряму:

3.1. підвищення захищеності критичної інформаційної інфраструктури та стійкості її функціонування;

3.2. розвиток механізмів виявлення та попередження інформаційних загроз і ліквідації наслідків їх прояву, викликаних інформаційно-технічним впливом на об’єкти критичної інформаційної інфраструктури;

3.3. підвищення безпеки функціонування об’єктів інформаційної інфраструктури;

3.4. розробка механізмів обміну інформацією з країнами НАТО та ЄС про передові практики у сфері забезпечення безпеки функціонування елементів критичної інформаційної інфраструктури.

4 блок – забезпечення розвитку інформаційно-комунікаційних технологій**. Серед пріоритетів виокремимо такі заходи:**

4.1. розробка й виробництво конкурентоспроможних засобів забезпечення інформаційної безпеки;

4.2. інноваційний розвиток галузі інформаційних технологій, що має відбитися на розташування України в рейтингу Індексу розвитку інформаційно-комунікаційних технологій;

4.3. підтримка інноваційного та прискореного розвитку системи забезпечення інформаційної безпеки, галузі інформаційних технологій;

4.4. проведення наукових досліджень і здійснення дослідно-конструкторських розробок з метою створення перспективних інформаційних технологій забезпечення інформаційної безпеки.

*5 блок – забезпечення участі України в міжнародній системі інформаційної безпеки***. Провідними заходами цього напряму мають стати*:***

1) участь у формуванні системи міжнародної інформаційної безпеки на двосторонньому, багатосторонньому, регіональному, субрегіональному та глобальному рівнях;

2) участь у розробці міжнародних документів системи інформаційної безпеки;

3) формування механізмів міжнародного співробітництва у сфері протидії загрозам використання інформаційних та комунікаційних технологій у терористичних цілях;

4) продовження та посилення співпраці з НАТО та ЄС у сфері запобігання загрозам в інформаційній сфері на державному та глобальному рівнях;

5) участь у підготовці та прийнятті державами – членами Організації Об'єднаних Націй міжнародних правових актів, що регламентують застосування принципів і норм міжнародного права у сфері інформаційної безпеки;

6) розвиток співпраці з державами – членами НАТО та ЄС у сфері

7) протидії інформаційній злочинності; підвищення ефективності

8) інформаційного обміну між правоохоронними органами держав під час розслідування злочинів в інформаційній сфері.

З прийняттям Закону України «Про основні засади забезпечення інформбезпеки України» конкретизовано повноваження Державної служби спеціального зв'язку та захисту інформації України у сфері забезпечення інформбезпеки, зокрема:

– забезпечує формування та реалізацію державної

політики щодо захисту у інформпросторі державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, інформзахисту об’єктів критичної інформаційної інфраструктури, здійснює державний контроль у цих сферах;

– координує діяльність інших суб’єктів забезпечення інформбезпеки щодо інформзахисту;

– забезпечує створення та функціонування Національної телекомунікаційної мережі, впровадження організаційно-технічної моделі інформзахисту;

– здійснює організаційно-технічні заходи із запобігання, виявлення та реагування на інформінциденти і інформатаки та усунення їх наслідків;

– інформує про інформзагрози та відповідні методи захисту від них; забезпечує впровадження аудиту інформаційної безпеки на об’єктах критичної інфраструктури, встановлює вимоги до аудиторів інформаційної безпеки, визначає порядок їх атестації (переатестації);

– координує, організовує та проводить аудит захищеності комунікаційних і технологічних систем об’єктів критичної інфраструктури на вразливість;

– забезпечує функціонування Державного центру інформзахисту, урядової команди реагування на комп’ютерні надзвичайні події України CERT-UA.

Підтвердженням галузевого правового статусу є імплементація зазначених норм Закону України «Про основні засади забезпечення інформбезпеки України» до галузевого закону «Про Державну службу спеціального зв’язку та захисту інформації України» щодо формування та реалізація державної політики щодо захисту у інформпросторі державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена

законом, інформзахисту критичної інформаційної інфраструктури, здійснення державного контролю у цих сферах.

