ХМЕЛЬНИЦЬКА ОБЛАСНА РАДА
ХМЕЛЬНИЦЬКИЙ УНІВЕРСИТЕТ УПРАВЛІННЯ ТА ПРАВА
ІМЕНІ ЛЕОНІДА ЮЗЬКОВА
ФАКУЛЬТЕТ УПРАВЛІННЯ ТА ЕКОНОМІКИ
Кафедра публічного управління та адміністрування

МАГІСТЕРСЬКА РОБОТА

на тему:

«ІНФОРМАЦІЙНА БЕЗПЕКА УКРАЇНИ В УМОВАХ РОЗВИТКУ СУЧАСНОГО СУСПІЛЬСТВА»

Виконала: студентка магістратури за спеціальністю 281 Публічне управління та адміністрування (заочної форми навчання)
Супрович Тетяна Станіславівна
(прізвище, ім'я та по-батькові)

Керівник: Кандидат економічних наук
Омельчук Л.В.
(науковий ступінь, вчене звання, прізвище та ініціали)

Рецензент:

(науковий ступінь, вчене звання, прізвище та ініціали)

Хмельницький – 2022 рік

Анотація

Супрович Т.С. Інформаційна безпека України в умовах розвитку сучасного суспільства. – Рукопис.

Магістерська робота на здобуття освітнього ступеня магістра за спеціальністю 281 Публічне управління та адміністрування. – Хмельницький університет управління та права імені Леоніда Юзькова. – Хмельницький, 2022.

Магістерська робота присвячена обґрунтуванню теоретичних та практичних аспектів забезпечення інформаційної безпеки України в умовах розвитку сучасного суспільства. У роботі розкрито сутність та особливості інформаційної безпеки, досліджено організаційно-інституційне забезпечення інформаційної безпеки України. Автором виявлено ризики інформаційної безпеки України в контексті російсько-української війни, а також охарактеризовано функції забезпечення інформаційної безпеки в Україні в умовах повномасштабної збройної агресії російської федерації.

На основі проведеного дослідження, автором виявлені пріоритети підвищення інформаційної безпеки України та запропоновані стратегічні напрями забезпечення ІБ в сучасних умовах.

Annotation

Suprovych T.S. Information security of Ukraine in the conditions of development of modern society. – Manuscript.

Master's thesis for a master's degree in Specialty 281 Public Management and Administration. – Leonid Yuzkov Khmelnytsky University of Management and Law. – Khmelnitsky, 2022.

The master's thesis is devoted to the substantiation of theoretical and practical aspects of ensuring information security of Ukraine in the conditions of the development of modern society. The work reveals the essence and features of

information security, investigates the organizational and institutional provision of information security in Ukraine. The author identified the risks of information security of Ukraine in the context of the Russian-Ukrainian war, and also characterized the functions of ensuring information security in Ukraine in the conditions of full-scale armed aggression of the Russian Federation.

On the basis of the conducted research, the author identified the priorities of improving information security of Ukraine and proposed strategic directions for IS provision in modern conditions.

ЗМІСТ

ВСТУП

Актуальність теми дослідження. Динаміка відносин в інформаційній сфері постійно випереджає розвиток суспільної правосвідомості, встановлені норми суспільних відносин, ускладнює створення стабільної правової регламентації. Недосконаліть нормативно-правової бази дозволяє окремим суб'єктам реалізовувати свої протиправні наміри в інформаційній сфері як щодо життєво важливих інтересів інших суб'єктів, так і об'єктів національної безпеки. Питання забезпечення інформаційної безпеки (далі – ІБ) є вкрай важливими для української держави на сучасному етапі, що, насамперед, обумовлено необхідністю протистояти протиправним посяганням на інформаційний простір України, збереження інформаційних ресурсів, захисту населення від негативного інформаційного впливу тощо.

Окрім цього, стратегічно визнаним пріоритетом зовнішньої політики України є європейська інтеграція, що вимагає удосконалення нормативно-правової бази забезпечення ІБ України, яке б відповідало не лише міжнародним стандартам, а передусім українським національним інтересам в інформаційній сфері. Зазначене вище знаходить відображення у прийнятій Стратегії Національної безпеки України [87]. У своїх положеннях вона визначила пріоритети державної політики національної безпеки, вказавши на основні її цілі, а саме: мінімізацію загроз державному суверенітету та створення умов для відновлення територіальної цілісності України у межах міжнародно-визнаного державного кордону України, гарантування мирного майбутнього України як суверенної і незалежної, демократичної, соціальної, правової держави; утвердження прав і свобод людини і громадянина, забезпечення нової якості економічного, соціального і гуманітарного розвитку, забезпечення інтеграції України до ЄС та формування умов для вступу в НАТО. Крім того, Стратегія визначила як основні загрози ІБ: ведення інформаційної війни проти України; відсутність цілісної

комунікативної політики держави, недостатній рівень медіакультури суспільства. Викладене обумовлює актуальність теми дослідження.

Ступінь розробленості проблеми. Дослідженню різнобічних аспектів інформаційної безпеки присвячені праці значної кількості вітчизняних та зарубіжних науковців: Архипової Є. [3], Березовської І. [6], Гаврильців М. [11], Гончарова М. [15], Гурковського В. [20], Довганя О. [24, 25], Заярного О. [27], Золотар О. [28, 29], Кормича Б. [33, 34], Логінова О. [39], Максименка Ю. [40], Малашко О. [41, 42, 81, 83, 84], Нашинець-Наумової А. [45], Перун Т. [53, 54], Сопільник Л. [83, 84], Тихомирова О. [90], Ткачук Т. [91, 92] та інших. Проте, незважаючи на значний рівень наукового осмислення проблем ІБ, в сучасних умовах стрімкого розвитку інформаційних технологій, засобів та способів ведення інформаційних війн нагальними є питання удосконалення її забезпечення, що й обумовлює актуальність теми магістерського дослідження.

Метою магістерської роботи є обґрунтування теоретичних та практичних аспектів забезпечення ІБ України в умовах розвитку сучасного суспільства. Для виконання поставленої мети були сформульовані та послідовно виконані такі **завдання:**

— розкрити сутність та особливості ІБ;

— дослідити організаційно-інституційне забезпечення ІБ України;

— виявити ризики ІБ України в контексті російсько-української війни;

— охарактеризувати функції забезпечення ІБ в Україні в умовах повномасштабної збройної агресії російської федерації;

— виявити пріоритети підвищення ІБ України;

— запропонувати стратегічні напрями забезпечення ІБ в сучасних умовах.

Об’єктом магістерської роботи є ІБ як складова національної безпеки, що відіграє одну з ключових ролей у забезпеченні життєво важливих інтересів держави. **Предметом** – ІБ України в умовах розвитку сучасного суспільства.

Для розв’язання поставлених завдань у магістерській роботі використано загальнонаукові та спеціальні **методи дослідження**, вибір яких обумовив достовірність отриманих результатів та висновків: цілісність дослідження забезпечує системний підхід; для визначення причинно-наслідкових зв’язків виникнення проблем у процесах забезпечення ІБ України та їх подальшого вдосконалення було використано процесний підхід. За допомогою категоріального аналізу досліджено понятійний апарат. Індуктивний метод був використаний при узагальненні результатів дослідження.

Інформаційною базою дослідження стали чинні нормативно-правові акти України, які стосуються досліджуваної проблематики, монографії, статті у наукових фахових виданнях тощо.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ЗАСАДИ РЕАЛІЗАЦІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1. Сутність та особливості інформаційної безпеки

В умовах європейської інтеграції України та враховуючи сучасні вимоги побудови інформаційного суспільства все більшої актуальності набуває питання про сутність ІБ в умовах розвитку сучасного суспільства. Слід зазначити, що в сучасному світі проблеми ІБ набувають принципово нових рис. Військова агресія проти України призвела до необхідності негайного перегляду стратегічних засад і наукових поглядів, на яких функціонувала система ІБ нашої держави.

Питання сутності ІБ в умовах розвитку сучасного суспільства є одним із головних для України, яке тісно пов’язане з вирішенням таких питань, як захист суверенітету та територіальної цілісності країни, забезпечення її економічної безпеки, оскільки рівень ІБ активно впливає на політичну, економічну, оборонну та інші складові національної безпеки держави.

На сьогодні сутністю ІБ України є здатність нашої держави захистити національні економічні інтереси від зовнішніх і внутрішніх загроз, а також здатність національної економіки підтримувати й відновлювати процес суспільного відтворення.

Необхідною умовою розвитку сучасного суспільства є високий рівень ІБ. Тому ефективне регулювання інформаційних ресурсів є важливою умовою забезпечення ІБ та реалізації продуманої державної політики.

Наша держава повною мірою включена в процеси комп’ютеризації суспільства та створення єдиного світового інформаційного ринку. Інформаційний чинник має певне значення в процесі формування та становлення основних інститутів влади, у представленні та захисті інтересів держави. Велике значення в цьому спектрі суспільних відносин посідають

проблеми сутності ІБ та розробки якісної системи захисту інформації, яка б відповідала сучасним вимогам і нагальним потребам України [46, с. 17).

Перш за все, потребує уточнення визначення поняття «ІБ». Законодавство України донедавна не містило визначення цього поняття, за винятком, лише умовним, Закону України «Про основні засади розвитку інформаційного суспільства в Україні у 2007-2015 роках» від 9 січня 2007 р. [69], оскільки його назва містить певні обмеження для реалізації цього закону. Згідно з нею ІБ – це стан захищеності життєво важливих інтересів людини, суспільства і держави, за якого унеможливлено заподіяння шкоди внаслідок: неповноти, застарілості та недостовірності інформації, що використовується; негативний вплив інформації; негативні наслідки використання інформаційних технологій; несанкціоноване поширення, використання та порушення цілісності, конфіденційності та доступності інформації.

Сучасний стан захисту прав і законних інтересів людини, суспільства і держави в інформаційній сфері України свідчить про низький рівень забезпечення ІБ. Вітчизняна наука почала приділяти увагу проблемам ІБ як складової частини забезпечення національної безпеки держави. Останні два десятиліття характеризуються інтенсивними дослідженнями в цій галузі, але при цьому єдиної наукової концепції щодо сутності ІБ в Україні немає. Тому виникає необхідність наукового аналізу формування та реалізації державної політики у сфері ІБ.

Вивчення проблем сутності ІБ базується на вивченні загальних методологічних основ процесу забезпечення ІБ, закономірностей розвитку інформаційного життя суспільства, шляхів і засобів використання інформаційної сфери для реалізації основних завдання держави.

У системі національної безпеки держави основне місце посідає ІБ, під якою зазвичай розуміють стан відсутності інформаційних загроз або, у разі їх виникнення, стан стабільності основних сфер життєдіяльності.

Переважна більшість сучасних дослідників характеризує ІБ як такий стан захищеності інформаційного середовища, що відповідає інтересам держави, який забезпечує можливості для створення, використання та розвитку незалежно від дії внутрішніх і зовнішніх інформаційних загроз і загроз.

При цьому під поняттям ІБ слід розуміти певну групу суспільних відносин, що виникають у процесі захисту конституційних прав і свобод людини, суспільства і держави від внутрішніх і зовнішніх небезпек і загроз в інформаційній сфері.

Слід також зазначити, що важливою особливістю ІБ, на думку Н.С. Мороза, є її динамічність, оскільки в широкому розумінні вона являє собою забезпечення стабільності та розвитку інформаційної сфери, яка постійно змінюється у зв'язку з різними потребами населення та інших учасників інформаційних відносин [44, с. 136).

За визначенням Б.О. Кормича, ІБ полягає в охороні встановлених законом правил, за якими в державі відбуваються інформаційні процеси, що забезпечують умови для існування та розвитку людини, всього суспільства, гарантовані Конституцією держави [33, с. 89).

ІБ України, на думку І. Громико, Т. Саханчук, – це захист інтересів держави, що забезпечує попередження, виявлення та нейтралізацію внутрішніх і зовнішніх інформаційних загроз, захист інформаційного суверенітету держави та безпечний розвиток міжнародного інформаційного співробітництва [19, с. 130–134].

В.С. Цимбалюк характеризує ІБ як стан інформації, за якого забезпечується збереження визначених політикою безпеки властивостей інформації [97, с. 204].

С.С. Єсімов зазначає, що сутністю інституту ІБ в системі інформаційного права є реалізація правових, організаційних і технічних заходів щодо забезпечення безпеки всіх складових державного інформаційно-комунікаційного комплексу, ресурсів інформаційної системи,

інформаційно-комунікаційної інфраструктури, науково-технічний і виробничий комплекс інформаційної галузі, ринок інформаційних продуктів і послуг, система масової інформаційної освіти, виховання та підготовки професійних кадрів для інформаційної сфери. окремі організації та кожна людина [26, с. 75].

Під ІБ Р.А. Калюжний розуміє такий вид публічно-інформаційних правовідносин щодо створення, підтримки, охорони необхідних людині, суспільству і державі умов для безпечної життєдіяльності [31, с. 234-244).

Водночас С.Ф. Гуцу пропонує визнати ІБ умовою існування інформаційної потреби особистості, суспільства і держави, що забезпечує їх функціонування та поступальний розвиток незалежно від виникнення внутрішніх і зовнішніх інформаційних загроз [21, с. 35].

На завершення Л.С. Харченко зазначає, що ІБ – це частина національної безпеки, процес управління небезпеками і загрозами державними та недержавними установами, особами, що забезпечують інформаційний суверенітет України [95, с. 65].

Слід зазначити, що на сьогодні в наукових працях досі немає єдиної концепції щодо змісту терміна «ІБ», а також не вироблено єдиного методологічного підходу до сутності ІБ.

Дослідження сутності ІБ України пов’язане зі створенням якісної системи захисту інформації, яка відповідатиме сучасним вимогам нашої держави.

Державотворчі процеси в Україні вимагають подальшого підвищення якості державного управління щодо забезпечення ІБ, розвитку методів управління, що враховують специфіку цієї сфери суспільних відносин.

Державна політика у сфері ІБ держави спрямована на захист національних інтересів держави, суспільства та особи. Основну роль у реалізації державної політики у сфері забезпечення ІБ відіграють органи державної влади. Можна визначити такий зміст державного управління у сфері забезпечення ІБ в Україні:

– нормативно-правове регулювання потреб учасників інформаційних відносин шляхом прийняття нормативно-правових актів, рішень державних органів, спрямованих на реалізацію державної політики, у тому числі сфери;

– розгляд органами державної влади важливих питань ІБ, визначення пріоритетів державної політики у цій сфері та розроблення та реалізація комплексних програм;

– достатнє фінансування та матеріально-технічне забезпечення, виділення в державному бюджеті та бюджетах місцевого самоврядування цільових коштів на фінансування державної політики у сфері ІБ України тощо.

Створення належного рівня ІБ є необхідною умовою розвитку інформаційного суспільства. Тому розбудова ефективної системи захисту інформації є одним із головних завдань забезпечення національної безпеки України. Державна політика у сфері ІБ має базуватися на науково-методичних дослідженнях, систематизованих та об’єднаних в одну концепцію.

Головною метою державної політики забезпечення ІБ України є управління реальними загрозами з метою створення необхідних умов для задоволення інформаційних потреб держави, суспільства та особи.

