МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ПОЛІСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет права, публічного управління та національної безпеки
Кафедра економічної теорії, інтелектуальної власності та публічного управління

Кваліфікаційна робота
на правах рукопису

ЯРТИМ ВОЛОДИМИР ОМЕЛЯНОВИЧ
(прізвище, ім'я, по батькові здобувача вищої освіти)

УДК: 351.347:004
(індекс)

КВАЛІФІКАЦІЙНА РОБОТА

ІНФОРМАЦІЙНА ПОЛІТИКА ДЕРЖАВИ В УМОВАХ ВОЄННОГО СТАНУ

(тема роботи)

281 «Публічне управління та адміністрування»
(шифр і назва спеціальності)

Подається на здобуття освітнього ступеня магістр кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

В. О. ЯРТИМ
(підпис, ініціали та прізвище здобувача вищої освіти)

Керівник роботи
ХОДАКІВСЬКИЙ Євгеній Іванович
(прізвище, ім'я, по батькові)

доктор економічних наук, доцент
(науковий ступінь, вчене звання)

Житомир – 2023

Висновок кафедри економічної теорії, інтелектуальної власності та публічного управління
за результатами попереднього захисту:**ЯРТИМА Володимира Омеляновича** допущено до захисту.

Протокол засідання кафедри економічної теорії, інтелектуальної власності та публічного управління № ____ від «____» грудня 2023 р.

Завідувач кафедри економічної теорії, інтелектуальної власності та публічного управління
к.е.н., професор _____ Валентина ЯКОБЧУК
(науковий ступінь, вчене звання) (підпис) (власне ім'я, прізвище)

«___» грудня 2023 р.

Результати захисту кваліфікаційної роботи

Здобувач вищої освіти **ЯРТИМ Володимир Омелянович** захистив
(прізвище ,ім'я, по батькові)

кваліфікаційну роботу з оцінкою:
сума балів за 100-бальною шкалою _____
за національною шкалою _____

Секретар ЕК
_____-____ _____ Настасія ПУГАЧОВА
(науковий ступінь, вчене звання) (підпис) (власне ім'я, прізвище)

АНОТАЦІЯ

ЯРТИМ В. О. Інформаційна політика держави в умовах воєнного стану – Кваліфікаційна робота на здобуття освітнього ступеня «Магістр» за спеціальністю 281 – «Публічне управління та адміністрування». – Поліський національний університет, Житомир, 2023.

Досліджено суть, принципи, інструменти та напрями удосконалення державного управління у сфері використання інформаційних ресурсів країни в умовах воєнного стану, зроблено акценти на завданнях розвитку ефективної інформаційної політики держави та стратегіях забезпечення інформаційної незалежності в контексті зростання кіберзагроз та зміни технологій. Проаналізовані основні аспекти адміністрування інформаційними ресурсами в Україні в умовах воєнно-політичної кризи, зростання інформаційних загроз та активізації інформаційних війн.

Ключові слова: інформація, держава, ресурси ,політика, безпека, публічне управління, стратегія, війна.

SUMMARY

YARTYM V. Information Policy of the State in the Conditions of Martial Law - Qualification work for the degree of Master's Degree in specialty 281 - «Public Administration and Management.» - Polissia National University, Zhytomyr, 2023.

The essence, principles, tools and directions of improving public administration in the field of using the country's information resources under martial law are investigated, emphasis is placed on the tasks of developing an effective information policy of the state and strategies for ensuring information independence in the context of growing cyber threats and changing technologies. The main aspects of information resources administration in Ukraine in the context of the military-political crisis, growing information threats and intensification of information wars are analyzed.

Keywords: information, state, resources, policy, security, public administration, strategy, war.

ЗМІСТ

ВСТУП

Актуальність теми. В умовах воєнного стану, перед урядом нашої країни постали актуальні завдання захисту інформаційного простору, збереження інформаційних ресурсів, забезпечення інформаційної безпеки країни і кожного пересічного громадянина, які можна вирішити лише при умові ефективної політики держави в інформаційній сфері. Успішність державного управління набула виключного значення на всіх рівнях адміністрування, що потребує принципово нових, інноваційних механізмів, що формують не результативні стратегії збереження та примноження інформаційних ресурсів.

Особливості інформаційної політики держави аналізувались Бучиком С.С., Довганем О.Д., Марутяном Р., Приймаком Ю.Ю., Сосіним О.В., Юдіним О.К., що стосується питань інформаційної безпеки то вони аналізувались в працях Аніщука В., Виздрика В., Кормича Б.А., Костікова М.В., Мельника О., Нестеренка Г., Плєхова Г. А. та в роботах інших зарубіжних та вітчизняних вчених. Проте, в умовах широкомасштабного воєнного втручання в інформаційний простір країни та розгортання інформаційних війн потребує більш детального аналізу особливостей інформаційної політики держави, чому присвячена кваліфікаційна робота.