Законом України «Про Державну службу спеціального зв'язку та захисту інформації України» у ст. 15 визначено також права Державної служби спеціального зв'язку та захисту інформації України, окремий перелік яких характеризує саме галузевий адміністративно-правовий статус, зокрема:

– одержувати в установленому порядку від органів державної влади, органів місцевого самоврядування, військових формувань, підприємств, установ і організацій незалежно від форми власності інформацію, документи і матеріали;

– доступу в установленому порядку своїх уповноважених представників на об'єкти, державний контроль щодо яких покладено на Державну службу спеціального зв'язку та захисту інформації України;

– проводити планові та позапланові перевірки: стану криптографічного та технічного захисту державних інформаційних ресурсів та інформації; додержання ліцензійних умов провадження господарської діяльності з надання послуг у галузі криптографічного та технічного захисту інформації; стану протидії технічним розвідкам;

– складати протоколи про адміністративні правопорушення; ініціювати в установленому порядку проведення службових розслідувань щодо з'ясування причин та умов виникнення порушень, виявлених за результатами державного контролю;

– зупиняти дію або скасовувати: експертні висновки; свідоцтва про допуск до експлуатації засобів криптографічного захисту інформації; декларації та атестати відповідності комплексних систем захисту інформації;

– порушувати в установленому законодавством порядку питання про: припинення обробки інформації; зупинення дії або скасування спеціальних дозволів.

У свою чергу, аналогічно до норм, що визначають обовязки, із врахуванням вимог Закону України «Про основні засади забезпечення інформбезпеки України» Закон України «Про Державну службу спеціального зв'язку та захисту інформації України» доповнено правами звертатися до суду в разі виникнення спорів з питань організації спеціального зв'язку та захисту інформації, криптографічного та технічного захисту державних інформаційних ресурсів та інформації; та проводити планові й позапланові перевірки: кваліфікованих надавачів електронних довірчих послуг, їхніх відокремлених пунктів реєстрації, засвідчувального центру, центрального засвідчувального органу щодо дотримання вимог законодавства у сфері електронних довірчих послуг [61].

Треба зазначити, що безпосередня діяльність щодо забезпечення інформзахисту покладена на спеціальний орган, який функціонує у складі Державної служби спеціального зв'язку та захисту інформації України – Державний центр інформзахисту та протидії інформзагрозам (далі – (ДЦКЗ), Центр), положення про який затверджено наказом Державної служби спеціального зв'язку та захисту інформації України від 11 листопада 2016 року № 704 [62].

ДЦКЗ створено Державною службою спеціального зв'язку та захисту інформації України на базі Державного центру захисту інформаційно-телекомунікаційних систем Держспецзв'язку. Необхідність створення центру передбачена Законом України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 № 80/94-ВР. Свою роботу ДЦКЗ розпочав з 1 липня 2015 року. Функції Центру мають, переважно, координаційну спрямованість та полягають у забезпеченні ефективної взаємодії органів державної влади з питань запобігання та усунення наслідків

інформінцидентів; координації діяльності операторів та провайдерів щодо збору інформації про інформінциденти; міжнародної координації з питань інформзахисту. На нашу думку, така спеціалізація визначає індивідуальний адміністративно-правовий статус Центру у сфері забезпечення інформбезпеки України, так як фіксує можливості та обов'язки конкретного суб'єкта.

Державний центр інформзахисту та протидії інформзагрозам відповідно до покладених на нього завдань здійснює:

1) забезпечення функціонування команди реагування на комп'ютерні надзвичайні події України CERT-UA;

2) проведення оцінки стану захищеності державних інформаційних ресурсів в інформаційно-телекомунікаційних системах органів державної влади;

3) забезпечення функціонування та розвитку системи антивірусного захисту інформації для органів державної влади;

4) забезпечення функціонування, безпеки та розвитку Національної системи конфіденційного зв'язку;

5) забезпечення функціонування та модернізації Системи захищеного доступу до мережі Інтернет органів державної влади України та Захищеного вузлу Інтернет-доступу Держспецзв'язку;

6) впровадження новітніх і перспективних технологій в інформаційно – телекомунікаційних системах;

7) проведення експертиз комплексних систем захисту інформації та засобів захисту інформації в органах державної влади, а також експертиз програмних, апаратних і програмно-апаратних засобів у сфері захисту інформації;

8) адміністрування та модернізація Реєстру інформаційно-телекомунікаційних систем державних органів.