У багатьох наукових працях з питань ІБ завданнями державної політики України у сфері ІБ є: захист інформаційного суверенітету держави в сучасних умовах глобалізації; забезпечення достатності інформації для прийняття рішень органами влади, суб'єктами господарювання та громадянами; реалізація конституційних прав і законних інтересів людини, суспільства і держави в інформаційній сфері.

ІБ в державі має забезпечуватися реалізацією єдиної державної політики в інформаційній сфері, збалансованою системою економічних, політичних, соціальних та організаційних заходів, реальними загрозами і небезпеками національним інтересам особи, суспільства і держави в інформаційній сфері.

Таким чином, у зв’язку з розвитком інтеграційних зв’язків, входженням України в європейський інформаційний простір виникає необхідність уважного вивчення праць вчених і дослідників із зазначеної тематики з метою побудови ефективної системи захисту інформації в Україні.

Як відомо, ІБ є одним із важливих елементів системи національної безпеки України при вирішенні завдань у політичній, економічній, соціальній та інших сферах діяльності держави [41]. Водночас М. Присяжнюк та Ю. Бєлошевич зазначають, що у XXI столітті ІБ посідає перше місце в системі національної безпеки держави, тому лише ця держава може розраховувати на лідерство в економічній сфері; у військовій, політичній та інших сферах вони мають перевагу стратегічну і тактичну, більш гнучко регулюють економічні витрати на розвиток озброєння і військової техніки, зберігають перевагу в ряді передових технологій, мають перевагу в засобах інформації та інформаційній війні» [59, с. 43].

Таким чином, ІБ – це стан захищеності (в статичному вираженні) та комплекс заходів (в динамічному вираженні) в інформаційній сфері життєво важливих інтересів окремої людини (людини, громадянина) або групи людей, суспільства чи держави загалом, які своєчасно виявляють, запобігають і знешкоджують реальні, існуючі або потенційні явища та фактори, що становлять загрозу в інформаційній сфері, за змістовими, структурними та класифікаційними ознаками, а також ознаками, що забезпечують ІБ [41].

Для забезпечення ІБ, враховуючи системність та міжгалузевий характер, доцільно класифікувати за ознаками [41]:

1) за сферами державної політики в різних сферах суспільного життя;

2) за об'єктами системи забезпечення національної безпеки;

3) залежно від елементів змісту діяльності держави у сфері забезпечення ІБ;

4) через розглянуті аспекти сучасного розуміння ІБ;

5) за основними та допоміжними видами інформаційної діяльності;

6) за формами і методами забезпечення державою ІБ;

7) за напрямами (шляхами) досліджень у сфері ІБ;

8) залежно від специфіки обміну та режиму доступу з урахуванням заходів безпеки до інформації за її видами.

1.2. Організаційно-інституційне забезпечення інформаційної безпеки України

Вирішення проблеми ІБ має здійснюватися шляхом:

- створення повноцінної функціональної інформаційної інфраструктури держави та забезпечення захисту її критичних елементів;

- підвищення рівня координації діяльності державних органів щодо виявлення, оцінки та прогнозування загроз ІБ, запобігання таким загрозам та забезпечення ліквідації їх наслідків, здійснення міжнародного співробітництва з цих питань;

- удосконалення нормативно-правової бази забезпечення ІБ, зокрема захисту інформаційних ресурсів, протидії комп'ютерним злочинам, захисту персональних даних, а також правоохоронної діяльності в інформаційній сфері;

- впровадження та розвиток Національної системи конфіденційного зв'язку як сучасної захищеної транспортної бази, здатної інтегрувати територіально розподілені інформаційні системи, в яких обробляється конфіденційна інформація [69].

Після Революції Гідності 2013-2014 рр. та початку військової агресії рф проти України національне законодавство, яке почало бурхливо розвиватися, на жаль, залишило без уваги ІБ. Закон України «Про національну безпеку» від 21 червня 2018 р. хоч і містить поняття «ІБ» як складову національної безпеки, але не визначає її, на відміну від таких понять, як «військова безпека», «громадська безпека», «державна безпека», «національна безпека».

Крім того, в цьому законі залишилося невизначеним поняття економічної, зовнішньополітичної та екологічної безпеки [63].

Дещо схоже визначення міститься в Законі України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 р., але стосовно кібербезпеки, яка визначається як захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі – мережі Інтернет та інші глобальні мережі передачі даних [68] (напр., VPN-сервіси). І оскільки інформаційна діяльність поступово зміщується від традиційних типів, таких як телебачення та радіо, до Інтернету та його підтипів, таких як соціальні мережі та програми мобільного обміну повідомленнями для приватного та групового спілкування, кібербезпеку можна вважати типом ІБ як такої. Крім того, зазначеним законом визначено суб'єктів кібербезпеки, а саме:

а) загальні:

1) Президент України, який через очолювану ним Раду національної безпеки і оборони України координує діяльність у сфері кібербезпеки як складової національної безпеки України;

2) Національний координаційний центр кібербезпеки як робочий орган Ради національної безпеки і оборони України – координує та контролює діяльність суб'єктів сектору безпеки і оборони, що забезпечують кібербезпеку, вносить пропозиції Президенту України щодо формування та уточнення Стратегії кібербезпеки України;

3) Кабінет Міністрів України – забезпечує формування та реалізує державну політику у сфері кібербезпеки, захисту прав і свобод людини і громадянина, національних інтересів України в кіберпросторі та боротьби з кіберзлочинністю; організовує та надає засоби та ресурси, необхідні для функціонування національної системи кібербезпеки; формує вимоги та

забезпечує функціонування системи аудиту ІБ на об’єктах критичної інфраструктури (крім об’єктів критичної інфраструктури банківської системи України);

б) спеціальні:

1) міністерства та інші центральні органи виконавчої влади;

2) місцеві державні адміністрації;

3) органи місцевого самоврядування;

4) правоохоронні, розвідувальні та контррозвідувальні органи, суб'єкти оперативно-розшукової діяльності;

5) Збройні Сили України, інші утворені відповідно до закону військові формування;

6) Національний банк України;

7) підприємства, установи та організації, віднесені до об'єктів критичної інфраструктури. При цьому до об’єктів критичної інфраструктури можуть належати підприємства, установи та організації незалежно від форми власності, які: 1) провадять діяльність та надають послуги у сферах енергетики, хімічної промисловості, транспорту, інформаційно-комунікаційних технологій, електронних комунікацій, банківської та фінансові сектори; 2) надають послуги у сферах забезпечення життєдіяльності населення, а саме у сферах централізованого водопостачання, водовідведення, електро- та газопостачання, виробництва харчових продуктів, сільського господарства, охорони здоров'я; 3) є комунальними, аварійно-рятувальними службами, екстреним обслуговуванням населення; 4) включено до переліку підприємств, що мають стратегічне значення для економіки та безпеки держави; 5) є об'єктами потенційно небезпечних технологій і виробництв;

8) суб’єкти господарювання, громадяни України та об’єднання громадян, інші особи, які провадять діяльність та/або надають послуги, пов’язані з національними інформаційними ресурсами, електронними

інформаційними послугами, здійсненням електронних транзакцій, електронними комунікаціями, захистом інформації та кіберзахистом [68].

Другий блок включає, знову ж таки, як органи загального характеру (місцеві державні адміністрації, органи місцевого самоврядування), так і органи спеціальної компетенції. Водночас, як йдеться у новій Стратегії кібербезпеки України, затвердженій Указом Президента України від 26.08.2021 р. За результатами експертних оцінок стан виконання Стратегії кібербезпеки України, схваленої Указом Президента України 15.03.2016 р., [86] за вказаними показниками не перевищує 40%. Невирішеними залишаються питання оперативного обміну інформацією про кіберзагрози, дієвої системи підготовки персоналу, ефективної моделі державно-приватного партнерства. Організація та проведення наукових досліджень у сфері кібербезпеки є недостатніми.

Про важливість державних програмних документів у сфері ІБ можна говорити, посилаючись на інший акт глави держави – Стратегію ІБ (далі – Стратегія), затверджену Указом Президента України від 28.12.2021 р. [85]. Стратегія, хоч і не є законодавчим актом, але, на відміну від деяких програмних документів, містить своєрідний блок визначення термінів. Таким чином, він визначає ІБ як невід'ємну частину національної безпеки України, стан захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу, інших життєво важливих інтересів людини, суспільства і держави, в якому права та свободи особи щодо збору, зберігання, використання та поширення інформації, доступ до достовірної та об'єктивної інформації, діє ефективна система захисту та протидії шкоді, заподіяній поширенням негативних інформаційних впливів, у тому числі скоординованим поширенням неправдивої інформації, деструктивної реклами, інші інформаційні операції, несанкціоноване розповсюдження, використання та порушення цілісності інформації з обмеженим доступом [85].

Тому зазначене визначення є ширшим, на відміну, наприклад, від визначення кібербезпеки, наданого у Стратегії кібербезпеки, оскільки додатково наголошує на забезпеченні основних прав людини на інформацію, проголошених Основним Законом – Конституцією України (ст. 31, 32) та міжнародні акти з прав людини.

Крім того, Стратегія містить, хоч і не прямим переліком, суб'єктів забезпечення ІБ, але визначає механізм реалізації мети та визначених завдань Стратегії, який включає значну кількість суб'єктів із визначенням їх відповідних функцій та компетенцій, які, на нашу думку, слід розглянути детальніше.

1. Рада національної безпеки і оборони України (РНБО). Відповідно до Конституції України (ст. 107) та в порядку, встановленому законом [70] координує діяльність органів виконавчої влади із забезпечення національної безпеки у сфері інформації, зокрема з використанням можливостей Центру протидії дезінформації. Крім нормативної діяльності, як-от розроблення та затвердження програмних документів у сфері інформатизації (доктрини, стратегії), РНБО здійснює також заходи цілеспрямованого індивідуального характеру з метою виявлення та своєчасної нейтралізації інформаційних загроз для України.

Так, відповідно до Закону України «Про санкції» санкції можуть бути застосовані Україною щодо іноземної держави, іноземної юридичної особи, юридичної особи, яка перебуває під контролем іноземної юридичної особи, або фізичної особи, яка не є юридичною особою. фізичні особи-резиденти, іноземці, особи без громадянства, а також суб'єкти, які здійснюють терористичну діяльність. Рішення про застосування, скасування та внесення змін до санкцій приймається РНБО України, вводиться в дію указом Президента України та затверджується протягом 48 годин з дня видання указу Президента України. України постановою ВРУ. Відповідне рішення набирає чинності з моменту прийняття постанови ВРУ та є обов'язковим до виконання [74].

З 2015 р. РНБО прийняла понад 50 рішень про застосування персональних спеціальних економічних заходів та інших обмежувальних заходів (санкцій) до фізичних та юридичних осіб, діяльність яких становить небезпеку для України, зокрема в інформаційній сфері, з метою виконувати зазначений закон. Так, рішенням РНБО від 02.02.2021 р. застосовано обмежувальні заходи (санкції) до юридичних осіб: ТОВ «Аріадна ТВ», ТОВ «Новий Формат ТВ», ТОВ «ТВ Вибір», ТОВ «Телерадіокомпанія «112-ТВ», ТОВ «Лідер ТВ», ТОВ «Партнер ТВ», «Новини 24 години», ТОВ «Нові комунікації»; рішенням РНБО від 16.02.2022 р. застосовано обмежувальні заходи до 16 фізичних та юридичних осіб, зокрема щодо Шарія А. та ІА «Шарій.нет» [71, 73]

Таким чином, РНБО оперативніше реагує на інформаційні загрози Україні за свої рішення, застосовуючи заборонні та обмежувальні санкції, обходячи при цьому звернення до суду, оскільки передбачено повноваження іншого конституційного органу – Національної ради України з питань телебачення і радіомовлення, про діяльність якої йтиметься далі.

2. Кабінет Міністрів України (КМУ) – реалізує державну політику у сфері комп’ютеризації, сприяє створенню єдиного інформаційного простору на території України [62]; забезпечує формування та реалізує інформаційну політику держави, забезпечує суверенітет інформації, фінансування програм, пов’язаних із забезпеченням ІБ, спрямовує та координує роботу міністерств та інших органів виконавчої влади у цій сфері. КМУ розробляє та затверджує план заходів щодо реалізації Стратегії, на підставі якого відповідні органи виконавчої влади здійснюють заходи щодо забезпечення ІБ. Органи державної влади у взаємодії з органами місцевого самоврядування, Центром протидії дезінформації та інститутами громадянського суспільства забезпечують реалізацію Стратегії відповідно до плану заходів, затвердженого КМУ.

3. Центральний орган виконавчої влади, що забезпечує формування та реалізує державну політику в інформаційній сфері:

- здійснює нормативно-правове регулювання у сфері ІБ України в межах своєї компетенції;

- визначає перспективи та пріоритетні напрями розвитку у сфері ІБ України;

- спільно з МЗС України сприяє популяризації та формуванню позитивного іміджу України на світових інформаційних ресурсах та національних інформаційних ресурсах іноземних держав з метою захисту їх політичних, економічних та соціально-культурних інтересів, зміцнення національної безпеки та відновлення територіальної цілісності України.

Нині таким органом є Міністерство культури та інформаційної політики України (МКІП), утворене у 2019 р. в результаті злиття Міністерства культури та мистецтв України з Міністерством інформаційної політики України, створеним у 2014 р. У відповідному положенні зазначено, що МКІП є головним органом системи центральних органів виконавчої влади, що забезпечує формування та реалізує державну політику у сферах культури, державної мовної політики, популяризації України у світі, інформаційного суверенітету України (в частині повноважень щодо управління комплексами, що належать державній компанії «Українська іноземномовна мультимедійна платформа» та Національного інформаційного агентства України «Укрінформ») та ІБ, а також забезпечення формування та реалізація державної політики у сферах відновлення та збереження національної пам'яті, міжнаціональних відносин, релігії та захисту прав громадян-національних меншин в Україні, мистецтво, охорона культурної спадщини, музейна справа, вивезення, ввезення та повернення культурних цінностей [58].

Ще одним центральним органом виконавчої влади, але вже зі спеціальним статусом, діяльність якого координується КМУ через Міністра культури та інформаційної політики є Державний комітет телебачення і радіомовлення України (Держкомісія з питань телебачення і радіомовлення). Цей орган за дорученням Міністра культури та інформаційної політики за

участю інших державних органів виконує завдання, зокрема, щодо забезпечення ІБ, вживає заходів щодо підвищення художньої якості національних телерадіопрограм, захисту суспільства від негативного впливу аудіо- та відеопродукції, що становить загрозу суспільній моралі [57]. Серед пріоритетних завдань цього органу на 2022 рік виділяються впровадження заходів медіаграмотності та заходів боротьби з дезінформацією, недопущення потрапляння на український ринок іноземної редакційної продукції антиукраїнського змісту [60].