Предметом дослідження є сукупність актуальних питань теоретичного, методологічного та прикладного удосконалення механізмів публічного управління інформаційними ресурсами в умовах воєнного стану.

Об'єктом дослідження є процес формування та реалізації інформаційної політики держави.

Метою дослідження є на основі теоретичного обгрунтування цілей та принципів сучасної інформаційної політики в Україні показати конкретні шляхи її удосконалення в умовах воєнного часу.

Відповідно до мети, у роботі потрібно вирішити низку *завдань:*

1. Розкрити сутність поняття та завдання інформаційної політики держави та механізмів управління інформаційними ресурсами.

2. Проаналізувати механізми управління інформаційними ресурсами в Україні.

3. Дати оцінку імплементації світового досвіду інформаційної політики.

4.Обгрунтувати напрями удосконалення інформаційної політики в умовах воєнного стану

Для вирішення поставлених в дослідженні завдань було використано ряд загальнонаукових та специфічних методів наукового пізнання, а саме, монографічно-описовий метод, аналізу та синтезу, методологія порівнянь, методи узагальнень і систематизації при аналізі особливостей інформаційної політики в умовах воєнного стану; наукової абстракції та поєднання логічного з історичним в аналізі управління інформаційними ресурсами, методи економіко-математичні та статистичні для обґрунтування пропозицій щодо покращення інформаційної політики.

Елементи наукової новизни кваліфікаційної роботи полягають в обґрунтуванні основних концептуальних підходів до механізмів публічного управління інформаційними ресурсами в умовах зростання кіберзагроз.

Практичне значення отриманих результатів. Запропоновані у кваліфікаційній роботі пропозиції, можуть бути використані в практиці реалізації інформаційної політики держави.

Апробація результатів дослідження. Результати проведеного дослідження за темою кваліфікаційної роботи доповідались та опубліковані в збірниках тез науково-практичних конференцій.

Інформаційною базою дослідження були дослідження вітчизняних та зарубіжних науковців у сфері публічного управління інформаційними ресурсами, нормативно-правові акти, звіти органів виконавчої влади, Internet-ресурси.

Структура роботи. Кваліфікаційна робота складається зі вступу, трьох розділів та висновків, що викладені на 39 сторінках друкованого тексту, списку використаних джерел із 41 найменування.

РОЗДІЛ 1.
ТЕОРЕТИЧНІ ЗАСАДИ ФОРМУВАННЯ ІНФОРМАЦІЙНОЇ ПОЛІТИКИ ДЕРЖАВИ

1.1. Поняття та інструменти інформаційної політики держави

Інформаційна політика держави є сукупністю принципів, цілей, пріоритетів, заходів та механізмів, які визначаються державою з метою забезпечення ефективного функціонування та розвитку інформаційної сфери, а також захисту національних інтересів у цій сфері. Формування інформаційної політики держави базується на таких концептуальних засадах: по-перше, інформаційна сфера є важливою складовою національної безпеки держави, по-друге, інформація є стратегічним ресурсом, який може використовуватися як для мирних, так і для ворожих цілей. Тому держава має забезпечувати захист інформаційних ресурсів від несанкціонованого доступу, використання та поширення, по-третє, інформація є основою демократичного суспільства і необхідним інструментом для формування громадянської свідомості та участі громадян у політичному житті. Тому держава має створювати умови для вільного доступу громадян до інформації та її обміну [1].

На основі цих теоретичних засад науковці визначаються основні принципи інформаційної політики держави:

1. Наявність державного суверенітету у інформаційній сфері, який визначає, що держава має забезпечувати суверенітет у інформаційній сфері, захищаючи національні інформаційні інтереси від негативного впливу ззовні.

2. Соціальна справедливість означає, що держава має забезпечувати доступ громадян до інформації незалежно від їх соціального статусу, політичних поглядів чи релігійних переконань.

3. Інформаційна відкритість, означає, що державні інститути мають забезпечувати відкритість інформаційної сфери, сприяючи взаємному обміну інформацією між державою, суспільством та окремими громадянами.

4. Ефективність, полягає у результативності інструментів інформаційної політики держави, вона має бути спрямованою на досягнення конкретних цілей і завдань. Ці принципи є основою для формування конкретних цілей, пріоритетів, заходів та механізмів інформаційної політики держави [4].