У складі ДЦКЗ функціонує спеціалізований структурний підрозділ – Команда реагування на комп'ютерні надзвичайні події України (англ. Computer

Emergency Response Team of Ukraine, CERT-UA) для забезпечення інформзахисту та протидії інформзагрозам. CERT-UA є акредитованим членом FIRST (англ. Forum for Incident Response and Security Teams, FIRST) та активно взаємодіє з аналогічними командами в усьому світі.

2 лютого 2018 року у складі Державного центру інформзахисту та протидії інформзагрозам Держспецзв'язку відкрито новий підрозділ – Центр реагування на інформзагрози (англ. Cyber Threat Response Centre – CRC). Основною діяльністю підрозділу є забезпечення інформзахисту органів державної влади та об'єктів критичної інформаційної інфраструктури України.

Зокрема, ст. 23 Закону України «Про Національну поліцію», поліція запобігає вчиненню адміністративних та кримінальних правопорушень, шляхом здійснення превентивної та профілактичної діяльності [63].

Загалом, завданнями поліції є надання поліцейських послуг у сферах:

1) забезпечення публічної безпеки і порядку;

2) охорони прав і свобод людини, а також інтересів суспільства і держави;

3) протидії злочинності;

4) надання в межах, визначених законом, послуг з допомоги особам, які з особистих, економічних, соціальних причин або внаслідок надзвичайних ситуацій потребують такої допомоги [63].

Безпосередньо у галузі забезпечення інформбезпеки НПУ наділена повноваженнями щодо забезпечення прав і свобод людини і громадянина, інтересів суспільства і держави від злочинних посягань у інформпросторі; запобігання, виявлення, припинення та розкриття інформзлочинів; підвищення поінформованості громадян про безпеку в інформпросторі [509]. Діяльність Нацполіції спрямовується та координується КМУ через підпорядковуваний орган – Міністерство внутрішніх справ (далі – МВС). Слід відзначити, що МВС як Центральний орган виконавчої влади також відіграє значну роль у процесі забезпечення інформбезпеки. Виконуючи функції центрального органу

виконавчої влади МВС реалізує повноваження щодо: створення і забезпечення функціонування підрозділів з протидії інформзлочинності; розробки та реалізації комплексу організаційних і практичних заходів, спрямованих на боротьбу з інформзлочинами; створення і забезпечення функціонування цілодобової контактної мережі для надання невідкладної допомоги у розслідуванні інформзлочинів тощо [64]. Вважаємо суттєвим недоліком відсутність серед суб'єктів забезпечення інформбезпеки України, визначених Законом України «Про основні засади забезпечення інформбезпеки України», МВС України.

У структурі Національної поліції відповідно до постанови Кабінету Міністрів України № 831 від 13 жовтня 2015 року «Про утворення територіального органу Національної поліції» [65] створено спеціальний підрозділ, діяльність якого безпосередньо пов'язана із організацією протидії правопорушенням у інформсфері – інформполіцію.

Служба безпеки України реалізує повноваження щодо забезпечення національної безпеки у інформсфері через Ситуаційний центр забезпечення інформбезпеки, завдання якого безпосередньо пов'язані:

1) із запобіганням, виявленням, припиненням та розкриттям злочинів проти миру і безпеки людства, які вчиняються у інформпросторі;

2) здійсненням контррозвідувальних та оперативно-розшукових заходів, спрямованих на боротьбу з інформтероризмом та інформшпигунством;

3) проведенням негласних перевірок готовності об'єктів критичної інфраструктури до можливих інформатак та інформінцидентів;

4) протидією інформзлочинності, наслідки якої можуть створити загрозу життєво важливим інтересам держави;

5) розслідуванням інформінцидентів та інформатак щодо

державних електронних інформаційних ресурсів, критичної інформаційної інфраструктури;

6) забезпеченням реагування на інформінциденти у сфері державної безпеки.