4. Міністерство оборони України, а також сили оборони в межах своєї компетенції забезпечують:

- моніторинг інформаційного простору, прогнозування та виявлення інформаційних загроз національній безпеці держави у воєнній сфері;

- підготовка та здійснення інформаційних заходів з питань захисту держави, координація діяльності з питань національної безпеки держави;

– розвиток та функціонування системи стратегічного зв'язку сил оборони;

- здійснення правових, організаційних, технічних, інформаційних та інших заходів щодо забезпечення самої безпеки інформації, у тому числі захисту єдиного інформаційного середовища Сил оборони, зокрема в місцях дислокації, дислокації та застосування угруповань, військових частин і підрозділів. Збройних Сил України, інших утворених відповідно до законів України військових формувань;

- взаємовідносини з українськими та іноземними ЗМІ щодо висвітлення ситуації в районах здійснення заходів із забезпечення національної безпеки і оборони, відсічі та стримування збройної агресії російської федерації;

- протидія розвідувальним та іншим заходам інформаційного впливу, спрямованим проти Збройних Сил України (ЗСУ) та інших утворених відповідно до законів України військових формувань;

- доведення достовірної інформації до військовослужбовців ЗСУ, інших складових Сил оборони.

Готовність оборони держави в мирний час включає, зокрема: проведення розвідувальної діяльності та аналізу інформації в інтересах готовності оборони держави; захист інформаційного простору України та її входження у світовий інформаційний простір, створення розвиненої інфраструктури в інформаційній сфері. Відсіч збройній агресії проти України передбачає на підставі відповідного рішення Президента України ведення ЗСУ спільно з іншими військовими формуваннями бойових дій, у тому числі проведення спеціальних операцій (розвідувальних, інформаційних та психологічні та ін.) у кіберпросторі [66].

5. Служба безпеки України в межах своєї компетенції здійснює:

- моніторинг спеціальними методами і засобами вітчизняних і зарубіжних ЗМІ та мережі Інтернет з метою виявлення загроз національній безпеці України в інформаційній сфері;

- для боротьби з проведенням спеціальних розвідувальних операцій проти України, спрямованих на підрив конституційного ладу, порушення суверенітету та територіальної цілісності України, загострення суспільно-політичної та соціально-економічної ситуації.

6. Розвідувальні органи України під час здійснення розвідувальної діяльності сприяють реалізації та захисту національних інтересів України у сфері інформатизації за кордоном, виявленню та протидії зовнішнім інформаційним загрозам у сфері безпеки і оборони держави.

7. Національна рада України з питань телебачення і радіомовлення (далі – Нацрада), відповідно до компетенції, бере участь у забезпеченні захисту українського інформаційного простору від пропагандистської аудіовізуальної продукції держави-агресора, сприянні розповсюдженню українського телерадіомовлення на тимчасово окупованих територіях України. Основними повноваженнями, відповідно до закону, є контроль і нагляд за дотриманням законодавства у сфері телерадіомовлення, його ліцензування та державна реєстрація телерадіоорганізацій та постачальників програмних послуг [64]. Стосовно санкцій, які застосовує Нацрада, то

спеціальний закон відсилає до іншого профільного закону, в якому деякі санкції за порушення законодавства про телебачення і радіомовлення застосовуються за рішенням суду або за рішенням Нацради. Вона може застосувати до телерадіоорганізацій та провайдерів програмних послуг такі санкції: оголошення попередження; стягнення штрафу; анулювання ліцензії на підставі рішення суду за позовом Національної ради. При цьому рішення про оголошення попередження приймається в першу чергу через порушення законодавства чи умов ліцензії телерадіоорганізацією або з першим порушенням законодавства провайдером програмної послуги [76]. Як випливає з зазначеного, ступеневий порядок застосування зазначених інформаційно-правових санкцій є важливою гарантією дотримання свободи слова як ключового принципу демократичної, правової держави.

До реалізації Стратегії відповідними державними органами можуть залучатися наукові та науково-дослідні установи, які забезпечують науково-аналітичне та експертне супроводження процесу формування та реалізації державної інформаційної політики.

З урахуванням викладеного можна констатувати, що наведений перелік суб'єктів (державних) забезпечення ІБ буде неповним, якщо не спрямувати їхню діяльність на взаємодію з інститутами громадянського суспільства, зокрема незалежними спілками журналістів та інших творчих працівників медійної сфери, які як ніхто інший найбільше зацікавлені у прозорості та виваженості державної інформаційної політики зі створенням рівних умов для діяльності в цій сфері.

Більше того, нинішній стан інформаційної політики в умовах воєнної агресії рф щодо України вимагає нових, нестандартних підходів до налагодження співпраці з військовими адміністраціями в регіонах, складовою чого також є ІБ.

Формування цілісної системи забезпечення ІБ вимагає багато людських, фахових та матеріально-технічних ресурсів, зокрема для здійснення цілеспрямованої зовнішньої інформаційної політики, чим, на

жаль, не володіє ще достатньо Україна, на відміну від держави-агресора, яка роками вибудовувала одночасно з озброєнням свою пропагандистську імперію, в т. ч. за кордоном.

РОЗДІЛ 2
ПРАКТИЧНІ АСПЕКТИ СУЧАСНОЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

2.1. Ризики інформаційної безпеки в контексті російсько-української війни

Нова європейська реальність змушує знову і знову звертатися до питання безпеки. Сьогодні майже всі іноземні аналітики в один голос стверджують, що Україна виграла інформаційну складову війни, залишилася лише фізична війна.

Для іноземних аналітиків головним фактором перемоги над російською пропагандою є високий рівень мобілізації українського населення у віртуальному просторі: реальні фото з війни, волонтерство, яке об'єднало знаменитостей, блогерів, простих громадян, інтелектуалів, політиків, злагоджені дії кіберполіції, кіберхакерів, політичні виступи президента, чоловіки, які повернулися в Україну, щоб приєднатися до ТРО чи ЗСУ, жінки, які намагалися захистити життя своїх дітей. Усі ці дії, безумовно, сформували позитивний імідж України, а також дуже вплинули на те, що Європа скасовує російські наративи та прислухається до українських.

Проте ще до повномасштабного вторгнення відбулося «розгойдування» емоційно-психологічного стану українців. Протягом перших двох місяців Україна постійно зазнавала кібератак з боку російської федерації: численні фейки, пропаганда, дезінформація, витоки інформації, атаки на офіційні сторінки різних державних відомств України, псевдомінери шкіл, супермаркетів, повідомлення про можливу широкомасштабну російську інтервенцію на територію України.

Усе це мало ознаки стратегічних інформаційно-психологічних спеціальних операцій (далі – ІПСО), метою яких було дестабілізувати та дезорієнтувати українське суспільство, посіяти ворожнечу, паніку та змусити країну піти на поступки російській федерації. Адже в уявленнях агресора

частина українців повинна була радісно зустріти «визволителів», а інша – здатися через страх перед «другою світовою армією». Найактуальнішими прикладами пропаганди були створені проросійськими активістами та бойовиками псевдореспубліки «ЛДНР» відеофрагменти та «прес-релізи» про вибухи, здійснені ЗСУ, в той час, коли ці повідомлення мали всі ознаки добре режисованого сценарію. Основною метою цих фейкових відео є просування образу ворога, посилення почуття страху, незахищеності, а також посилення паніки громадян, які проживають на території «ЛДНР» та навколишніх територій, підконтрольних Збройними Силами України.

У період з 19 лютого терористи «евакуювали» громадян України, які проживають на окупованих територіях України, від неіснуючих обстрілів ЗСУ, проводили мобілізацію неповнолітніх та відкрито розповсюджували агітаційні листівки на кшталт «Вступай до народного ополчення. Батьківщина-мати кличе вас! Республіка потребує вас». Людей викрадають, а звірства в Бучі називають «живими трупами». Проте масштабне вторгнення не тільки продемонструвало, що українці мають достатньо високий рівень емоційної стійкості (всенародний страх виконує мобілізуючу функцію, що остаточно було доведено під час Революції Гідності 2014 р.), але й принципово розвінчало міфи про «можемо повторити» і «другу світову армію».

Розглядаючи пропаганду, як інструмент впливу на суспільну свідомість, варто підкреслити дві особливості: з одного боку, вона має досить давню історію, і сьогодні ми бачимо численні повідомлення про те, що «російська пропаганда неефективна» або «російська пропаганда досить примітивно» і фактично ці наративи розслаблюють і призупиняють українську боротьбу в інформаційному просторі, тому недооцінювати російські методи «управління масами» не варто. Адже населення рф за офіційними даними досягає 142,42 мільйонів осіб, більшість з яких абсолютно не знають про все, що зараз відбувається на території України, і не намагаються зупинити своє політичне керівництво від спроби повністю

знищити Україну, більше того, активно беруть участь у просуванні наративів про «спорт поза політикою», «культура поза політикою», «церква Московського патріархату поза політикою» тощо.

Будучи інструментом політичної маніпуляції, пропаганда спеціально спрямована на мотиваційну та емоційно чутливу внутрішню сферу особистості. Інформаційне суспільство та поява соціальних мереж, а також друку, радіо і телебачення в певний час сприяють тому, що пропагандистська інформація, будучи стратегічно важливим елементом спеціальних психологічних операцій, поширюється надзвичайно швидко. Пропагандистська інформація здатна, по суті, сконструювати нову політичну реальність.

Теза Путіна про те, що росія проводить превентивну «військову операцію» проти України, тому що Україна, за його словами, відкрито готувалася до нової «каральної операції на Донбасі» та «вторгнення» на російські «історичні території», особливо в Крим, насправді може бути досить успішною. І підтвердженням цього є приєднані території Донецької та Луганської областей, а також Крим, який росія спочатку вважає своєю територією, але ця територія ніколи не була російською, хіба що в періоди окупації. Водночас у тезах сьогоднішніх світових лідерів ми часто чуємо, що сьогоднішньої війни не було б, якби в 2014 р. вірили Україні, а не наративам Путіна про «громадянську війну на Донбасі», «українську хунту», «розіп'яті хлопці» тощо. Проте у 2014 р. Україна, відверто кажучи, не була готова ні до збройного, ні до інформаційного протистояння.

За останні вісім років в українському суспільстві відбулися досить значні зміни щодо готовності протистояти витокам і дезінформації. Численні фактчекінгові проекти, навчання медіаграмотності, запровадження відповідних курсів у системі освіти на різних рівнях та розвиток критичного мислення підвищили здатність розрізняти фейки та споживати інформацію виключно з перевірених та офіційних джерел. Власне, такої кількості

свідомих громадян було достатньо, щоб зберегти інформаційний захист від російської пропаганди і навіть перемогти в інформаційній війні.

Під поняттям інформаційної війни розуміють дії з метою отримання інформаційної переваги над супротивником, за допомогою процесів обробки персональних даних, використання інформаційних систем і комп'ютерних мереж. У нашому розумінні інформаційна війна – це навмисні злочинні дії, метою яких є дезінформація, деморалізація та побудова «тихої покори населення», що здійснюються державою-агресором за допомогою хакерських атак, злому внутрішньої життєдіяльності, забезпечення та обороноздатності, дискредитація політичного керівництва та збройних сил, проведення спеціальних стратегічних інформаційних, кризових, бойових і психологічних операцій на території держави, яка стала об'єктом інформаційної чи гібридної агресії.

В контексті інформаційної війни виділяють три рівні її функціонування: індивідуальний, груповий і глобальний. В українських реаліях ми пропонуємо виділяти чотири рівні: індивідуальний, територіальний (регіональний), національний та глобальний. Ми можемо окреслити кожен із цих рівнів так, що російська пропаганда, поширюючи певні наративи, підходить до них окремо, формуючи та змінюючи чітко встановлені норми залежно від ситуації.

Індивідуальний рівень сприйняття пропаганди більше залежить від особистісних характеристик особистості. Те, що лякає одних громадян і змушує покинути домівку, інших мобілізує. Розвиток інформаційного суспільства сприяє тому, що атомізованій особистості досить часто доводиться боротися за свою ідентичність. Соціальні медіа та популяризація почуття самотності у сучасної людини призводять до того, що вона все більше сприймає політичну реальність крізь призму власного его, інтерпретуючи себе як нерелігійну чи аполітичну людину. Дотримуючись уявлень про те, що певний тип людини, демократичний чи масовий, створюється самим суспільством, можна припустити, що байдуже ставлення

до політики є скоріше наслідком насиченості інформацією світу, ніж причиною спалахів конфліктів. В українському суспільстві це також можна вважати наслідком тривалого споживання пропагандистських наративів: «від політики», «політика – це брудно», «політики завжди крадуть», «бариги», «олігархи заробляють на війні» і так далі. Наслідки: бажання залишитися осторонь, байдуже або занадто радикальне ставлення до політичних реалій. Тому російська пропаганда на індивідуальному рівні здатна розмивати ідентичність, формувати відчуття відчуженості, мозаїчності, самотності тощо.

На територіальному рівні інформаційної війни російська пропаганда апелює до колективних, особливо етнічних, ідентичностей. Оскільки українське суспільство є полікультурним і включає багато етнічних груп, російська пропаганда апелює до тієї його частини, яка характеризується найбільш лояльним ставленням і довірою до росії та російської культури, яка сформувалася під впливом багатьох факторів: родинних зв'язків, використання поширених російськомовних практик у суспільному житті, домінування російської символіки (пам'ятники, топонімічні назви тощо), перегляд переважно російських ЗМІ (російською мовою), зрештою, проживання на території, що межує з агресором, і пряме спілкування з громадянами російської федерації.

Саме через високий рівень залученості до російської культури та побутових практик ця категорія населення вкрай негативно реагує на будь-які зміни нормативно-правових актів щодо заборони російської музики, мовлення, навчання в школах, перейменування вулиць, населених пунктів тощо. Ці фактори лягли в основу позитивного сприйняття пропагандистських наративів Кремля, які завжди базувалися на історичних міфах про «єдиний народ», «ми брати», «українська влада про нас не думає», «поганих бандерівців», «добрих росіян». Сьогодні російська пропаганда продовжує «тримати» такі етнічні групи в повній дезінформації. Відомо, що коли

російські війська заходять в окуповані міста та села, вони одразу починають встановлювати «свої порядки».

Отже, з перших хвилин масштабного втручання надзвичайно важливою була мобілізація українців в інформаційному полі, що дозволило значною мірою утримувати громадян та нівелювати панічні стани саме за рахунок скорочення повідомлень про гіпотетичні вибухи, погрози застосування хімічної зброї тощо. Велике значення мала й українська контрпропаганда, яка запускала інформацію про «привида Києва», «героїв острова Зміїного», «збитий консервною банкою ворожий безпілотник». Такі наративи сприяли формуванню почуття спільності та мобілізували населення на масову волонтерську допомогу.

Прикладом глобального рівня сприйняття пропаганди є спроба Путіна, його уряду, а також російських державних ЗМІ прирівняти Україну до «неонацистів». Однак ця заява не витримує навіть найпростішої перевірки фактів, оскільки в Україні немає ні тоталітарної системи, ні навіть представників ультраправих сил у парламенті. Спроби дискредитувати Україну в очах Заходу рф зашифровує в наративах про «появу трупів у Бучі після того, як російські війська залишили місто», називаючи вбивства та зображення трупів змонтованими. Те ж саме стосується відео з розбомбленого пологового будинку в Маріуполі, яке російська пропаганда назвала «постановочним відео Зеленського». У глобальному масштабі російська пропаганда неефективна, але це не означає, що її поширення перестало становити ризик для України.