Виходячи з цього, основними цілями інформаційної політики держави можна визначити забезпечення інформаційної безпеки держави, сприяння розвитку інформаційної сфери, формування громадянської свідомості та забезпечення демократичного розвитку суспільства. Для досягнення цих цілей держава визначає ряд пріоритетів, які полягають в захисті національних інформаційних ресурсів від несанкціонованого доступу, використання та поширення, розвитку інформаційної інфраструктури, створенні умов для вільного доступу громадян до інформації, формуванні інформаційної культури суспільства [5].

На сьогоднішній день, реалізація пріоритетів інформаційної політики держава здійснюється через розробку та реалізацію нормативно-правового забезпечення інформаційної сфери, формування та розвиток інформаційних ресурсів, створення та підтримка інформаційних систем та технологій, пропаганда інформаційної культури. Такі дії можуть бути забезпечені через впровадження механізмів інформаційної політики шляхом створення системи органів, установ та організацій, які відповідають за її розроблення, реалізацію та контроль. До інститутів, що спроможні реалізувати механізми державної інформаційної політики належать:

- органи державної влади та управління;
- інформаційні агентства та засоби масової інформації;
- науково-дослідні установи;
- громадські організації [6].

Формування інформаційної політики держави — це складний і багатогранний процес, який вимагає системного підходу та врахування широкого спектру факторів. Теоретичні засади інформаційної політики держави є основою для її ефективного формування та реалізації. У багатьох

контекстах інформація сьогоді відіграє активну роль, яка стає все більш важливою з точки зору влади. Держава створює механізми регулювання інформаційної системи для того, щоб зберегти свою владу над великими групами економічної, соціальної, культурної та військової діяльності. Наприклад, мова йде про підтримку культурних стандартів суспільства через контроль над газетами та видавництвами, а також нав'язування державної мови меншинам, як єдиної мови, серед іншого [7].

На міжнародному рівні інформаційна система відіграє центральну роль з часів холодної війни, і зараз вона зосереджена на цілях так званої «війни проти тероризму». Її функція також є фундаментальною в економічному контролі та конкурентоспроможності підприємств, що застосовуються на міжнародних ринках. Однією з головних тенденцій у розвитку інформаційної політики останнім часом є, таким чином, боротьба з введення серйозних обмежень на свободу вираження поглядів, що є основою концепції демократії [8].

Сьогодні приватне життя людей стає все більш контрольованим, діяльність, переконання, судимості, а також інформація про зв'язки, переконання, різноманітні стосунки відстежуються, а дані про них зберігаються в системах баз даних, які можуть також включати, в деяких випадках, генетичну інформацію, таку як ДНК. Іншою тенденцією розвитку систем інформаційного нагляду є все більше включення в них цифрових систем інформаційного спостереження, оцифрованих карт та методів супутникової локалізації [9].

Важливо також відзначити, що нинішня превалююча позиція щодо обмежень свободи вираження поглядів не обмежується контролем над голосами людей або їх промовами, які ефективно виголошуються або поширюються будь-якими письмовими чи аудіовізуальними засобами комунікації. Вони також, включає «символічні дії», тобто будь-які дії або жести (наприклад, спалення прапора), які можуть бути витлумачені як підозрілі з точки зору встановленого порядку. Символічні дії також виявляються в культурних чи мистецьких творах або маніфестаціях. Одним із наслідків такого

бачення ролі інформації в системі влади стосується контролю між соціальними групами та різними суб'єктами, він не обмежуються геополітичними аспектами, а включає в себе економічну та соціальну діяльність, різні території за культурними, етнічними, релігійними чи будь-якими іншими критеріями [10].

Таким чином, ми доходимо до парадоксу: з одного боку, нові інформаційні технології, очевидно, пропонують можливість життя без кордонів (у багатьох його значеннях), але, з іншого боку, через політичні, дипломатичні, комерційні та військові причини, інформаційні системи використовуються існуючою владою для утримання зручних для неї кордонів, в тому числі і щодо пересування людей (особливо у випадку імміграції). Інший аспект стосується інформаційних механізмів на службі політичним інститутам та виборчим системам або системам голосування, які завжди вважались першочерговою умовою представницької демократії [11].