Комплексний підхід до визначення стратегії розвитку системи інформаційної безпеки в умовах глобалізації поєднує функціонування джерел захисту інформації, високий рівень технічного й нормативно-правового забезпечення, конкурентоспроможну професійну компетенцію державних службовців. Запропоновано концептуальні засади державного управління у сфері інформаційної безпеки при реагуванні на загрози, які включають сукупність спеціальних практичних заходів, засобів, важелів, спрямованих на досягнення головної мети якнайшвидшої ліквідації наслідків таких ситуацій та відновлення нормальної життєдіяльності громадян, органів державного управління та місцевого самоврядування, підприємств тощо.

ВИСНОВКИ

У магістерській роботі вирішено актуальне наукове завдання, яке полягає в розробці організаційних основ державної політики запобігання інформаційним загрозам, що надали змогу сформулювати ряд висновків і рекомендацій, що мають як теоретичне, так і практичне значення.

1. Досліджено засади державного управління інформаційною безпекою в умовах зовнішнього впливу. Проаналізовано риси та ознаки національної безпеки, суспільний запит на інформаційну безпеку, виділені значущі фактори державної інформаційної безпеки. Доведено, що з позиції системного підходу система забезпечення інформаційної безпеки являє собою відкриту систему зі специфічними і структурними елементами, яка має власні внутрішні зв'язки і зв'язки з навколишнім середовищем, а також функціонує й розвивається під впливом численних факторів. Доведено, що інформаційна безпека займає ключове місце в системі національної безпеки держави. Проблеми інформаційної безпеки на сьогодні актуалізуються тим, що значно зросла роль накопичення, обробки й поширення інформації, зокрема, в ухваленні стратегічних рішень, збільшилася кількість суб'єктів інформаційних відносин і споживачів інформації.

2. Досліджено сучасний стан нормативно-правового регулювання інформаційної безпеки та з'ясовано, що нормативно-правові документи з проблематики знаходяться в стадії формування, а тому це несе риси перехідного етапу, визначено проблеми правового забезпечення державного управління інформаційною безпекою. Запропоновані рекомендації щодо покращення функціонування системи інформаційної безпеки органів державної влади, які спрямовані на підвищення ефективності їх діяльності, на захист інтересів держави, а також на захист органів державної влади від несанкціонованого доступу до наявних інформаційних ресурсів. Виділено національні інтереси в

інформаційній сфері України, що, у свою чергу, включають інтереси особистості, інтереси суспільства та інтереси держави. Визначено, що для реалізації національних інтересів в інформаційній сфері слід переглянути пріоритети державної політики, розробити нові концептуальні підходи щодо регулювання ринку інформаційно-комунікаційних технологій, інформаційної та інвестиційної політики, розвитку інформаційного законодавства та забезпечення інформаційної безпеки.

3. Обґрунтовано комплексний підхід до визначення стратегії розвитку системи інформаційної безпеки в умовах глобалізації, що поєднує функціонування джерел захисту інформації, високий рівень технічного й нормативно-правового забезпечення, конкурентоспроможну професійну компетенцію державних службовців. Важелем такого підходу виступає стратегічне управління, що спрямоване на моделювання ситуації успіху й загроз, здатності виявляти необхідність змін, які відповідають виклику з боку оточення та дають змогу досягати інноваційних переваг, їх гнучко реалізовувати, тим самим формуючи довгострокові перспективи

4. Запропоновано шляхи вирішення проблеми державного управління у сфері забезпечення інформаційної безпеки в умовах турбулентності, які полягають у симбіозі делегування широких повноважень на локальний рівень при належному контролі центру й «культури безпеки» як форми реалізації турботи про себе. Розвиток культури інформаційної безпеки передбачає кілька важливих кроків - це зміцнення громадянської свідомості, посилення локальних спільнот і розширення певних прав громадян, пов’язаних із самозахистом, самоактуалізацією та особистою відповідальністю за теперішнє і майбутнє. На прикладі розгляду інформаційних викликів державі та особистості підтверджена ефективність застосування моделі підтримки рівноваги стану динамічної системи для вироблення дієвих стратегій забезпечення інформаційної безпеки в державному управлінні.