У той час як Захід відкидає російські наративи, інші впливові політичні гравці прислухаються до них і приймають їх. Зокрема, це стосується Китаю, американських прихильників теорії змови, глобального Півдня, який неохоче засуджує Росію за війну та практично не протидіє її дезінформації. Сорок країн не підтримали позачергову резолюцію Генасамблеї ООН із засудженням вторгнення Росії в Україну. Білорусь, Еритрея, Північна Корея та Сирія вирішили підтримати Росію. Серед 35 тих, хто утримався були

Китай, Іран, Індія, Ірак, Пакстан, Південна Африка, Південний Судан та В'єтнам – держави, які на той час мали підтримку з боку США, мали партнерські відносини або поглибили відносини з ними в останні роки. Отже, російська дезінформація та гібридна війна, яку росія веде проти України, матиме серйозні наслідки для міжнародних відносин ще досить тривалий час після її завершення. Водночас варто підкреслити, що пропагандистський вплив, реалізація на глобальному рівні несе відповідні ризики, зокрема, можливість втрати репутаційного капіталу держави.

2.2. Функції забезпечення інформаційної безпеки в Україні в умовах повномасштабної збройної агресії російської федерації

Збройна агресія рф в повному обсязі поставила перед суб'єктами ІБ України нагальні завдання щодо захисту інформаційного суверенітету, зниження деструктивного вплив наративів, які ворог активно використовує для дестабілізації функціонуючих органів державного управління та морально-психологічного стану населення тимчасово окупованих територій. Ці завдання є актуальними, і відкладення їх вирішення на інший, більш сприятливий час, як свідчить восьмирічний досвід протидії збройній агресії російської федерації, лише посилює та ускладнює наявні проблеми.

На жаль, відсутність системності та комплексності у сфері ІБ не дозволяє побудувати ефективну систему протидії деструктивним інформаційним впливам противника. Безперечно, сьогодні можна констатувати певні досягнення на шляху подолання інформаційних ризиків, хоча вони радше залежать від активної роботи окремих органів державного управління – Офісу Президента України, прес-служби ЗСУ, Міністерство оборони України, Служба безпеки України та окремих представників органів місцевого самоврядування. Проте на національному рівні досі немає єдиної

стратегії забезпечення ІБ в умовах повномасштабної російської збройної агресії.

Відносини у сфері забезпечення ІБ органів державного управління мають публічно-правовий характер, оскільки стосуються здійснення державою функцій з метою захисту інформаційного суверенітету, забезпечення інформаційних прав і свобод учасників правовідносин.

Забезпечення ІБ є функцією держави, оскільки цій правовій категорії притаманні такі змістові характеристики, які є іманентними характеристиками поняття функції держави: це об’єктивні, найбільш важливі напрямки діяльності; соціальне призначення держави в суспільстві розкривається через поняття функції; через поняття функції конкретизуються завдання держави та її призначення; функції держави здійснюються не одноосібно, а за допомогою державних органів, громадян та інших суб'єктів практичної діяльності [77, с. 13]. Слід зазначити, що функції держави та функції забезпечення ІБ не можна ототожнювати, оскільки коло суб’єктів, які забезпечують ІБ, є значно ширшим і включає велику кількість недержавних (неурядових) суб’єктів, від органів місцевого самоврядування до інститутів громадянського суспільства.

Термін «функція» в загальному розумінні визначається як основний напрямок, сфера діяльності, характерна властивість, притаманна певному предмету чи явищу, його головна ознака, яка служить метою і сенсом його існування. Функцію можна розглядати з точки зору наслідків (сприятливих, несприятливих – дисфункціональних або нейтральних афункціональних). Отже, поняття «функція» і «функціонування» нерозривно пов’язані між собою і, якщо функція є характеристикою об’єкта в певний момент часу, в умовній статиці, визначеній інтервалом часу, то функціонування є динамічною характеристикою об’єкта.

Отже, функції забезпечення ІБ публічної адміністрації в Україні – це методи, притаманні діяльності публічних адміністрацій щодо збереження власної працездатності в умовах деструктивних інформаційних впливів та

запобігання небезпеці щодо інформаційних прав та інтересів людей, громадянського суспільства, органів влади, підприємств, установ та організацій, а також держави в цілому.

Можна виділити такі етапи реалізації функцій забезпечення ІБ:

- фаза констатації та узагальнення призначена для виявлення існуючих інформаційних загроз, накопичення інформації про них та виявлення спільних рис. Цей етап дає змогу перейти від трансцендентального сприйняття інформаційних загроз до їх аналізу на основі підтверджених фактів заподіяння або спроби заподіяння шкоди інформаційним правовідносинам;

- етап аналізу дозволяє виявити та структурувати закономірності, характерні для об’єкта, скласти ієрархію найбільш значущих з них, виявити періодичність, джерело, форми розповсюдження найбільш значущих інформаційних загроз, їх призначення, спрямованість та характеристики керованості;

- фаза моделювання дає змогу визначити найбільш вразливі точки інформаційної діяльності противника щодо виробництва інформаційних загроз та підготувати оптимальні засоби і способи її ліквідації або ослаблення (зниження ефективності);

- фаза нормативного закріплення передбачає прийняття управлінського рішення про включення до поточних завдань і комплексу оперативних дій органів державної влади та інших суб’єктів забезпечення ІБ оптимальних методів і засобів припинення інформаційної активності противника, а також закріплення зазначеного рішення у відповідних нормативно-правових актах;

- фаза практичної реалізації функцій забезпечення ІБ державного управління включає безпосереднє виконання завдань, дій та засобів для подолання інформаційних ризиків і загроз, визначених нормативно-правовими актами;

- фаза рефлексії та оцінки дозволяє визначити результативність діяльності на попередніх етапах і скорегувати майбутню діяльність у сфері ІБ з метою підвищення її ефективності.

Зазначені етапи, як правило, проводяться послідовно, проте не можна не згадати про випадки, коли через недоліки в організації та плануванні або через дефіцит часу, спричинений підвищеною небезпекою певної інформаційної загрози, окремі етапи можуть бути пропущені. На нашу думку, це сприяє посиленню хаосу у функціонуванні системи ІБ.

Функції забезпечення ІБ можна класифікувати за різними критеріями, але вважаємо, що доцільніше класифікувати їх за критерієм ефективності.

Функція збереження інформаційного суверенітету – здатність системи державного управління керувати процесами зовнішніх інформаційних впливів, протистояти деструктивним інформаційним способам завдання шкоди національній безпеці держави та інтересам громадянського суспільства.

Функція інформування міжнародної спільноти про порушення ворогом законів і звичаїв війни, заподіяння шкоди здоров'ю, життю та майну цивільного населення передбачає запобігання руйнівному впливу фальсифікацій та інших способів спотворення об'єктивної інформації про поведінку. бойових дій та поводження з цивільним населенням. Таке передбачення досягається завдяки активній роботі публічних адміністрацій щодо оприлюднення фактів, що характеризують ворожі дії, для широкої міжнародної аудиторії.

Функція виховання високого рівня інформаційної культури вимагає створення органами публічного управління умов для найповнішого оволодіння їх кадрами, а також широкими верствами громадян знаннями, уміннями та навичками, що перешкоджають системі публічного управління та суспільство від уразливості до ворожих інформаційних атак, у тому числі кібератак. В умовах повної збройної агресії рф така неможливість уразливості є однією зі складових кіберзахисту – комплексу політичних,

економічних, соціальних, військових, наукових, науково-технічних, інформаційних, правових, організаційних та інших заходів, які реалізуються в кіберпросторі та спрямовані на забезпечення захисту суверенітету та обороноздатності держави, запобігання збройним конфліктам та відсіч збройній агресії.

Функція консолідації є фокусом зусиль публічних адміністрацій щодо створення національного консенсусу, що передбачає об’єднання різних суб’єктів ІБ на основі усвідомлення спільної мети, толерантності та взаємоповаги. З цього приводу хотілося б зробити деякі зауваження щодо розуміння сутності такої взаємодії в правовій демократичній державі. Деякі дослідники вважають, що людина, громадянин і демократичне суспільство в цілому зобов'язані дотримуватися уявлень держави про силу, спрямованість і періодичність її громадянської активності в інформаційній сфері. Інакше кажучи, держава формулює цілі та методи дій, а громадяни зобов'язані докладати максимум зусиль для досягнення цих цілей безоплатно та беззастережно.

Наприклад, в сучасних умовах інститути громадянського суспільства є повноправними учасниками процесу забезпечення ІБ України. Як показує суспільно-політична практика, для ефективної протидії інформаційним загрозам зусиль держави зазвичай недостатньо. Це, у свою чергу, змушує вище державне керівництво до діалогу з інститутами громадянського суспільства, які виступають надійними союзниками держави. Водночас у взаємодії громадянського суспільства та держави в Україні існує ряд проблемних питань. Йдеться насамперед про наявність скептичних настроїв серед населення щодо можливості реального впливу на прийняття політичних рішень у секторі безпеки; недосконалість інституційної основи; відсутність досвіду взаємодії громадянського суспільства та держави в умовах інформаційної війни; недосконалість українського законодавства.

Основними шляхами вирішення цих проблем є ефективна інформаційна політика держави та громадського сектору в напрямку

формування активістського типу політичної культури українського суспільства, а також удосконалення інституційно-правової бази. Виходячи із зазначених проблем, ефективність механізмів залучення громадянського суспільства до політики безпеки в інформаційній сфері ще далека від оптимальної. Особи, соціальні групи та українське суспільство в цілому мають формувати активістський тип політичної культури та максимально використовувати всі доступні засоби впливу на прийняття політичних рішень у секторі безпеки. Застосування терміну «повинен» до людини і громадського суспільства в контексті становлення їх громадської активності видається нам некоректним і типовим для ідеології тоталітарної держави. Особи та громадяни, окремі інститути громадянського суспільства здійснюють свою діяльність у цей момент і у спосіб, який вони вважають за потрібне (якщо така діяльність не порушує правових норм). Примус до громадської активності в демократичному суспільстві неприпустимий, а тому суть консолідаційної функції полягає в зборі інформації про позиції недержавних суб'єктів у забезпеченні ІБ та пошуку спільних основ для сумісної з ними діяльності. Крім того, зазначаємо, що в умовах правового режиму надзвичайного стану відбувається обмеження деяких прав і свобод людини і громадянина, у тому числі в ІТ-сфері, яке, безумовно, може здійснюватися лише на основі Конституції та законів України. Такі обмеження слід враховувати при побудові концепції консолідації громадянського суспільства та державного управління у сфері ІБ.

Виходячи з вищевикладеного, можна зробити висновок, що функції забезпечення ІБ державного управління є одними з пріоритетних серед інших функцій забезпечення національної безпеки. Відмінність у реалізації зазначених функцій в умовах повної збройної агресії російської федерації полягає в тому, що сьогодні в основному використовується кінетична зброя. Проте здатність України ефективно протистояти російській агресії значною мірою залежить від уміння та успішного виконання функції інформування міжнародної спільноти про порушення противником законів та звичаїв війни,

заподіяння шкоди здоров’ю, життю та майну цивільного населення. Крім того, зберігається фактична функція підвищення високого рівня ІТ-культури, що унеможливлює деструктивний вплив ворога на життєдіяльність держави та громадянського суспільства.

РОЗДІЛ 3
ПЕРСПЕКТИВИ УДОСКОНАЛЕННЯ СУЧАСНОЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УКРАЇНІ

3.1. Пріоритети підвищення інформаційної безпеки України

Фактором, який послаблює здатність держави нейтралізувати загрози, є посилення взаємозалежності країн та їх відкритості зовнішнім впливам. Держава здебільшого перестає бути монополістом на своїй території, її інформаційна політика все більше обмежується, видозмінюється, нівелюється діями інших держав, міжнародних та неурядових організацій, неформальних об'єднань негативної спрямованості, кримінальних угруповань тощо. Ідеологічно, інституційно та економічно слабка держава не може скористатися технологічними, економічними та соціокультурними перевагами глобалізації, але активно переймає її негативні риси.

Розвиток глобальних процесів на основі комплексної інформатизації породжує широкий спектр інформаційних загроз – від витіснення вітчизняної продукції більш конкурентоспроможною на внутрішньому інформаційному ринку до ведення цілеспрямованих інформаційних війн. Згідно зі звітом Національної розвідувальної ради США, інформаційна війна стане домінуючим фактором поточного століття. Вони відбуватимуться на всіх рівнях соціальної структури людства, в тому числі між блоками держав. Сучасна інформаційна революція відбувається на тлі інформаційних війн, головною метою яких є підрив національної безпеки держав. З урахуванням таких підходів охоронно-інформаційна функція держави набуває особливого значення в усіх регіонах світу.

Сучасна ситуація у світовому інформаційному просторі зумовлена таким: більшість країн світу зіткнулися з проблемами кібертероризму, комп'ютерної злочинності та іншими проблемами ІБ; в останні десятиліття спостерігається тенденція до поширення інформаційної агресії та насильства;

поширюється агресивна реклама, намагаються маніпулювати свідомістю людини, регулярно проводяться інформаційно-психологічні операції; майже 120 країн світу (за оцінками американських експертів) розробляють інформаційну зброю або її елементи (для порівняння, зброя масового ураження розробляється приблизно в 20 країнах); наслідки застосування сучасної інформаційної зброї (за висновками науковців та експертів європейських країн, України та США) можна порівняти із застосуванням зброї масового ураження; новітні виклики та загрози в інформаційній сфері створюють реальну загрозу безпеці людини та міжнародному правопорядку.

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

- недосконалість державної політики у сфері ІБ України;
- відсутній стратегічний рівень забезпечення ІБ;
- недостатній рівень інформаційного забезпечення зовнішньої та внутрішньої політики України;
- відомча автономність державних органів та установ, на які покладено забезпечення ІБ України, дублювання їх повноважень та недостатня якість існуючої координаційної складової;
- відсутність ефективних механізмів експертної оцінки інформаційної продукції, поширення якої загрожує ІБ щодо прав людини, інтересів суспільства та держави;
- відсутність ефективних механізмів залучення державного та приватного секторів України до боротьби з негативними інформаційними впливами, міжнародної співпраці у цій сфері;
- наявність законодавчих та організаційних прогалин у сфері обігу інформації з обмеженим доступом.

Сучасні виклики ІБ України зумовлені водночас внутрішніми та зовнішніми чинниками: внутрішніми – найбільшою мірою пов’язаними з

відсталістю інформаційних технологій в Україні порівняно з провідними країнами світу, низьким рівнем інформатизації, розпорошення повноважень органів державної управління в інформаційній сфері; зовнішні – світові тенденції створення та застосування інформаційних технологій та намагання іноземних суб'єктів впливати на світовий та внутрішній інформаційний простір з метою забезпечення власних інтересів, залежність від іноземного програмного забезпечення.