На додаток до маніпуляцій у місцевих виборчих процесах відбуваються маніпуляції в дослідженнях на користь передвиборчої кампанії того чи іншого кандидата, підозра в тому, що ці маніпуляції здійснюються за допомогою використання певних видів електронного голосування. Знову ж таки, спостерігається парадокс: з одного боку, нові інформаційні технології дозволяють децентралізацію, з великою свободою вираження поглядів, доступу до інформації та розповсюдження, але з іншого боку, нові інформаційні технології в певних контекстах є об'єктом маніпуляцій через певні політичні чи економічні чинники та корумповані, групові, егоїстичні інтереси [11].

Таким чином, спостерігається дуже швидкий процес посилення ролі інформації у діяльності владних систем, що перебувають під контролем держави. Фактично, науково-технічний прогрес, який характеризує інформаційні системи, з одного боку, робить можливим краще, адекватніше або точніше прийняття рішень та умови для економічних агентів, громадян, виборців та інших, але, з іншого боку, вони створюють кращі, адекватніші або точніші умови в контексті «війни з тероризмом», інформаційні системи формуються та орієнтуються на жорсткіший контроль за цивільною

інформацією. Сучасна «інформаційна держава» (держава, яка систематично використовує свої інформаційні системи для реалізації своєї політики) «дедалі більше знає про окремих громадян, але, з іншого боку, громадяни знають все менше і менше про державу» [14].

Інформаційна держава, в багатьох випадках, замінила стару «паноптику» на «панспектрон», з метою електронного спостереження за індивідами. Ще один висновок: «використання цифрових технологій обмежує, а не розширює, можливості для значної демократії участі». Незважаючи на те, що інформаційна система стає все більш потужною, вона не пропонує громадянам досконалої прозорості в політичному житті; навпаки, вона підживлює підозри щодо певних результатів виборів. Відбувається ще одна зміна: «в інформаційній державі індивід зникає як такий і перетворюється на ймовірність», тобто є статистично визначеним профілем. Таким чином, людина з певним профілем може розглядатися як підозрювана, навіть якщо вона ніколи не вчиняла жодного злочину [14].

1.2. Інформаційні ресурси, як об’єкт державного регулювання

Інформаційні ресурси, як об'єкт державного регулювання є важливим елементом розвитку сучасного суспільства, сьогодні вони відіграють вирішальну роль у всіх сферах життя, починаючи від економіки, політики, соціальної сфери, культури і завершуючи щоденною комунікацією між людьми. Державне регулювання інформаційних ресурсів спрямоване на те, щоб забезпечити їх ефективне використання, сформувати систему захисту від несанкціонованого доступу та поширення певних видів інформації, яка є державною або комерційною таємницею, а також на запобігання її використання в незаконних цілях [15].

Основними принципами державного регулювання інформаційних ресурсів є:

- доступність використання інформаційних ресурсів, які повинні бути доступні для всіх громадян України, незалежно від їх соціального статусу, місця проживання та інших обставин;

- захист, тобто інформаційні ресурси повинні бути захищені від несанкціонованого доступу, поширення та використання;

- якість, що визначається тим наскільки інформаційні ресурси є якісними та достовірними [15].

Основними завданнями державної політики в сфері використання інформаційних ресурсів є по-перше, створення умов для ефективного їх використання, захист інформаційних ресурсів від несанкціонованого доступу та поширення, забезпечення якісних характеристик та достовірності інформаційних ресурсів. Державне регулювання інформаційних ресурсів здійснюється шляхом прийняття нормативно-правових актів, створення відповідних інститутів, органів і організацій, які формують і реалізують державну інформаційну політику та стратегії, а також регуляторна роль держави полягає у проведенні інформаційно-просвітницької роботи тощо.

Основними нормативно-правовими актами, які регулюють відносини в сфері використання інформаційних ресурсів, є, насамперед Конституція України, а також Закон України «Про інформацію», «Про доступ до публічної інформації», «Про захист інформації в інформаційно-телекомунікаційних системах» та ряд інших підзаконних актів [4,5,7,8].

Що стосується інституційного забезпечення регуляторних дій держави в сфері використання інформаційних ресурсів, то вони включають Верховну Раду України, Кабінет Міністрів, Державну службу спеціального зв'язку та захисту інформації України, Службу безпеки України. Інформаційно-просвітницька робота в сфері інформаційних ресурсів спрямована на підвищення обізнаності громадян про їхні права та обов'язки в цій сфері. Таким чином, ефективне державне управління інформаційними ресурсами є вирішальним фактором, основою забезпечення інформаційної безпеки в Україні [17].