5. Аргументованість упровадження нової сучасної концепції розвитку системи державного управління у сфері інформаційної безпеки полягає в зміні орієнтиру, а саме нова концепція повинна бути людиноцентричною, сприяти забезпеченню захищеності і, як наслідок, стійкості основних сфер життєдіяльності (економіки, науки, сфери державного і військового управління, а також суспільної свідомості) від небезпечних, дестабілізуючих і деструктивних інформаційних впливів - на рівні суспільства й держави. У той же час на рівні особистості інформаційна безпека повинна забезпечити захищеність психіки і свідомості людей від небезпечних інформаційних впливів: маніпулювання, дезінформування, спонукання до самогубства.

6. Систематизовано та визначено сучасну систему принципів державного управління у сфері забезпечення інформаційної безпеки громадян. Окреслені принципи представлені наступним змістом: прогнозування і своєчасне виявлення загроз безпеки інформаційних ресурсів, причин і факторів, що сприяють нанесенню шкоди, порушенню його нормального функціонування й розвитку; створення умов функціонування з найменшою вірогідністю реалізації загроз безпеки інформаційних ресурсів і нанесення різних видів шкоди; забезпечення механізму й умов оперативного реагування на загрози інформаційної безпеки та прояву негативних тенденцій у функціонуванні, ефективне припинення зазіхань на ресурси на основі правових, організаційних і технічних заходів і засобів забезпечення безпеки; створення умов для максимально можливого відшкодування та локалізації збитку, що наноситься неправомірними діями фізичних і юридичних осіб.

7. Запропоновано концептуальні засади державного управління у сфері інформаційної безпеки, що загрожують національній безпеці, які включають державно-регулюючий, інформаційно-організаційний, медико-психологічний, превентивно-просветницький функціонали. Запропонований конструктив полягає у вирішенні завдань, щодо

забезпечення інформаційної безпеки як складової національної безпеки держави, а саме: необхідність нормативно-правового регулювання щодо протидії використання інформаційних технологій, які загрожують інтересам держави; необхідність створення економічних передумов для розвитку національних інформаційних ресурсів та інфраструктури, впровадження новітніх технологій в інформаційну сферу. Інформаційна безпека, виходячи з двоєдиної сутності інформації, повинна бути спрямована як на захист об’єктивної, так і суб’єктивної її складової. У першому випадку вона виступає у вигляді безпеки інформації, у другому - у вигляді інформаційно-психологічної безпеки.

Висвітлені концептуальні засади включають сукупність спеціального теоретико-методологічного підґрунтя, а також практичні заходи, засоби, важелі, спрямовані на досягнення основних цілей щодо розбудови надійної інформаційної безпеки держави, а саме: протистояння інформаційним загрозам, мінімізація їх наслідків, якнайшвидшої ліквідації наслідків таких ситуацій та відновлення нормальної життєдіяльності громадян, органів державного управління та місцевого самоврядування, підприємств тощо.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Конституція України, Закон від 28.06.1996 № 254к/96-ВР. Редакція від 01.01.2020. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96- %Б0%Б2%Б 1%80.

2. Ковтун С.В. Інформаційна безпека: підручник. Харків. Вид. ХНЕУ, 2009. 368 с.

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

4. Лопатин В.Н. Правовые проблемы защиты единого информационного пространства страны. Информация и государство. Вопросы защиты информации. 2001. № 2. С. 8-20.

5. Баранов О.А. Базовий принцип інформаційного права - забезпечення інформаційної безпеки. Запобігання новим викликам та загрозам інформаційній безпеці України: правові аспекти: матеріали наук.- практ. конф. 06 жовт. 2016 р. Упоряд. : В. М. Фурашев. Київ : НТУУ «КПІ імені Ігоря Сікорського», Вид-во «Політехніка». 2016. 204 с. С. 29-35

6. Закон України «Про Концепцію Національної програми інформатизації»; Концепція від 04.02.1998 № 75/98-ВР. URL: https://zakon.rada.gov.ua/laws/show/75/98-%D0%B2%D1%80

7. Настюк В.Я., Бєлєвцева В.В. Адміністративно-правовий захист інформації: проблеми та шляхи вирішення: монографія. Київ: Ред. журн. «Право України»; Харків: Право, 2013. 128 с. (Наук. зб. «Академічні правові дослідження». Дод. до юрид. журн. «Право України»; вип. 28.

8. Joint Publication 3-13, “Information Operations”, 27 November 2012, Incorporating Change 1, 20 November 2014, URL: http://www.fas.org/irp/doddir/dod/ip3 13.pdf (дата звернення: 16.11.2022).