Тому на сучасному етапі Україна має зосередитись на двох основних напрямках: зробити внутрішній український простір сучасним, повноцінно структурованим і конкурентоспроможним; забезпечити інформаційну присутність держави у світі та підтримати її позитивний імідж. Забезпечення національної безпеки здійснюється за умов пріоритетності національних інтересів, необхідності своєчасного вжиття заходів, що відповідають характеру та масштабам загроз цим інтересам, і ґрунтується на засадах правової демократичної держави. А оскільки ІБ є частиною національної безпеки, то національні інтереси в інформаційній сфері тут також мають бути пріоритетними.

Незважаючи на те, що виділяють дві складові забезпечення ІБ – активну і пасивну (розвиток і захист), в переважній більшості система працює проти загроз, тобто на пасивній складовій. Проте аналіз практики країн ЄС показує, що ІБ має базуватися на моделі стратегічного мислення: вжиття заходів для захисту цілей, їх підтримання та забезпечення безпеки на основі принципів демократії, прав людини та безпечного Інтернету.

ІБ також є невід'ємним напрямком побудови інформаційного суспільства, розвиток якого має відбуватися не лише через підвищення технологічних можливостей обміну інформацією, а й через її глибоке усвідомлення всіма суб'єктами інформаційних відносин. Внаслідок цього до проблем ІБ на цьому етапі починають додаватися питання інформаційної етики, забезпечення приватності в умовах інформаційного суспільства, захисту від маніпулятивних інформаційних впливів тощо.

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

- забезпечення інформаційного суверенітету України;

- удосконалення державного регулювання розвитку інформаційної сфери шляхом створення правових та економічних передумов для розвитку національної інформаційної інфраструктури та ресурсів, впровадження новітніх технологій у цій сфері, наповнення вітчизняного та світового інформаційного простору достовірною інформацією про Україну;

- активне залучення ЗМІ до запобігання та боротьби з корупцією, зловживанням владою та іншими явищами, що загрожують національній безпеці України;

- забезпечення неухильного дотримання конституційних прав на свободу вираження поглядів, доступ до інформації, захист персональних даних, недопущення незаконного втручання органів державної влади, органів місцевого самоврядування та їх представників у діяльність ЗМІ та журналістів, заборону цензури, дискримінація в інформаційній сфері та переслідування журналістів за політичні позиції, за виконання професійних обов'язків, за критику;

- вжиття комплексних заходів щодо захисту національного інформаційного простору та боротьби з монополізацією інформаційної сфери України.

Аналіз антиукраїнських дій в інформаційному просторі свідчить про те, що наголос слід робити на збереженні національної ідентичності та підтримці національної культури як основи не лише ІБ України, а й національної безпеки загалом. Захист інформаційного суверенітету України є одним із пріоритетних напрямів забезпечення національної безпеки. Проте законодавство не містить адекватного тлумачення зазначеного терміну, а також конкретних механізмів його надання. Наразі відсутній механізм ефективного та швидкого блокування (обмеження доступу) ресурсів із нелегальним контентом, особливо тих, що розміщені на технічних сайтах за

кордоном, а також правильного визначення шкідливого контенту. Крім того, відсутній механізм запобігання та запобігання поширенню інформаційної продукції антиукраїнського змісту шляхом визначення загальних критеріїв віднесення її до категорії забороненої до розповсюдження; визначення суб'єкта, який виконуватиме функцію експертної оцінки інформаційної продукції, що містить заклики до порушення конституційного ладу, територіальної цілісності, розпалювання війни, фашизму, національної та релігійної ворожнечі.

Поряд з поняттям «інформаційний суверенітет» широко використовується поняття «цифровий суверенітет», яке тісно пов'язане з поняттям «кібервійна», яка є продовженням війни з використанням інформаційно-комунікаційних систем, але з двома фундаментальними відмінності: не призводить до фронтального зіткнення між воюючими сторонами та безпосередніми жертвами. Враховуючи ряд важливих проблем, які перешкоджають створенню ефективної національної системи протидії загрозам у кіберпросторі, а саме: термінологічна невизначеність, недостатня координація діяльності відповідних відомств, залежність України від програмно-технічної продукції іноземного виробництва, проблеми з кадрового забезпечення відповідних структурних підрозділів є актуальним питанням побудови системи кібербезпеки.

Застарілість, складність системи захисту державної таємниці та службової інформації, створення умов для їх несанкціонованого поширення, переважний «паперовий характер» носіїв такої інформації ставить питання про необхідність узгодження інформаційного законодавства з так званих норм міжнародного права та правових актів ЄС, Ради Європи та НАТО, що передусім базується на невід'ємному праві на доступ до інформації. І в першу чергу саме держава має забезпечити якісний доступ усіх категорій громадян до інформації, яку вона виробляє, як до офіційних матеріалів, так і до роз'яснення змісту власної діяльності.

Крім того, аналіз законодавства розвинутих країн показує, що право на доступ до інформації трансформується в право на спілкування, яке включає не лише право на доступ до інформації, а й право брати участь у її створенні. Наприклад, замість того, щоб розумітися як «надіслана» від політичної організації чи державного органу громадянам, публічна інформація в Норвегії розглядається як спільно створена та використана разом з громадянами, а також групами громадян незалежно, у спосіб активних інноваційних практик відтворення різних типів доступної інформації, урядової чи іншої, у нові форми публічної інформації. При цьому доступ до «старої» публічної інформації має бути максимально відкритим, щоб можна було створювати та використовувати нову публічну інформацію без державного втручання, а «пересічного громадянина» слід вважати «розповсюджувачем публічної інформації».

Відтепер ідея публічності реалізується через використання соціальних медіа в процесі обміну інформацією, що стало якісно новим явищем у системі горизонтальних інформаційних зв'язків і створило принципово нову ситуацію в соціальній сфері суспільства, створення умов для організації віртуальних соціальних суб'єктів та їхнього зростання впливу на суспільне життя.

Тому пріоритетними напрямами вдосконалення ІБ є:

- вдосконалення правового забезпечення ІБ шляхом розробки її концептуальних засад;

- визначення або уточнення ролей, функції та повноваження суб'єктів забезпечення ІБ України;

- забезпечення інформаційного суверенітету України з метою запобігання інформаційній залежності та інформаційній експансії іншими державами чи міжнародними структурами;

- сприяння розвитку міжнародного співробітництва в інформаційній сфері за умов перегляду його принципів і механізмів;

- посилення міжнародно-правової відповідальність за застосування сил і засобів в інформаційних сферах, що негативно впливають або загрожують людині, суспільству і державі;

- посилення організаційних засад забезпечення ІБ: вирішення питання координації діяльності суб'єктів забезпечення ІБ, особливо у сфері протидії інформаційній агресії, забезпечення кібербезпеки України;

- створення системи державно-приватного партнерства у сфері забезпечення ІБ;

- запровадження системи демократичного контролю за діяльністю державних суб'єктів забезпечення ІБ;

- розвиток комунікаційної політики у відносинах «держава-суспільство».

Водночас необхідно розробити освітні програми дій, спрямовані на формування вмінь забезпечувати власну ІБ, особливо підвищення рівня культури користування засобами обробки інформації, оприлюднення власної інформації та методів її захисту, критичного доступу до інформації.

Для успішного входження нашої держави в міжнародні інформаційні обміни вона має зосередитись насамперед на таких напрямках у сфері правової діяльності:

- розробити систему нормативно-правових актів, спрямованих на якісне збереження національних інформаційних ресурсів, їх розвиток та ефективне використання в національних інтересах;

- здійснити необхідну адаптацію національного інформаційного законодавства до загальновизнаної міжнародно-правової бази з метою активізації своєї участі в обміні інформацією;

- активно брати участь у створенні міжнародного права, яке має оперативно регулювати нові явища у сфері комп'ютеризації;

- сформувати правову базу регулювання участі у міжнародній діяльності щодо забезпечення дотримання міжнародного інформаційного

законодавства, боротьби з кібертероризмом тощо, видами інформаційної злочинності.

3.2. Стратегічні напрями забезпечення інформаційної безпеки в сучасних умовах

Інформаційна політика провідних країн світу – це сукупність стратегічних вихідних положень діяльності компетентних органів публічної влади щодо планування та контролю процесів отримання, зберігання та розповсюдження інформації. Крім того, розвинуті країни наразі посилюють державну діяльність у напрямі законодавчої нормалізації відносин у державному інформаційному просторі. Для цього ці країни приймають спеціальні нормативно-правові акти щодо реалізації пріоритетних засад державної інформаційної політики.

В умовах сучасного глобального геополітичного протистояння актуальним питанням для України залишається захист вітчизняного інформаційного простору та забезпечення безпеки держави в інформаційній сфері, особливо в умовах поширення трансформаційних гібридних загроз, які поширюються переважно через державу-агресора. На цьому тлі затвердження Стратегії ІБ [85] на національному рівні 28.12.2021 р. є важливим та відповідальним кроком у напрямку визначення подальших перспектив розвитку вітчизняної інформаційної сфери.

Забезпечення ІБ в першу чергу передбачатиме чітке розуміння та побудову алгоритмів заходів зі стримування та запобігання реальним і потенційним загрозам, нейтралізації російської інформаційної агресії, у тому числі стримування можливих спеціальних інформаційних операцій держави-агресора, забезпечення інформаційної стабільності суспільства і держави, забезпечення ІБ та динамічний паритетний розвиток міжнародного співробітництва у сфері ІБ.

Необхідність прискорення визначення декларативних стратегічних засад забезпечення ІБ в сучасних реаліях викликана такими викликами, як: складна ситуація в національній інформаційній сфері, яка пов'язана як зі значним інформаційним впливом, так і з втручанням російських ЗМІ; масове поширення російськими ЗМІ дезінформації про Україну; виконання спеціального інформаційного завдання російської федерації з метою дискредитації та створення негативного міжнародного іміджу України у світі; технічні проблеми з трансляцією українських електронних ЗМІ в окремих регіонах нашої країни та світу.

Невипадково в положеннях Стратегії ІБ України, оприлюдненій у грудні 2021 р., проголошується теза про те, що інформаційна політика російської Федерації є загрозою не лише для України, а й для інших провідних демократичних країн світу. У такій ситуації актуальним і своєчасним є зазначення основних положень Стратегії ІБ України в рамках визначення ролі та завдань вітчизняної спецслужби у запобіганні загрозам і викликам у вітчизняному інформаційному просторі, забезпеченні безпеки країни в інформаційній сфері.

Можна переконливо стверджувати, що рф систематично використовує політичні, соціально-економічні, інформаційно-психологічні важелі та засоби для відновлення свого геополітичного впливу в Україні, яка продовжує гібридну війну. Деструктивна пропаганда ззовні та всередині України, використовуючи соціальні протиріччя, розпалює соціальну ворожнечу, провокує конфлікти та підриває суспільну єдність. З боку рф посилюється інформаційний вплив, що межує з явним ігноруванням вимог міжнародного та внутрішнього законодавства, особливо щодо розпалювання сепаратистських та автономістських настроїв.

Крім того, російська сторона активно залучає на фінансовій основі українських журналістів-розслідувачів для здійснення своєї пропагандистсько-деструктивної діяльності. Водночас російські технологи розробляють цілий ряд пропагандистських заходів, спрямованих на

дестабілізацію внутрішньополітичної ситуації в країні напередодні та під час виборів до органів місцевого самоврядування, особливо у східних та південних областях (Харків, Донецьк, Луганська, Запорізька, Дніпропетровська, Херсонська, Миколаївська, Одеська області), а також у Закарпатській області з точки зору «підігріву» сепаратистських настроїв.

Також основною метою політичного керівництва рф є роздмухування інформаційної істерії, до якої підсвідомо чи навмисно втягуються деякі українські ЗМІ, щоб створити умови, які перешкоджають проведенню будь-яких якісних реформ. Це змушує всі гілки влади ситуативно реагувати на внутрішні вогнища напруги та спрямовувати зусилля на їх локалізацію, збалансовуючи потенційні стабілізаційні процеси. Це означає, що обсяги російської пропаганди та дезінформації постійно зростають, набирають обертів, що спонукає до розвитку інституційних та організаційно-правових механізмів запобігання та боротьби з такими деструктивними явищами, вимагає активізації зусиль Служби безпеки України, посилення її здатність подолати російську інформаційну експансію.

Наразі у вітчизняному інформаційному просторі спостерігається високий рівень зовнішніх загроз, зумовлених активною інформаційно-пропагандистською експансією з боку рф. Зокрема, через інформаційну сферу здійснюються спроби вплинути на політичні та соціально-економічні процеси в нашій державі, підірвати авторитет легітимної української влади з метою деморалізації суспільства та посилення невдоволення та протестних емоцій.

Також російська сторона активно запроваджує технології оприлюднення актуальної інформації в мережі Інтернет та ЗМІ, розповсюдження якої розраховане на місцеве населення окупованих територій, громадян російської федерації та міжнародне співтовариство. Антиукраїнська інформаційна кампанія функціонально здійснюється російською стороною за кількома напрямками, які спрямовані на: популяризацію ідей федеративного державного устрою України як

альтернативи розпаду країни; забезпечення постійного потоку маніпулятивної дезінформації про події в Україні та на її окупованих територіях; внесення розколу в середовище українських правлячих кіл, у тому числі публікація провокаційних і деструктивних матеріалів, критика центральної влади, яка «ігнорує інтереси регіонів», компрометація громадських і політичних діячів, стимулювання масових акцій протесту; створення в Україні під виглядом представництв європейських організацій підконтрольних російській стороні громадських структур для проведення активної роботи в інформаційній, аналітичній та гуманітарній сферах у геополітичних інтересах рф тощо.

В таких умовах, при розгляді проблеми організації забезпечення ІБ особливого значення набуває її структурна класифікація, яка є відносно умовною і побудована відповідно до певних цілей і завдань. З цієї точки зору рекомендується поділяти ІБ за джерелами загроз на два типи – безпеку технічного характеру, зумовлену технологією інформаційно-комунікаційних процесів, і безпеку, спричинену соціальними чинниками. Таким чином, актуальні загрози ІБ мають соціальний характер і зосереджені у внутрішньополітичній, економічній, соціальній, екологічній, інформаційній та духовній сферах життєдіяльності нашого суспільства.

Для адекватного реагування на поширення гібридних загроз в Україні наприкінці 2021 р. на національному рівні затверджено Стратегію ІБ як основоположний документ, що визначає завдання та методи діяльності держави з метою запобігання кризовим явищам, зміцнення ІБ та її складових у вітчизняному інформаційному просторі. Очікується, що практична реалізація цієї стратегії посилить спроможність країни забезпечувати власну ІБ та захист інформаційного простору. Цей документ визначає росію та її інформаційну політику як головну загрозу безпеці України. Стратегія має бути реалізована до 2025 р. Метою цієї стратегії є зміцнення спроможності забезпечити ІБ країни, її інформаційного простору, забезпечення інформаційними ресурсами та заходами соціально-політичної стабільності,

захисту країни, захисту державного суверенітету, територіальної цілісності України, демократичного конституційного ладу, що гарантує права і свободи кожного громадянина.

Досягнення мети здійснюватиметься заходами щодо стримування та боротьби із загрозами ІБ України та нейтралізації інформаційної агресії, у тому числі проведенням спеціальних інформаційних операцій держави-агресора, спрямованих на підрив державного суверенітету та територіальної цілісності України, забезпечення інформаційної стабільності суспільства і держави, створення ефективної системи взаємодії органів державної влади, місцевого самоврядування з суспільством, розвиток міжнародного співробітництва у сфері ІБ на засадах партнерства та взаємопідтримки.