Структура інформаційних ресурсів може розглядатися з різних точок зору, за одним з підходів, структуру інформаційних ресурсів можна розкрити за такими ознаками. Так в залежності від форми подання, вони поділяються на документі, це інформаційні ресурси, які представлені у вигляді документів, а саме, книги, журнали, газети, патенти, нормативно-правові акти, наукові статті та недокументні інформаційні ресурси, які не представлені у вигляді документів. До них належать відомості, що містяться в пам'яті людей, а також інформаційні ресурси, представлені у вигляді кодів, програм, баз даних та інших електронних форм інформації [18].

В залежності від змісту інформації їх можна поділити на фактографічні інформаційні ресурси, які містять відомості про фактичні події, явища, особи тощо, до них належать довідники, енциклопедії, статистичні збірники, концептуальні інформаційні ресурси, які містять відомості про теорії, концепції, ідеї, це наукові статті, монографії, навчальні посібники, та творчі інформаційні ресурси ті, що містять відомості про художні твори, музику, кіно, до них відносяться книги, журнали, газети, пісні, фільми тощо. Інформаційні ресурси також можна класифікувати за призначенням, а саме, інформаційно-довідкові, це інформаційні ресурси, які призначені для надання інформації, до них відносяться довідники, енциклопедії, статистичні збірники, наукові інформаційні ресурси, що призначені для наукових досліджень, включають наукові статті, монографії та практичні інформаційні ресурси, які застосовуються у практичній діяльності, це нормативні документи, нормативні акти, керівні матеріали тощо [19].

Крім того, інформаційні ресурси залежать від сфери використання і їх можна представити в складі державних інформаційних ресурсів, це ті, що належать державі у вигляді законодавчих актів, нормативно-правових документів, державних програм. В свою чергу вони поділяються на публічні, які доступні для широкого загалу та непублічні інформаційні ресурси, доступ до яких обмежений, до них відносяться секретні документи, комерційна таємниця. В залежності від способу зберігання інфлрмаційні ресурси

поділяються на паперові, що зберігаються на папері та електронні інформаційні ресурси представлені у вигляді баз даних, веб-сайтів, електронних документів тощо. Цей перелік ознак не є вичерпним і може бути доповнений іншими ознаками, що дозволяють більш детально описати структуру інформаційних ресурсів [20].

В українському законодавстві нема повного визначення структурних елементів інформаційних ресурсів, вичерпних критеріїв їх кількісної оцінки, це створило певні складності в їх використанні в інформаційній політиці держави та правових регуляторах. У відповідності до Закону України «Про інформацію», права власності на інформаційні ресурси виникають наступними при створенні інформації, переході права власності на інформацію до інших осіб тощо.

Державні інформаційні ресурси, в умовах воєнної агресії, повинні відповідати ряду умов:

– чітка вирогідність, актуальність, надійність, реальність наведених даних, які мають бути підтверджені надійними джерелами;

– вичерпна повнота інформації, достатня кількість і якість даних, документів, посилань, що допомагають комплексно оцінити надану інформацію;

– компактність, зрозумілість і лаконічність, системність, доступність до інформації при належній організації управління;

– оперативність та ефективність користування інформацією тощо [13, с. 89].

Особливої ваги, в умовах воєнної агресії, набувають державні інструменти застосування електронних інформаційних ресурсів, завданнями яких є управління:

– утворенням та веденням Національних реєстрів, реєстрацією та обліком електронної інформації державного рівня, створенням та можливостями доступності до інформаційних ресурсів;

– упорядкуванням, забезпеченням доступу до державних електронних ресурсів та їх актуалізація;

– формуванням та гарантуванням ефективного їх використання органами державної влади;

– покращенням нормативно-правового поля, порядком і умовами користування та захистом ресурсів;

– погоджуванням діяльності органів публічної влади та бізнесом в сфері формування та захисту державних електронних інформаційних ресурсів [17].

Таким чином, інформаційні ресурси визнаються високим ступенем значимості для державного управління в умовах воєнного стану, оскільки вони є базою для прийняття ефективних управлінських рішень та національної безпеки. Сучасні інформаційні ресурси держави мають визначальне значення на економіку, науку, культуру, політику та інші галузі, отже, забезпечивши якість, об'єктивність, доступність, системність інформації, це інструмент підвищення ефективності політики держави в інформаційному середовищі, а в умовах воєнного стану та посилення інформаційної війни стратегічним чинником національної безпеки.