9. Манжай О.В. Використання інформпростору в оперативно-розшуковій діяльності. *Право і Безпека.* 2009. № 4. С. 215-219.

10. Мартинюк В. ЄС у протидії гібридним загрозам та Україна: нечіткість у підходах. URL: https://dt.ua/mtemal/yes-u-protidiyi-gibridmm-zagrozam-ta- ukrayina-nechitkist-u-pidhodah-253570_.html

11. Магда Є.М. Гібридна війна: сутність і структура феномену. *Міжнародні відносини. Серія «Політичні науки».* № 4 (2014). URL: http: //j ournals. iir.kiev.ua/index.php/pol_n/article/view/2489/2220.

12. Закон України «Про національну безпеку України» від 21.06.2018 № 2469-VIII. URL: https://zakon.rada.gov.ua/ laws/show/2469-19.

13. Закон України «Про Національну програму інформатизації» від 04.02.1998 № 74/98-ВР. URL: https://zakon.rada.gov.ua/ laws/show/74/98- %D0%B2%D1%80.

14. Логінов О.В. Адміністративно-правове забезпечення інформаційної безпеки органів виконавчої влади: дис. ... канд. юрид. наук: спец. 12.00.07. Київ, 2005. 210 с.

15. Указ президента України №47/2017. Про рішення Ради національної

безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України». URL: http://www.president.gov.ua/documents/472017-21374 (дата звернення: 28.10.2022).

16. Указ Президента України № 96/2016 від 15.03.2016 р. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України»: URL: https://zakon.rada.gov.uaЛaws/show/n0003525-16#Text. (дата звернення:28.10.2022).

17. Ліпкан В.А. Стратегічні комунікації: словник. Київ: ФОП Ліпкан О.С., 2016. 416 с.

18. Ліпкан В.А. Теоретичні основи та елементи національної

безпеки : монографія. Київ: «Текст», 2003. 600 с.

20. Триняк В.Ю. Сутнісні аспекти інформаційної безпеки в умовах глобалізації. *Наукові записки Харківського університету Повітряних Сил. Соціальна філософія, психологія.* Харків: ХУПС, 2007. Вип. 3(29). С. 142-149.

21. Маруженко О.П. Інформаційне забезпечення законотворчого процесу в Україні: дис. ... канд. юрид. наук: 12.00.07. Київ, 2009. 202 с.

22. Шульга В. І. Сучасні підходи до трактування поняття інформаційна безпека. Ефективна економіка, № 4, 2015. 13.06.2017 ЦКк: http://www.economy.nayka.com.ua/ ?op=1&2=5514.

20. Скулиш Є., Прокоф'єва Д. Безпека кіберпростору як елемент національної безпеки в умовах глобалізації інформаційних процесів. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні.* 2007. Вип. 2 (15). С. 26-31.

21. Соловйов В.М. Поняття і сутність правового регулювання державного управління в Україні. *Університетські наукові записки.* 2007. № 3 (23). С. 27-33.

22. Марценюк О.Г. Теоретико-методологічні засади інформаційного права України: реалізація права на інформацію: автореф. дис. на здобуття наук. ступеня канд. юрид. наук: спец. 12.00.07 «Адміністративне право і процес; фінансове прав Нестеряк Ю. Міжнародні критерії інформаційної безпеки держави: теоретико- методологічний аналіз // Публічне управління: теорія та практика. 2014. Вип. 1. С. 62-67.

23. Нестеряк Ю. Законодавче врегулювання відносин влади і засобів масової комунікації: принципи та механізми на основі узагальнення міжнародного досвіду // НАДУ. ШЬ: http://www.academy.gov.ua/ej/ej14/txts/Nesteryak.pdf.

24. Нестеряк Ю. Міжнародні критерії інформаційної безпеки держави: теоретико- методологічний аналіз // Вісник Національної академії державного управління при Президентові України. Науковий журнал. 2013. № 3. С. 40-45.

25. Скулиш Є., Прокоф'єва Д. Безпека кіберпростору як елемент національної безпеки в умовах глобалізації інформаційних процесів. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні.* 2007. Вип. 2 (15). С. 26-31.