Цей декларативний документ (Стратегія ІБ) визначає 7 важливих довгострокових цілей. Перший включає боротьбу з дезінформацією та інформаційними операціями, переважно держави-агресора, спрямованими проти України. Друге – забезпечення всебічного розвитку української культури та утвердження української громадянської ідентичності. Третє – підвищення медіакультури та медіаграмотності суспільства. Четвертий – забезпечення дотримання прав особи на збір, зберігання, використання та поширення інформації, свободу вираження поглядів і переконань, захист приватного життя, доступ до об’єктивної та достовірної інформації та забезпечення захисту прав журналістів. П’яте – інформаційна реінтеграція громадян України, які проживають на тимчасово окупованих територіях та суміжних територіях України, у загальноукраїнський інформаційний простір. Шосте – розвиток інформаційного суспільства та підвищення культури діалогу. Сьома мета – створити ефективну систему стратегічних комунікацій. Таким чином, зазначені цілі формують сфери, які потребують посилення контролю з боку держави та є визначальними в контексті забезпечення ІБ.

Таким чином, до переліку загроз і викликів, які стоять перед нашою державою, входять: широка інформаційна політика російської федерації в її повному обсязі; досить низький рівень медіаграмотності громадян;

динамічне зростання кількості глобальних кампаній дезінформації; інформаційне домінування російської федерації на тимчасово окупованих територіях; використання технологій для маніпулювання свідомістю пересічних громадян щодо наслідків вступу України до НАТО та ЄС тощо. Зокрема, передбачається, що успішна реалізація Стратегії ІБ матиме такі позитивні наслідки, як побудова інформаційного простору, який забезпечує ІБ країни та його учасників; ефективна робота системи стратегічних комунікацій; запровадження ефективних заходів протидії поширенню нелегального контенту тощо.

В умовах гібридної війни наша країна, яка стала об'єктом агресії, неминуче наражається на широкий спектр інформаційних загроз, нейтралізація яких потребує неординарних правових і адміністративних заходів, з одного боку, а з іншого, може супроводжуватися суттєвим звуженням демократичних прав і свобод. Знаходження балансу між інтересами національної безпеки та ідеями правової держави є стратегічно важливим завданням органів влади. Тому ІБ набуває особливого значення в умовах глобалізаційних процесів та міжнародної інтеграції. Країни, які мають великий потенціал в інформаційному середовищі, можуть впливати на країни, в яких інформаційний простір є незахищеним. За останні три роки в Україні реалізовано більше заходів щодо забезпечення ІБ в інформаційному просторі, ніж за весь попередній період незалежності.

Загалом існує десяток різних видів інформаційного впливу. Тому слід розрізняти пропаганду, спеціальні інформаційні операції, психологічні операції, дезінформацію та інші види впливу, оскільки кожна з них має свій алгоритм, форми та методи здійснення. Досвід протидії інформаційним операціям переконливо свідчить, що вони здебільшого плануються та організовуються з-за кордону, але з опорою на наявні оперативні позиції та можливості країни, де така операція проводиться. Зазвичай російські інформаційні операції відрізняються тим, що вони плануються і проводяться в рамках єдиного оперативного плану і спільного стратегічного наративу, і

відрізняються лише формами і методами проведення, а також вибором цільової аудиторії. Але прямі замовники часто проживають в Україні, що дозволяє вітчизняній спецслужбі виявляти окремих осіб, мережі фермерських ботів чи фермерських тролів і вживати до них відповідних заходів, передбачених чинним законодавством.

Наприклад, ферми тролів – це складна структура, яка має свою ієрархію, де працюють «живі» люди. Верхня ланка – це ті, хто пише пости, виступає з «експертною» думкою, ініціює дискусію та визначає напрямок дискусії. Як правило, вони самостійно пишуть тексти на задану клієнтом тему, відповідно до затверджених методичних рекомендацій. Показовою ознакою таких тролів є збіг повідомлень і часу підняття тієї чи іншої теми. Нижче за ієрархією йдуть виконавці, які діляться дописами перших, додають власні слова та активно відповідають на коментарі користувачів, щоб підтримати пост у стрічці новин. Найнижча ланка – це люди, які дають позиційні коментарі. Як правило, вони роздають заздалегідь написані коментарі (10-20 варіантів) і неохоче обговорюють. Вони не можуть відповісти на більш-менш серйозне питання по темі, яку коментують. Головне завдання тролів – ініціювати в мережі інформаційну хвилю на певну тему (або хвилю «флуду», «флейму»), до якої масово приєднаються реальні користувачі. Але ферми ботів чи тролів за своєю суттю небезпечні. Їх вражаюча ефективність забезпечується тим, що практично всі сегменти бото- і трол-ферм (якщо мова йде про російські) є функціональними компонентами російських автоматизованих комплексів моніторингу Інтернету з прихованими функціями впливу на процеси в середовищі соцмережі. Так, в російській федерації діють системи управління компаній «Крібрум», «Медіалогія», «Квант», «Бастіон», «Бренд Аналітика» та ін. Кількість автоматизованих облікових записів ботів, що працюють у всьому світі, становить понад 100 млн акаунтів.

Таке поєднання дозволяє реалізувати небезпечну технологію впливу на користувачів соціальних мереж, так званий «астротурфінг» – імітацію

широкої суспільної підтримки певних ідей, думок, повідомлень, а також осіб чи політичних сил. Астротурфінг дозволяє створити хибну громадську думку або інтерпретацію події, яка буде сприйматися користувачами Інтернету як реальна. Наявність таких систем дозволяє російській федерації на основі моніторингу інтернет-контенту та аналітичної обробки «великих даних» виявляти вразливі місця противника, планувати, реалізовувати та коригувати власні інформаційні атаки, відстежувати їх ефективність.

За таких умов не можна недооцінювати роль і місце Служби безпеки України в забезпеченні ІБ в Україні. Логічно, що у положеннях Стратегії ІБ важлива роль відводиться діяльності вітчизняної спецслужби, яка в межах своїх повноважень здійснює контроль спеціальними методами та способами вітчизняних та іноземних ЗМІ з метою виявлення реальних та потенційних загроз безпеці країни в інформаційній сфері; організовує та забезпечує протидію проведенню спеціальних інформаційних операцій проти України, особливо російської федерації, спрямованих на підрив конституційного ладу, порушення суверенітету та територіальної цілісності України.

Наприклад, за результатами успішної діяльності з попередження та протидії інформаційним загрозам вітчизняна спецслужба за перше півріччя 2021 р. відзвітувала про такі досягнення: відкрито 21 кримінальне провадження за ст. 109 та ст. 110 КК України; 19 осіб обвинувачують у діях, відповідальність за які передбачена ст. 109 та ст. 110 КК України; заборонено в'їзд в Україну понад 50 іноземним громадянам; заблоковано 8 ботів із загальною кількістю понад 35 тис. акаунтів; припинено діяльність 16 інтернет-агітаторів; здійснено понад 180 профілактичних заходів; заблоковано 58 інтернет-ресурсів, на яких поширювався неправдивий та деструктивний контент. За перше півріччя 2021 р. кіберфахівці Служби безпеки України локалізували майже 350 потенційних загроз ІБ нашої країни. Притягнуто до кримінальної відповідальності 35 хакерів і ворожих пропагандистів, засуджено 14 злочинців.

На цьому тлі СБУ стала ефективним інструментом у роботі РНБО. Також зазначимо, що у липні 2021 р. при РНБО було створено групу захисту національного інформаційного простору. Очікується, що напрацювання та результати робочої групи можуть бути використані для ініціювання впровадження відповідних регуляторних змін з урахуванням досвіду демократичних країн світу щодо забезпечення високого рівня захисту від трансформаційних гібридних загроз.

Цілеспрямоване маніпулювання громадською думкою із застосуванням технологій інформаційно-психологічного впливу – один із найнебезпечніших проявів гібридної війни, яку держава-агресор веде проти України. ІБ – характеристика стійкого стану загальної системи управління державою, яка зберігає свої важливі складові під впливом внутрішніх і зовнішніх загроз. Іншими словами, ІБ відповідає за захист інтересів громадянина і держави в інформаційній сфері від різних загроз, як реальних, так і віртуальних.

Концепція ІБ України розкривається через стратегію існування суверенної та стабільної держави, а також через розробку та реалізацію цілеспрямованої системної та виваженої політики захисту національних інтересів від зовнішніх та внутрішніх інформаційних загроз.

Важливим і актуальним нормативно-правовим актом, який узагальнює та декларує нагальні питання безпеки в національному інформаційному просторі, є Стратегія ІБ держави на наступні п’ять років (2022-2025 рр.). У положеннях зазначеної Стратегії концептуально розкрито важливі для нашої держави аспекти, такі як:

- глобальні та національні загрози та виклики національній ІБ;
- завдання та напрямки реалізації основних положень Стратегії;
- засади стратегічного планування в цій сфері;
- методику досягнення результатів впровадження основних правил та ін.

Цим важливим завданням держави визначено прискорення затвердження плану заходів щодо реалізації Стратегії ІБ та моніторингу її

реалізації. Актуальним завданням державного стратегічного планування залишається раціональний розподіл потенційних можливостей і наявних ресурсів держави (людських, інформаційних, фінансових, телекомунікаційних, технічних, технологічних), завдяки чому держава гарантує забезпечення національної безпеки та стабільного соціально-економічного та цифрового розвитку громадянського суспільства в цілому. Для досягнення цієї мети необхідний достатньо високий рівень культури управління державним апаратом та застосування методів системного аналізу та прогнозування, спеціальних методів забезпечення ІБ тощо. Саме стратегічне планування у сфері ІБ дає змогу суттєво підвищити ефективність та якість державного управління у цій сфері.

Стратегічне планування має розглядатися всіма органами державної влади та управління як універсальний інструмент, завдяки якому можна забезпечити виконання нагальних державних завдань у сфері ІБ, в тому числі з використанням механізму державно-приватного партнерства. У сучасних умовах суспільство в цілому та державно-громадський сектор в ІТ-сфері зокрема відчувають на собі наслідки триваючої агресії російської федерації, яка має гібридний характер, проникаючи в інформаційний простір, завдаючи значної шкоди державним інтересам та приватнийому бізнесу.

Рф намагається маніпулювати свідомістю пересічних громадян, нагнітати соціальну напругу, а також поширювати заборонену законом інформацію за рахунок використання нових технологій, зокрема соціальних мереж і систем мікроблогів тощо. Найближчим часом очікується зростання кількості подальших спеціальних інформаційних операцій рф проти України з метою створення умов для соціальної напруги, формування загальної недовіри до чинної влади, шляхом поширення фейкової або спотвореної інформації про діяльність центральної влади, військових командування та правоохоронних органів. Кінцевою метою зазначеної діяльності є формування суспільно-політичної платформи проросійського спрямування та

прихід до влади проросійськи орієнтованих політиків для кардинальної зміни зовнішньополітичного курсу України.

У сучасних реаліях гібридна війна стає все більш інтенсивною та набуває нових форм. Тому реформа Служби безпеки України має враховувати інноваційні гібридні загрози з боку російської федерації та передбачати спеціальні механізми захисту від таких загроз. Важливими завданнями, які повинні бути віднесені до компетенції Служби безпеки України, є:

- здійснення заходів, спрямованих на виявлення, попередження та припинення використання іноземними організаціями та їх посадовими особами, радикально налаштованими представниками вітчизняних ЗМІ на шкоду безпеці України;

- систематичне вжиття додаткових заходів, спрямованих на блокування поширення в ЗМІ та мережі Інтернет матеріалів, що містять заклики до посягань на державний суверенітет, територіальну цілісність України, міжнаціональних, міжконфесійних конфліктів, пропаганду війни тощо.

Термін «ІБ» необхідно включити до загальних положень Доктрини ІБ [89], а також до ст. 1 чинного Закону «Про національну безпеку України» [63], зокрема – щодо досягнення та в контексті забезпечення балансу між свободою та безпекою в інформаційній сфері, що є ключовою цінністю демократичних суспільств.

З метою розробки Доктрини ІБ України, відповідно до ст. 17 Конституції України [32], питання розробки, прийняття та впровадження спеціального Закону України «Про інформаційну безпеку України», який має бути сформований на єдиній методологічній основі з чинним Законом України «Про національну безпеку України», деталізуючи його положення щодо: а) ІБ людини і громадянина, суспільства і держави; б) основні принципи державної політики забезпечення національної (інформаційної) безпеки.

Водночас для забезпечення ефективного функціонування системи ІБ України необхідно підвищити ефективність роботи структурних підрозділів системи захисту інформації в органах державного управління, організаціях та на підприємствах, що призведе до оптимізації роботи та підвищення ефективності системи захисту інформації України.

Отже пріоритетними стратегічними напрямами забезпечення ІБ України в контексті європейської інтеграції є:

1) розроблення та реалізація відповідних заходів державної політики щодо протидії асиметричним діям, проявам і формам інформаційної агресії;

2) спротив інформаційним операціям проти України, а також маніпуляції свідомістю суспільства;

3) формування інтегрованої системи оцінювання впливу інформаційних загроз і протидії (нейтралізації) цих загроз;

4) розроблення та впровадження в дію органами державної влади скоординованої інформаційної політики;

5) пошук та виявлення суб'єктів інформаційного простору в Україні з метою протистояння веденню інформаційної війни відносно України;

6) формування та розвиток спеціалізованих інститутів, до основних компетенцій яких належить забезпечення захисту інформаційно-психологічної безпеки в Україні, базуючись, зокрема, на практиці країн-членів НАТО;

7) покращення основ професійної підготовки осіб, які вивчають захист ІБ, у розробленні та реалізації спеціальних освітніх програм із медіакультури у сучасному інформаційному суспільстві спільно з громадськістю та бізнесом.

У контексті цієї необхідної умови для подальшого ефективного та дієвого партнерства і співробітництва між Україною та країнами-членами Європейського Союзу у сфері забезпечення і посилення національної безпеки в інформаційній сфері є безумовне і комплексне виконання центральними органами виконавчої влади України, зокрема Міністерством закордонних

справ України та Міністерством цифрової трансформації України, положення Доктрини ІБ України.

Розвиток цифрової економіки та цифровізація пріоритетних сфер життєдіяльності суспільства (в контексті забезпечення ІБ в Україні) повинна супроводжуватися відповідним (належним) рівнем довіри, безпеки і відповідальності; при реалізації заходів розвитку цифрової економіки необхідно передбачити заходи щодо формування безпечного інформаційного простору та забезпечення ІБ на основі єдиної політики ІБ та кібербезпеки держав-учасників ЄС та НАТО з урахуванням юридичної відповідальності за правопорушення у сфері забезпечення ІБ. Представлені пропозиції необхідно врахувати при удосконаленні Концепції розвитку цифрової економіки та суспільства України.