1.3. Особливості інформаційної політики держави в сучасних умовах

Інформаційна політика держави в умовах посиленні інформаційних небезпек і війн має ряд особливостей, які обумовлені характером цих процесів. Так, основна мета інформаційних війн – це вплив на суспільну думку, формування певних настроїв і цінностей в суспільстві, а також дискредитація противника. Для досягнення цих цілей використовуються різні інформаційні інструменти, такі як дезінформація, пропаганда, маніпуляція. У таких умовах інформаційна політика держави має мати спрямування на захисні функції та інформаційний суверенітет держави, захист інформаційного простору від несанкціонованого впливу ззовні, у формуванні позитивного іміджу країни в

міжнародних спільнотах, а це, в свою чергу, пов’язане з поширенням достовірної інформації про державу та її діяльність. Важливим завданням держави, в таких умовах є інформаційна безпека громадян, їх захист від впливу дезінформаціних та пропагандиських впливів [21].

Для реалізації цілей інформаційної політики держава повинна розробити і використовувати ряд заходів:

- створення ефективної системи захисту в інформаційному просторі держави, що включає в себе розвиток інформаційного інфраструктурного забезпечення, а також створення системи заходів з протидії інформаційним атакам, розвиток системи захисту засобів масової інформації, а також створення системи, яка б забезпечувала доступ громадян до достовірної інформації;

- розвиток національної системи в сфері інформаційної безпеки, це включає в себе підвищену обізнаність громадянського суспільства про інформаційні ризики, а також розвиток навичок критичного мислення [22].

Таким чином, можна на підставі вищевикладеного та враховуючи особливості інформаційної політики держави, в умовах посилення інформаційних небезпек та війн, сформулювати основні пріоритети регуляторних дій держави, спрямованих на захист інформаційного суверенітету держави, формування позитивного образу держави в міжнародній спільноті та забезпечення інформаційної безпеки громадян.

Інститути, що формують інформаційну політику повинні базуватись на принципах свободи слова, але при цьому повинна забезпечувати захист громадян від впливу дезінформації та пропаганди, дії інформаційної політики повинні бути спрямовані на розвиток національних інформаційних інфраструктурних платформ та підвищення обізнаності громадян про інформаційні ризики. В умовах сучасних інформаційних війн інформаційна політика держави є одним з ключових факторів забезпечення її безпеки та стабільності [23].

Сучасна система адміністрування інформаційною сферою – це процес, спрямований на реалізацію ефективної державної політики пов’язаною з використанням, розвитком і захистом інформаційних ресурсів держави. Її завданнями є повне забезпечення доступу до достовірної, об’єктивної, повної інформації, оптимальне використання сучасних інформаційних технологій управління та забезпечення інформаційної безпеки [24].

В сучасних умовах, інформація стала основним продуктом виробничих відносин і продовжує відігравати особливу роль в переході до інформаційно-інтелектуального суспільства, або суспільства, заснованого на знаннях, нині, таке суспільство, може функціонувати і розвиватись на основі ефективних інформаційно-комунікаційних технологій, які задовольняють потреби і інтереси не тільки окремих людей, але й мають велике значення для суспільства в цілому. Державні інститути, реагуючи на такі виклики, приймають норми та закони, що регулюють діяльність, пов'язану з використанням інформації, вони формують інформаційну політику, але не завжди ефективну, оскільки вона залежить як від рівня розвитку самої державної інституції, так і від розвитку інформаційних технологій [25].

Слід зазначити, що традиційно саме постіндустріальні держави є найбільш розвиненими в цьому плані, сучасні наукові дослідження здебільшого зосереджені на вивченні індикаторів впливу розвитку інформаційних технологій на темпи розвитку держави, вони є свідченням її впливовості на міжнародній арені. Проблема взаємозв'язку інформаційної політики з показниками розвитку держави, а також особливостей інформаційної політики, на наш погляд, значною мірою залишається поза увагою світової дослідницької спільноти.

Інформаційна політика, яка виникла в останні десятиліття 20-го століття, виокремившись в окрему галузь, сьогодні стала одним із проявів переходу від індустріального суспільства інформаційно-інтелектуального. Задля безпеки населення, державним органам влади, важливо контролювати таку діяльність, з цією метою в структурі загальної державної політики, потрібно посилити

інформаційну складову. Класичне визначення інформаційної політики, що охоплювало питання доступу до урядової інформації і, фактично базувалось на пропагандистських заходах, в сучасних умовах трансформується в ідею розробки всеосяжної національної інформаційної політики, це переломний момент в оцінці важливості інформаційної політики, адже. вона створює умови, за яких відбувається прийняття рішень, публічний дискурс та політична діяльність [26].

Сучасна Концепція національної всеосяжної інформаційної політики стає можливою лише завдяки тому, що політичні лідери в усьому світі визнали, що закони, які регулюють інформаційну сферу, насправді є питаннями стратегічного значення. Однак, сьогодні, небагато урядів впровадили єдину інформаційну політику, але, незважаючи на це, інтенсивність формування інформаційної політики продовжувала зростати в усьому світі. Всеосяжна інформаційна політики спроможна стимулювати розвиток технологій до такої міри, що державні урядові органи стали активно заохочувати наукові дослідження та розробки в цій галузі [27].