26. Олійник О. Стан забезпечення інформаційної безпеки в Україні // Юридичний вісник. Повітряне і космічне право. 2014. № 2. С. 59-65.

27. Новицький Г.В. Теоретико-правові основи забезпечення національної безпеки України: [монографія]. К.: Інтертехнологія, 2008. 496 с.

28. Мельник С.В. До проблеми формування понятійно-термінологічного апарату інформбезпеки. *Актуальні проблеми управління інформаційною безпекою держави:* зб. матер. наук.-практ. конф. (Київ, 22 березня 2011 р.). Київ: Вид-во НА СБ України, 2011. Ч. 2. С. 43-48.

29. Старіш О.Г. Інформаційна політика держави в контексті глобалізації. Дисертація на здобуття наукового ступеня доктора політичних наук за спеціальністю 23.00.03. Політична культура та ідеологія. Київський національний університет імені Тараса Шевченка. Київ. 2008. 401 с.

30. Пазюк А. Питання міжнародного інформаційного права: предмет, завдання та принципи // Український часопис міжнародного права. 2013. №2 1. С. 46-50.

31. Твердохліб О. Організаційно-правові засади забезпечення інформаційної відкритості органів державної влади в контексті розвитку інформаційного суспільства в Україні. Реформування публічного управління: теорія, практика, міжнародний досвід : матеріали Всеукр. наук.-практ. конф. за міжнар. участю (31 жовт. 2014, м. Одеса). Одеса: ОРІДУ НАДУ, 2014. С. 308-309.

32. Житко А.О. Кібервійна як складова гібридної війни. *Українське суспільство в умовах війни: виклики сьогодення та перспективи миротворення:* матеріали Всеукраїнської науково-практичної конференції, м. Маріуполь, 9 червня 2017 р. Маріуполь: ДонДУУ. 2017. С.263-266.

33. Петров В. Воєнно-інформаційна безпека України за умов посилення загроз інформаційних війн: автореф. дис. ...канд. політ. н. (спеціальність: 21.01.01 - основи національної безпеки держави). Київ. 2010. 24 с.

34. Рижук О. Аналіз підходів щодо визначення поняття «інформаційна безпека» в умовах глобалізації. 02.08.2017 URL: http://ioumals.iir.kiev.ua/index.php/pol n/article/view/3007/2697 (дата звернення: 16.10.2022).

35. Заплатинський В.М. Логіко-детермінантні підходи до розуміння поняття «Безпека». *Вісник Кам ’янець-Подільського національного університету імені Івана Огієнка. Фізичне виховання, спорт і здоров’я людини.* Кам'янець-Подільський: Кам’янець-Подільський національний університет імені Івана Огієнка. 2012. Випуск 5. С. 90-98.

36. Морозова В.О. Державна політика та стратегії сша у сфері інформаційної безпеки в умовах глобальних викликів. *Політика і духовність в умовах глобальних викликів. Серія 22. Політичні науки та методика викладання соціально-політичних дисциплін.* 2014. С. 154-159.

37. Золотар О.О. Інформаційна безпека людини:теорія і практика : монографія. Київ : ТОВ «Видавничий дім «АртЕк», 2018. 446 с

38. Довгань О.Д. Правові засади формування і розвитку системи забезпечення інформаційної безпеки України. Інформаційна безпека людини, суспільства, держави. 2015, № 3 (19). С. 6-17

39. Стратегія національної безпеки України, затверджена Указом Президента України від 26 травня 2015 року № 287/2015 28.07.2017 URL: www.rada.gov.ua (дата звернення: 16.10.2022).

40. Нашинець-Наумова А.Ю. Інформаційна безпека: питання правового регулювання: монографія. Київ: Видавничий дім «Гельветика», 2017. 168 с.

41. Мануйлов Є.М. Аксіологічний вимір інформаційної безпеки української держави. Вісник Національного університету «Юридична академія України імені

Ярослава Мудрого» № 3 (34) 2017. С. 13-30

42. Марущак А. Інформаційна безпека: правовий аналіз // Детектор медіа 20 травня 2008 URL: https://detector.media/infospace/article/38472/2008-05-20-informatsiina- bezpeka-pravovii-analiz/ (дата звернення: 16.10.2022).