З метою забезпечення ІБ Україна повинна активно співпрацювати із країнами-членами Європейського Союзу і така співпраця повинна, насамперед, полягати у формуванні і розвитку регіональної та міжнародної системи ІБ, основна спрямованість функціонування якої має бути націлена на запобігання, протидію та усунення уже виниклих інформаційних загроз, зокрема, таких як кіберзлочинність і кібертероризм. Забезпечення ІБ України має базуватися на стандартах Європейського Союзу та НАТО.

ВИСНОВКИ

У сучасних умовах інформаційна складова національної безпеки держави відіграє надзвичайно важливу роль через наявні в ній ризики та загрози, до яких належать кібертероризм, кіберзлочинність, агресивна пропаганда, поширення антиконституційних та антидержавних гасел, обмеження доступу населення до публічної інформації тощо.

Громадські структури є повноправними учасниками процесу забезпечення ІБ держави. Як свідчить суспільно-політична практика, для ефективної протидії інформаційним загрозам зусиль держави зазвичай недостатньо, що зумовлює необхідність побудови діалогу із суспільством. Основними елементами механізму взаємодії влади та суспільства у цій сфері є інституційна, правова та практична складові. Ефективність усієї державної системи ІБ залежить від повного використання всіх можливостей і ресурсів, наявних у суспільстві. Політика ІБ має бути спрямована на забезпечення гарантій ІБ всіх суб'єктів інформаційного суверенітету та ІБ України, оскільки ІБ – це процес задоволення інформаційних потреб суб'єктів національної безпеки.

Характер інформаційних потреб суб'єктів національної безпеки визначає зміст інформаційного забезпечення національної безпеки. ІБ відіграє важливу багатогранну роль у визначенні національних інтересів і пріоритетів національної безпеки. Для забезпечення ІБ держави необхідним є: комплексне задоволення потреб громадян, підприємств, установ та організацій усіх форм власності щодо доступу до достовірної та об'єктивної інформації; збереження та примноження духовних, культурних і моральних цінностей народу України, розвиток медіакультури суспільства та соціально відповідального медіасередовища, формування ефективної правової системи захисту особи, суспільства та держави від деструктивного впливу пропаганди, створення системи та механізмів захисту від зовнішніх

інформаційно-психологічних негативних впливів, насамперед пропаганди, на основі норм міжнародного права, розвиток інформаційного суспільства.

В умовах війни основні напрямки інформаційної політики держави не змінилися, але виклики, пов’язані з агресією противника, вимагають від держави суттєвої активізації дій у напрямку інформаційної безпеки, співпраці з громадянським суспільством, розбудови інформаційної системи.

Основною метою державної політики у сфері ІБ України є управління реальними загрозами та небезпеками з метою створення необхідних умов для задоволення інформаційних потреб держави, суспільства та особи. У багатьох наукових працях з питань ІБ цілями державної політики України у сфері ІБ є: захист інформаційного суверенітету держави в сучасних умовах глобалізації; забезпечення достатності інформації для прийняття рішень органами влади, суб'єктами господарювання та громадянами; реалізація конституційних прав і законних інтересів людини, суспільства і держави в інформаційній сфері. ІБ в країні має забезпечуватися реалізацією єдиної державної політики в інформаційній сфері, збалансованою системою заходів економічного, політичного, соціального та організаційного характеру, реальних загроз і небезпек національним інтересам особи, суспільства.

Сучасний стан інформаційної політики в умовах військової агресії рф проти України вимагає нових, нестандартних підходів до налагодження взаємодії з військовими адміністраціями регіонів, складовою якої також є ІБ. Нарешті, створення нормативно-правової та інституційної бази не завершує формування цілісної системи ІБ. Це потребує надто багато людських, професійних та матеріально-технічних ресурсів, зокрема для реалізації цілеспрямованої зовнішньої інформаційної політики, яких, на жаль, Україні поки що не вистачає, на відміну від держави-агресора, яка роками вибудовувала свою пропаганду водночас із озброєнням, у тому числі за кордоном.

Функції забезпечення ІБ належать до пріоритетів інших функцій забезпечення національної безпеки. Відмінністю виконання зазначених

функцій в умовах широкомасштабної збройної агресії рф є те, що на сьогоднішній день пріоритетним є використання кінетичної зброї. Проте здатність України ефективно протистояти російській агресії значною мірою залежить від успішного застосування функції оповіщення міжнародної спільноти про порушення противником законів і звичаїв війни, заподіяння шкоди життю, здоров'ю, власності цивільного населення. Крім того, актуальною залишається функція підвищення високого рівня інформаційної культури, що унеможливлює деструктивний вплив противника на життєдіяльність держави та громадянського суспільства.

За допомогою пропаганди інформаційна війна діє на чотирьох рівнях: індивідуальному, територіальному (регіональному), національному та глобальному. Кожен із цих рівнів містить певні ризики: втрата ідентичності, відчуття відчуженості, формування образу «внутрішнього ворога» за територіальною (регіональною) ідентичністю або втрата капіталу авторитету держави.

Цілеспрямоване маніпулювання громадською думкою з використанням інформаційних технологій та психологічного впливу є одним із найнебезпечніших проявів гібридної війни, яку держава-агресор веде проти України. ІБ – ознака стійкого стану загальної системи управління державою, яка зберігає свої важливі складові під впливом внутрішніх і зовнішніх загроз. Іншими словами, ІБ відповідає за захист інтересів громадянина і держави в інформаційному полі від різних загроз, реальних і віртуальних. Концепція ІБ України розкривається як стратегія існування суверенної та стабільної держави, а також через розробку та реалізацію системної та виваженої політики, спрямованої на захист національних інтересів від зовнішніх та внутрішніх інформаційних загроз.

Важливим і актуальним нормативно-правовим актом, який узагальнює та декларує нагальні проблеми забезпечення безпеки у вітчизняному інформаційному просторі, є Стратегія інформаційної безпеки держави, яка розрахована на найближчі 5 років (2022 – 2025 роки). Положення цієї

стратегії концептуально розкривають такі важливі для нашої держави аспекти, як: проблеми та напрями реалізації основних положень стратегії, принципи стратегічного планування в цій сфері, методику досягнення ефективності реалізації її основних положень, механізми успішної реалізації її положень у практичному вимірі, у контексті побудови основ державної інформаційної політики. Водночас важливим завданням держави є прискорення затвердження плану заходів щодо реалізації Стратегії інформаційної безпеки та забезпечення контролю за її виконанням.

Актуальною проблемою державного стратегічного планування залишається раціональний розподіл державою потенційних можливостей та наявних ресурсів (людських, інформаційних, фінансових, телекомунікаційних, технічних, технологічних), завдяки чому держава гарантує забезпечення національної безпеки та стабільної соціально-економічної ситуації, а також та цифровий розвиток громадянського суспільства загалом. Для досягнення цієї мети необхідний достатньо високий рівень культури управління державним апаратом та використання методів системного аналізу та прогнозування, спеціальних методів забезпечення ІБ тощо.

Сьогодні стратегічною метою зовнішньої політики України є національні інтереси та європейська інтеграція, де реалізація курсу на інтеграцію до ЄС потребує особливих заходів, а також удосконалення нормативно-правової бази ІБ України відповідно до міжнародних стандартів. Для забезпечення ІБ Україна має активно співпрацювати з державами-членами ЄС, і ця співпраця, насамперед, має полягати у формуванні та розвитку регіональної та міжнародної системи ІБ, головною метою якої є: бути спрямованими на запобігання, протидію та усунення вже існуючих загроз ІБ, зокрема, таких як кіберзлочинність та кібертероризм. ІБ України має базуватися на стандартах ЄС та НАТО.

Стратегічне планування у сфері ІБ дає можливість значно підвищити ефективність та якість державного управління у цій сфері. Стратегічне

планування всіма органами державної влади та управління слід розглядати як універсальний інструмент, завдяки якому можна забезпечити реалізацію актуальних державних проблем у сфері ІБ, в тому числі з використанням механізму публічно-приватного співробітництва.

В умовах наростаючої активізації глобальних процесів у сучасному світі, які поряд із позитивними аспектами свого впливу на світову спільноту створили також небезпеки інформаційної агресії та кіберзлочинності, саме загальнодержавна система ІБ, координована держави у своїй діяльності, якою може стати нейтралізація інформаційних загроз та інформатизація, гарантія використання позитивних факторів розвитку. Важливою складовою загальної політики забезпечення ІБ України є активізація участі суспільства і держави в процесах удосконалення відносин між суспільством і державою. Про подальше зміцнення ІБ країни свідчать спільні злагоджені дії всіх державних інституцій, суспільства та медійної спільноти. У сучасних умовах необхідно вирішувати не лише такі важливі проблеми, як формування власного інформаційного простору та його захист від загроз, а й переходити від оборонної стратегії до наступальної.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Арабаджиєв Д.Ю., Сергієнко Т.І. Політична маніпуляція та інформаційно-психологічна безпека в політичних відносинах. Політикус : наук. журн. Одеса: Гельветика, 2020. № 2. С. 36–43. https://doi. org/10.24195/2414-9616-2020-2-36-43
2. Арістова І.В. Державна інформаційна політика: організаційно-правові аспекти: монографія. Харків: Видавництво Харківського державного університету внутрішніх справ. 2000. 368 с.
3. Архипова Є.О. Інформаційна безпека: соціально-філософський вимір: автореф. дис. … канд. філософ. наук: 09.00.03. Київ, 2012. 21 с.
4. Баранов О.А. Правове забезпечення інформаційної сфери: теорія, методологія і практика. Київ: Едельвейс, 2014. 497 с.
5. Баровська А. Інституційне забезпечення державної комунікативної політики : досвід країн Європи : аналітична доповідь. – Режим доступу : //www.niss.gov.ua /articles/1730
6. Березовська І.Р. Адміністративно-правові засоби забезпечення інформаційної безпеки в Україні: дис. … канд. юрид. наук: 12.00.07. Київ, 2012. 239 с.
7. Бєляков К.І. Інформація в праві: теорія і практика / Державний НДІ Міністерства внутрішніх справ України. Київ: КВІЦ, 2006. 118 с.
8. Бєляков К.І. Організаційно-правове та наукове забезпечення інформатизації в Україні: проблеми теорії та практики: автореф. дис… д-ра юрид. наук: 12.00.07 / НАН України, Інститут держави і права ім. В.М. Корецького. Київ, 2009. 38 с.
9. Боднар І.Р. Інформаційна безпека як основа національної безпеки. Механізм регулювання економіки. Суми, 2014. URL: http://www.lac.lviv.ua/ fileadmin; www. lac.lviv.ua/data/kafedry/MEV/Bodnar/Bodnar_Vy b_Pub_9.pdf

10. Бурило Ю.П. Організаційно-правові питання державного управління в інформаційній сфері: автореф. дис. … канд. юрид. наук: 12.00.07. Київ, 2008. 18 с.
11. Гаврильців М.Т. Інформаційна безпека держави в системі національної безпеки України. Юридичний науковий журнал. 2020. № 2. С. 200-203.
12. Ганжуров Ю. Політична комунікація: проблеми структуризації. Політ. менеджмент. Київ, 2004 . № 2. С. 121–129. URL : http://nbuv.gov.ua/UJRN/P oMe_2004_2_12
13. Гладенко О.М. Міжнародно-правове співробітництво України з Європейським Союзом у сфері спільної зовнішньої політики та політичної безпеки: автореф. дис. … канд. юрид. наук: 12.00.11. Одеса, 2010. 21 с.
14. Головка А.А. Вдосконалення механізмів залучення громадянського суспільства до реалізації політики безпеки у інформаційній сфері України // Наук.-інформ. вісн. Академії нац. безпеки, 2016. № 1-2. С. 86–98.
15. Гончаров М.В. Сутність інформаційної безпеки в умовах розвитку сучасного суспільства [Електронний ресурс] / М. В. Гончаров // Міжнародний науковий журнал "Інтернаука". Серія : Юридичні науки. - 2022. - № 4. - С. 77-82. - Режим доступу: http://nbuv.gov.ua/UJRN/mnjiu_2022_4_12
16. Горбулін В.П., Биченок М.М. Проблеми захисту інформаційного простору України: монографія. Київ: Інтертехнологія, 2009. 136 с.
17. Гордієнко С. Доктринальні положення інформаційної безпеки України в умовах сучасності. Юридичний вісник. 2019. № 3. URL: https://lexinform.com.ua/dumka-eksperta/doktryn alni-polozhennya-informatsijnoyi-bezpeky-ukrayiny-v-umovah-suchasnosti
18. Горовий В.М. Правові перспективи національного розвитку. – Режим доступу : http://uaforeignaffairs.com/ua/ekspertna-dumka/view/article/nablizhajuchi-derzhavu-do-suspilstva/#st hash.AgJjKJa4.dpuf

19. Громико І., Саханчук Т. Державна домінантність визначення інформаційної безпеки України в умовах протидії загрозам // Право України. 2008. № 8. С. 130–134.
20. Гурковський В.І. Організаційно-правові питання взаємодії органів державної влади у сфері національної інформаційної безпеки: дис. … канд. юрид. наук: 25.00.02. Київ, 2004. 225 с.
21. Гуцу С. Ф. Правові основи інформаційної діяльності: навч. посібник. Х.: «Нац. Аерокосм. Ун-т «Харк. авіац. ін.-т», 2009. 48 с.
22. Деякі питання забезпечення функціонування інформаційно-комунікаційних систем, електронних комунікаційних систем, публічних електронних реєстрів в умовах воєнного стану: Постанова Кабінету Міністрів України від 12.03.22 р. № 263. URL: https://zakon.rada.gov.ua/laws/show/263-2022п#Text
23. Дзьобань О.П., Панфілов О.Ю., Чемчекаленко Р.А. Методологічний контекст дослідження проблеми інформаційної безпеки. Зовнішня торгівля: економіка, фінанси, право. 2014. № 2. С. 171–180.
24. Довгань О.Д. Організація правового гарантування безпеки інформаційних обмінів у контексті глобалізації // Правова інформатика. – 2013. – № 4(40). – С. 79-88.
25. Довгань О.Д., Ткачук Т.Ю. Система інформаційної безпеки України: онтологічні виміри. Інформація і право. № 1(24)/2018. С. 89-103.
26. Єсімов С.С. Шляхи удосконалення нормативно-правового регулювання в сфері інформаційної безпеки. Наукові записки Львівського університету бізнесу та права. 2013. Вип. 11. С. 73–76.
27. Заярний О.А. Правове забезпечення розвитку інформаційної сфери України: адміністративно-деліктний аспект: монографія. Київ: Видавничий дім «Гельветика», 2017. 700 с.
28. Золотар О.О. Інформаційна безпека людини: теорія і практика : монографія. Київ : ТОВ «Видавничий дім «АртЕк», 2018. 446 с.