Оскільки розвиток і поширення інновацій в інформаційній сфері збільшився, сучасна інформаційна політика зумовлена розвитком технологій, а отже, відходить від традиційних поглядів. Таким чином, інформаційну політику почали, в умовах зростання національних загроз, використовувати для позначення політичних ініціатив, що сприяють використанню інструментів і концепцій, пов'язаних з глобальним інформаційним суспільством, з метою реалізації їх потенціалу в досягненні цілей національного, соціального та економічного розвитку [29].

Висновки до розділу 1

Беручи до уваги інформацію яка зазначена вище, можна підкреслити що, управління інформаційними ресурсами держави у сфері інформаційної безпеки

є невід’ємною складовою ефективного функціонування сучасного суспільства. Це включає в себе впровадження технологічних заходів, розробку стратегій та політик, які спрямовані на забезпечення конфіденційності, цілісності та доступності інформації державних інформаційних ресурсів. Основні завдання управління включають реалізацію ефективних заходів кіберзахисту, розробку політики безпеки та створення інфраструктури, яка забезпечує відповідність вимогам сучасного цифрового середовища. Ці заходи не лише забезпечують захист інформаційних ресурсів держави, але й сприяють підвищенню рівня прозорості, демократії та ефективності державного управління в цілому.

РОЗДІЛ 2.
АНАЛІЗ МЕХАНІЗМІВ ДЕРЖАВНОГО УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ РЕСУРСАМИ УКРАЇНИ

2.1. Характеристика механізмів управління інформаційними ресурсами

Сучасні механізми державного управління інформаційними ресурсами України становлять сукупність методів, засобів і процедур, що використовуються органами державної влади для реалізації державної інформаційної політики. Ці механізми спрямовані на забезпечення ефективного використання інформаційних ресурсів, захисту інформаційної безпеки держави та суспільства, а також створення умов для розвитку інформаційного суспільства.

До основних механізмів державного управління інформаційними ресурсами України належить, перш за все, нормативно-правове регулювання, яке передбачає прийняття законодавчих актів, які визначають правові основи функціонування інформаційного простору України, права та обов'язки суб'єктів інформаційних відносин, а також порядок регулювання інформаційного простору. На сьогоднішній день, нормативно-правове регулювання інформаційної сфери в Україні здійснюється Конституцією України, законами України «Про інформацію», «Про телебачення і радіомовлення», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про державну таємницю» та іншими нормативно-правовими актами [7,9,11,21].

Провідним інструментом, в системі механізмів публічного управління інформацією, є державне фінансування, що передбачає виділяння коштів з державного бюджету на розвиток інформаційної сфери, зокрема на створення інфраструктури, розвиток інформаційних технологій, а також на підтримку вітчизняного інформаційного продукту та залучення альтернативних фінансових ресурсів для реалізації інформаційної політики держави. Досвід

демократичних країн показує, що лише повне державне фінансування інформаційного середовища в стратегічно важливих сферах, забезпечило ефективність реалізації політики держави. Фінансування розвитку інформаційної сфери в Україні реалізується за рахунок коштів державного бюджету, місцевих бюджетів, а також за рахунок коштів підприємств, установ та організацій [29].

Залишається вагомим механізмом, який перейшов в спадщину від радянської системи, адміністративне регулювання, яке, в сучасних умовах суттєво змінило форми в напряму партисипації. Цей механізм передбачає здійснення органами державної влади контролю за дотриманням законодавства в інформаційній сфері, а також надання адміністративних послуг у сфері інформаційних відносин [30].

Адміністративне регулювання інформаційної сфери в Україні здійснюється органами державної влади, зокрема Кабінетом Міністрів України, Державною службою спеціального зв'язку та захисту інформації України, Міністерством культури та інформаційної політики України та іншими органами. Окрім того, в реалізації механізмів державного управління інформаційними ресурсами України приймають участь не лише органи державної влади, але і інші суб'єкти інформаційних відносин, зокрема підприємства, громадські об'єднання та пересічні громадянами [31].

Вищеназвані інструменти забезпечують розробку та реалізацію державної політики в інформаційній сфері, яка визначає цілі, завдання та пріоритети розвитку інформаційного простору України. Інформаційна політика держави в Україні визначається Указом Президента України «Про Стратегію національної безпеки України» та іншими документами [32].