43. Національний координаційний центр інформбезпеки повинен мобілізувати весь наявний потенціал для забезпечення надійного інформзахисту країни. URL: http: //turchynov.com/news/detail s/nacionalnij - koordinacij nij-centr- kiberbezpeki-povinen-mobilizuvati-ves-nayavnij -potencial.

44. Нестеряк Ю.В. Міжнародні критерії інформаційної безпеки держави: теоретико-методологічний аналіз. Вісник НАДУ. № 3. 2013. С. 40-45.

45. Корж І.Ф. Об’єкт і предмет наукового дослідження в інформаційній сфері. “Інформація і право” № 3(22)/2017. С. 19-26.

46. Баранов О.А. Базовий принцип інформаційного права - забезпечення інформаційної безпеки. Запобігання новим викликам та загрозам інформаційній безпеці України: правові аспекти: матеріали наук.- практ. конф. 06 жовт. 2016 р. Упоряд. : В. М. Фурашев. Київ : НТУУ «КПІ імені Ігоря Сікорського», Вид-во «Політехніка». 2016. 204 с. С. 29-35

47. Ткачук Т. Ю. Принципи забезпечення інформаційної безпеки держави: інформаційний аспект. Митна справа. 2012. № 1. Ч. 2. С. 399-405

48. Золотар О.О. Досвід правового забезпечення інформаційної безпеки в країнах східного партнерства ЄС (Молдова, Грузія). LEX PORTUS № 3 (5)’2017. С. 70-80

49. Нормативно-правове регулювання забезпечення інформаційної безпеки США. URL: https://pidruchniki.com/82889/politologiya/normativno-pravove_regulyuvannya_zabezpechennya_informatsiynoyi_bezpeki.

50. Пода Т. Інформаційно-комунікаційні технології в контексті сучасних міжнародних відносин: соціально-філософський аналіз // Вісник Національного авіаційного університету. Серія: Філософія. Культурологія: Збірник наукових праць. Київ: НАУ. 2013. С. 59-63.

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

52. Сащук Г. Інформаційна безпека в системі забезпечення національної безпеки // Сайт Інституту журналістики КНУ імені Тараса Шевченка. URL: http : //www.j ourn. univ.kiev.ua/trk/publikacii/satshuk_publ. php.

53. Кохановська О.В. Інформаційно-правова основа громадянського суспільства. *Право України,* 2015. № 4. С.35-42.

54. Олійник О.В. Інформаційна безпека США. *Боротьба з організованою злочинністю і корупцією (теорія і практика).* № 1 (27). 2012. С. 280-288. URL: http://irbis-nbuv.gov.ua/cgi-.

55. Присяжнюк М., Цифра Є.І. Особливості забезпечення інформбезпеки. *Реєстрація, зберігання і обробка даних.* 2017. Т. 19. № 2. С. 61-68.

56. National Security Telecommunications and Information Systems Security. National Training Standard for Information Systems Security (Infosec): URL: www.cnss.gov/Assets/pdf/nstissi 4011 .pdf (дата звернення: 16.10.2022).

57. Сопілко І. Роль доктрини інформаційної безпеки України в реалізації державної інформаційної політики України // Журнал східноєвропейського права. 2014. № 2. С. 36-42.

58. Степко О. Інформаційна діяльність ООН: автореф. дис. ...канд. політ. н. (спеціальність: 23.00.04 - політичні проблеми міжнародних систем та глобального розвитку). Київ. 2004. 17 с.

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

60. Проданюк Р. І. Інформаційна безпека в соціологічному контексті: до постановки проблеми. Наук.-теоретичний альманах «Грані». 2018. Т. 21. № 4. С. 84-90

61. Сащук Г. Інформаційна безпека в системі забезпечення національної безпеки. URL: http://journ.univ.kiev.ua/trk/publikacii/satshuk_publ.php (дата

звернення:16.10.2022

62. У Держспецзв’язку створено Державний центр інформзахисту та протидії інформзагрозам. URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=156473&cat_id=119123.

63. Мельник С.В. Понятійно-категоріальний аппарат у системі професійної підготовки майбутніх фахівців з кібербезпеки. Інформаційні технології і засоби навчання. 2016, Том 55, №5 С.187-197