29. Золотар О.О. Правові основи інформаційної безпеки людини: автореф. дис. …д-ра юрид. наук: спеціальність 12.00.07. Харків. 2018. 37 с.
30. Ісаєва В.В. Функції права: теоретико-правовий аналіз // Часопис Київського університету права, 2013. № 1. С.45–48.
31. Калюжний Р.А. Інформаційне право України: концептуальні основи формування // Науковий вісник Дніпропетровського юридичного інституту МВС України. № 3(6). 2001. С. 234–244.
32. Конституція України: Закон України від 08.06.1996 р. № 254к/96-ВР / Відомості Верховної Ради України. 1996. № 30. Ст. 141.
33. Кормич Б.А. Інформаційна безпека: організаційно-правові основи: навчальний посібник. К.: Кондор, 2004. 382 с.
34. Кормич Б.А. Організаційно-правові засади політики інформаційної безпеки України: монографія. Одеса: Юридична література, 2003. 472 с.
35. Красіков Д.О. Правове забезпечення інформаційної безпеки в діяльності органів внутрішніх справ України: дис. … канд. юрид. наук: 12.00.07. Київ, 2012. 220 с.
36. Крюков О.І. Комунікація влади і суспільства як чинник реалізації політики інформаційної безпеки. Вісн. Нац. ун-ту цивільного захисту України. Серія «Державне управління». Харків, 2017. Вип. 1. С. 201–207.
37. Лисенко С.О. Конституційні засади розуміння інформаційної безпеки. Публічне урядування. 2016. № 4. С. 154–161.
38. Ліпкан В.А. Теоретичні основи та елементи національної безпеки: монографія. Київ: «Текст», 2003. 600 с.
39. Логінов О.В. Адміністративно-правове забезпечення інформаційної безпеки органів виконавчої влади: автореф. дис. … канд. юрид. наук: 12.00.07. Київ, 2005. 20 с.
40. Максименко Ю.Є. Теоретико-правові засади забезпечення інформаційної безпеки України: дис. … канд. юрид. наук: 12.00.01 / Київський національний університет внутрішніх справ. Київ, 2007. 186 с.

41. Малашко О.Є. Адміністративно-правові засади забезпечення інформаційної безпеки в Україні у контексті європейської інтеграції: автореф. дис. … канд. юрид. наук: 12.00.07 / Львівський університет бізнесу та права. Львів, 2020. 20 с.
42. Малашко О.Є., Скриньковський Р.М. Пріоритетні напрями удосконалення інформаційної безпеки України // Міжнародний науковий журнал «Інтернаука». Серія: «Юридичні науки». 2020. № 6(28). С. 13–19. doi: https://doi.org/10.25313/2520-2308-2020-6-6163
43. Матійко М.В. Інформаційна функція цивільного права // Актуальні проблеми держави і права, 2008. № 45. С. 199–204.
44. Мороз Н.С. Сутність інформації в контексті загальних принципів інформаційної безпеки. Вісник Національного університету «Львівська політехніка». Юридичні науки. 2016. № 845. С. 137–142.
45. Нашинець-Наумова А.Ю. Інформаційна безпека: питання правового регулювання. Київ: Видавничий дім «Гельветика», 2017. 168 с.
46. Ніщименко О.А. Інформаційна безпека України на сучасному етапі розвитку держави і суспільства // Наше право. 2016. № 1. С. 17–23.
47. Новицький В.Я. Стратегічні засади забезпечення інформаційної безпеки в сучасних умовах [Електронний ресурс] / В.Я. Новицький // Інформація і право. - 2022. - № 1. - С. 111-118. - Режим доступу: http://nbuv.gov.ua/UJRN/Infpr_2022_1_13
48. Олійник О.В. Стан забезпечення інформаційної безпеки в Україні // Юридичний вісник. – 2014. – № 2(31). – С. 59-65.
49. Онищенко О.С. Національні інформаційні ресурси як інтегративний чинник вітчизняного соціокультурного середовища : монографія / [О.С. Онищенко, В.М. Горовий, В.І. Попик та ін.] ; НАН України, Національна бібліотека України ім. В.І. Вернадського. – К., 2014.
50. Онопрієнко С. Функції забезпечення інформаційної безпеки публічного адміністрування в Україні за умов повномасштабної збройної агресії російської федерації [Електронний ресурс] / С. Онопрієнко // Вісник

Київського національного університету імені Тараса Шевченка. Військово-спеціальні науки. - 2022. - Вип. 2. - С. 95-98. - Режим доступу: http://nbuv.gov.ua/UJRN/VKNU_vsn_2022_2_20

51. Остапенко М. Політична комунікація: теоретичні аспекти дослідження. Політ. менеджмент. Київ, 2012. № 3 . С. 135–144.
52. Панченко В.М. Співвідношення понять : інформаційна та кібернетична безпека // Інформаційна безпека людини, суспільства, держави. – 2013. – № 2 (12). – С. 20-24. “Інформація і право” № 3(15)/2015 42
53. Перун Т.С. Адміністративно-правовий механізм забезпечення інформаційної безпеки в Україні: дис. … канд. юрид. наук: 12.00.07. Львів, 2019. 268 с.
54. Перун Т.С. Адміністративно-правовий механізм забезпечення інформаційної безпеки в Україні: автореф. дис. …канд. юрид. наук: спеціальність 12.00.07. Львів. 2019. 23 с.
55. Пилипчук В.Г. Системні правові проблеми формування інформаційного суспільства : зб. наук. ст. та тез ; наукове повідомлення за матеріалами міжнародної науково-практичної конференції [“Інформаційне суспільство і держава : проблеми взаємодії на сучасному етапі”], (Харків, 26 жовтня 2012 р.). – Х. : НДІ державного будівництва та місцевого самоврядування, 2012. – 214 с.
56. Політологічний словник : навч. посіб. для студентів вищ. навч. закладів / за ред. М. Ф . Головатого та О. В. Антонюка. Київ : МАУП, 2005. 792 с.
57. Положення про Державний комітет телебачення і радіомовлення України: затв. постановою Кабінету Міністрів України від 13.08.2014 р. № 341. URL:http://comin.kmu.gov.ua/control/uk/publish/article?art_id=170429&cat_id=32820.
58. Положення про Міністерство культури та інформаційної політики України : затв. постановою Кабінету Міністрів України від 16.10.2019 р. № 885. URL : https://zakon.rada.gov.ua/laws/show/885-2019-%D0%BF#Text.

59. Присяжнюк М., Бєлошевич Я. Інформаційна безпека України в сучасних умовах // Вісник Київського національного університету імені Тараса Шевченка. Військово-спеціальні науки. 2013. Вип. 30. С. 42–46.
60. Пріоритетні завдання Держкомтелерадіо у 2022 році. URL : http://comin.kmu.gov.ua/control/uk/publish/article?art_id=182262&cat_id=68691.
61. Про інформацію: Закон України від 2.10.92 р. № 2657-XII. URL: https://zakon.rada.gov.ua/ laws/show/2657-12#Text
62. Про Кабінет Міністрів України : Закон України від 27.02.2014. Відомості Верховної Ради України. 2014. № 13. Ст. 222.
63. Про національну безпеку України: Закон України від 21.06.2018 р. № 2469-VIII (із змінами та доповненнями). URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text.
64. Про Національну раду України з питань телебачення і радіомовлення : Закон України від 23.091997. Відомості Верховної Ради України. 1997. № 48. Ст. 296.
65. Про нейтралізацію загроз інформаційній безпеці держави: Рішення Ради національної безпеки і оборони від 18.03.22 р. URL: https://zakon.rada.gov.ua/laws/show/n0003525-22#n2
66. Про оборону України : Закон України від 06.12.1991. Відомості Верховної Ради України. 1992. № 9. Ст. 106.
67. Про основи національної безпеки України : Закон України від 19.06.03 р. // Відомості Верховної Ради України (ВВР). – 2003. – № 39. – Ст. 351.
68. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/ laws/show/2163-19#Text.
69. Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки : затв. Законом України від 09.01.2007. Відомості Верховної Ради України. 2007. № 12. Ст. 102.

70. Про Раду національної безпеки і оборони України : Закон України від 05.03.1998. Відомості Верховної Ради України. 1998. № 35. Ст. 237.
71. Про рішення Ради національної безпеки і оборони України від 02.02.2021 р. «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)» : введено в дію Указом Президента України від 02.02.2021 № 43/2021. URL : https://www.rnbo.gov.ua/ua/Ukazy/4801.html.
72. Про рішення Ради національної безпеки і оборони України від 29.12.2016 р. «Про Доктрину інформаційної безпеки України»: Указ Президента України від 25.02.2017 р. № 47/2017. URL: https://zakon.rada.gov. ua/laws/show/47/2017#Text.
73. Про рішення Ради національної безпеки і оборони України від 30.12.2021 р. «Про внесення змін до персональних спеціальних економічних та інших обмежувальних заходів (санкцій)» : введено в дію Указом Президента України від 16.02.2022 р. № 57/2022. URL : https://www.rnbo.gov.ua/ua/Ukazy/5265.html.
74. Про санкції : Закон України від 14.08.2014 р. Відомості Верховної Ради України. 2014. № 40. Ст. 2018.
75. Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018–2020 рр. та затвердження плану заходів щодо її реалізації: Розпорядження Кабінету Міністрів України від 17.01.2018 р. № 67-р. URL: https://zakon.rada.gov.ua/laws/show/67-2018-р
76. Про телебачення і радіомовлення : Закон України від 21.12.1993 р. Відомості Верховної Ради України. 1994. № 10. Ст. 43.
77. Радовецька Л.В. Місце інститутів громадянського суспільства у механізмі реалізації функції забезпечення інформаційної безпеки // Інформаційна безпека людини, суспільства, держави, 2013. № 3. С. 12–18.
78. Самотуга А.В. Організаційно-інституційне забезпечення інформаційної безпеки України [Електронний ресурс] / А.В. Самотуга // Науковий вісник Дніпропетровського державного університету внутрішніх справ. -

2022. - № 1. - С. 195-203. - Режим доступу: http://nbuv.gov.ua/UJRN/Nvdduvs_2022_1_33

79. Самохвалов Ю.Я., Браіловський М.М. Оцінка інформаційної безпеки організації за критерієм впевненості. Захист інформації. 2019. Т. 21. № 1. С. 13-24.
80. Свідерська О.І. Цифрова пропаганда та ризики інформаційної безпеки у контексті російсько-української війни [Електронний ресурс] / О.І. Свідерська // Політикус. - 2022. - Вип. 2. - С. 60-65. - Режим доступу: http://nbuv.gov.ua/UJRN/polit_2022_2_12
81. Скриньковський Р.М., Малашко О.Є. Структурно-класифікаційна характеристика забезпечення інформаційної безпеки // Міжнародний науковий журнал «Інтернаука». Серія: «Юридичні науки». 2020. № 7(29). С. 25–32. doi: https://doi.org/10.25313/2520-2308-2020-7-6200
82. Солодка О.М. Пріоритети удосконалення інформаційної безпеки України. Інформація і право. № 3(15)/2015. С. 36-42.
83. Сопільник Л.І. Особливості забезпечення інформаційної безпеки в Україні [Електронний ресурс] / Л.І. Сопільник, О.Є. Малашко, С.С. Єсімов, І.М. Пилипенко, О.В. Куриліна // Міжнародний науковий журнал "Інтернаука". Серія : Юридичні науки. - 2022. - № 3. - С. 19-24. - Режим доступу: http://nbuv.gov.ua/UJRN/mnjiu_2022_3_4
84. Сопільник Л.І., Скриньковський Р.М., Малашко О.Є., Сопільник Р.Л. Особливості забезпечення інформаційної безпеки: досвід окремих країн Східної Європи // Міжнародний науковий журнал «Інтернаука». 2020. № 12(92). С. 60–68. doi: https://doi.org/10.25313/2520-2057-2020-12-6226
85. Стратегія інформаційної безпеки : затв. Указом Президента України від 28.12.2021 р. № 685/2021. URL : https://www.president.gov.ua/documents/6852021-41069.
86. Стратегія кібербезпеки України «Безпечний кіберпростір – запорука успішного розвитку країни» : затв. Указом Президента України від

26.08.2021 р. № 447/2021. Офіційний вісник Президента України. 2021. № 22. Ст. 1055.

87. Стратегія національної безпеки України : Указ Президента України від 26.05.2015 р. № 287/2015. − Режим доступу : //www.president.gov.ua
88. Субіна Т.В. Адміністративно-правове забезпечення інформаційної безпеки в органах Державної податкової служби України: автореф. дис. … канд. юрид. наук: 12.00.07. Ірпінь, 2010. 22 с.
89. Тарасенко Н. Доктрина інформаційної безпеки України в оцінках експертів. Резонанс. 2017. № 18. С. 3-14. URL: http://nbuviap.gov.ua/images/rezonans/2017/rez18.pdf
90. Тихомиров О.О. Забезпечення інформаційної безпеки як функція сучасної держави: монографія / заг. ред. Р. А. Калюжний. Центр навчально-наукових та науково-практичних видань Національної академії Служби безпеки України, 2014. 196 с.
91. Ткачук Т.Ю. Забезпечення інформаційної безпеки в умовах євроінтеграції України: правовий вимір: монографія. Київ: ТОВ “Видавничий дім “АртЕк”, 2018. 411 с.
92. Ткачук Т.Ю. Правове забезпечення інформаційної безпеки в умовах євроінтеграції України: дис. … д-ра юрид. наук: 12.00.07. Ужгород, 2019. 487 с.
93. Товмаш Д.А. Політична комунікація : сутність та специфіка. Вісн. Київ. нац. ун-ту ім. Т. Шевченка. Філософія. Політологія. 2006. Вип. 76 –79. С. 95–98.
94. Турчак А.В. Основні засади державної політики забезпечення інформаційної безпеки в Україні. Інвестиції: практика та досвід. 2019. № 11. С. 123-127.
95. Харченко Л.С., Ліпкан В.А., Логінов О.В. Інформаційна безпека України: глосарій / заг. ред. Р.А. Калюжний. Київ: «Текст», 2004. 134 с.
96. Хом’яков Д.О. Нормативно-правове регулювання інформаційної безпеки. Актуальні проблеми управління інформаційною безпекою держави:

збірник тез наукових доповідей науково-практичної конференції (Київ, 30 березня 2018 р.). Київ: НА СБУ, 2018. С. 182–184.

97. Цимбалюк В.С. Інформаційне право (основи теорії і практики): монографія. Київ: Освіта України, 2010. 388 с.
98. Шиманова О. Політична комунікація: особливості дослідження. Політична наука в Україні: стан і перспективи : матеріали всеукр. наук. конф. (Львів, 10–11 травня 2007 р.) / укл. Поліщук М., Скочиляс Л., Угрин Л. Львів : ЦПД, 2008. 308 с.
99. Щодо реалізації єдиної інформаційної політики в умовах воєнного стану: Рішення Ради національної безпеки і оборони від 19.03.22 р. URL: https://zakon.rada.gov.ua/laws/show/n00045 25-22#Text

Виконала:

студентка магістратури за спеціальністю 281 Публічне управління та адміністрування галузі знань 28 Публічне управління та адміністрування заочної форми навчання

«____» _____ 2022 р. _____ Т.С. Супрович

Підпис Ініціали, прізвище

Науковий керівник:

доцент кафедри публічного управління та адміністрування, к.держ. упр.

Л.В. Омельчук

«____» _____ 2022 р. _____ _____

Підпис Ініціали, прізвище

Робота допущена до захисту:

завідувач кафедри публічного управління та адміністрування

«____» _____ 2022 р. _____ Е.В. Щепанський

Підпис Ініціали, прізвище