В Україні інформаційна політика має три основні рівні, а саме, інфраструктурна політика, пов'язана з розвитком національної інфраструктури, необхідної для підтримки інформаційного суспільства. Вертикальна інформаційна політика, включає політичні дії в галузі освіти, туризму, виробництва, охорони здоров'я та горизонтальна інформаційна політика – це

політика, яка впливає на різні аспекти життя суспільства, наприклад, політика, пов'язана зі свободою інформації, тарифами та ціноутворенням, а також використанням ІКТ урядом всередині країни та у відносинах з іншими країнами [33].

Умови воєнного стану створюють суттєві виклики для управління інформаційною безпекою держави. Аналіз управління в цих умовах включає кілька ключових аспектів:

1. Кіберзахист та кібервійська безпека. Умови воєнного стану можуть підвищити загрозу кібератак та кібервійництва. Управління інформаційною безпекою повинно включати розширені заходи кіберзахисту, виявлення та протидії кібернападам, а також вдосконалення інфраструктури для захисту критичних інформаційних систем.

2. Забезпечення зв’язку та інформаційної доступності. Забезпечення надійного і безперебійного зв’язку стає пріоритетом для забезпечення ефективної комунікації та обміну інформацією між військовими, правоохоронними та цивільними структурами. Це може включати розробку резервних систем і засобів зв’язку.

3. Стратегічне управління інформацією. З урахуванням воєнних загроз інформаційне управління повинно бути орієнтоване на забезпечення безпеки критичної інформації та вдосконалення стратегій обробки, аналізу та розповсюдження важливої інформації для державних органів та військових підрозділів.

4. Роль громадськості та медіа. Важливо враховувати роль громадськості та медіа в умовах воєнного стану. Забезпечення точної та об’єктивної інформації, а також взаємодія з громадськістю, може бути критичним для підтримки національного єднання та реагування на інформаційні загрози.

5. Етичні та правові аспекти [34].

2.2 Оцінка напрямів імплементації Доктрини інформаційної безпеки України

Російська інформаційна агресія та епідемія медійних фейків, що поширюються по всьому світу, викликали серйозну необхідність реагувати на ці явища в Європі на глобальному рівні. Європейський Парламент усвідомив це з прийняттям власної резолюції про боротьбу з антиєвропейською пропагандою, поширеною в усьому ЄС, і відобразив основні принципи цієї протидії в Документі під назвою «Європейська стратегічна комунікація для протидії пропаганді проти неї третіми сторонами», прийнятому 23 листопада 2016 року. Наслідуючи приклад Європейського Парламенту та відповідаючи на виклики сьогоднішнього дня в Україні, Указом Президента України No 47/2017 від 25 лютого 2017 року було затверджено Доктрину інформаційної безпеки України (далі – Доктрина) [35].

Ця Доктрина визначає національні інтереси України в інформаційній сфері, загрози їх реалізації, напрями та пріоритети державної політики в інформаційній сфері. Документ конкретизує принципи формування та впровадження державної інформаційної політики, передусім щодо протидії деструктивному впливу інформації російської федерації в умовах гібридної війни, яку вона розпочала, використовуючи останні інформаційні технології. Ці технології спрямовані на вплив на свідомість громадян та на спровокування етнічної та релігійної ненависті, пропаганду агресивної війни, вторгнення в конституційний лад чи будь-яке порушення суверенітету чи територіальної цілісності України [36].

Доктрина ґрунтується на принципах поваги прав та свобод громадян, людської гідності, захисту законних інтересів особистості, суспільства та держави, забезпечення суверенітету та територіальної цілісності України. У впровадженні Доктрини безпосередньо беруть участь такі органи публічної влади як Національна рада безпеки і оборони України; Кабінет Міністрів України; Міністерство інформаційної політики України; Міністерство закордонних справ України; Міністерство оборони України; Міністерство

культури України; Українське державне агентство кіно; Національна рада з питань телебачення і радіомовлення України; Державний комітет телебачення і радіомовлення України; Служба безпеки України; розвідувальні агентства України; Державна служба спеціального зв'язку та захисту інформації України; Національний інститут стратегічних досліджень [37].

Основними принципами реалізації доктрини є верховенство права; пріоритетність захисту прав і свобод людини в інформаційній сфері, своєчасний і адекватний захист життєво важливих національних інтересів від реальних та потенційних загроз інформаційній безпеці. Також, основні принципи доктрини орієнтовані на своєчасний і адекватний захист життєво важливих національних інтересів від реальних та потенційних захист інформаційного суверенітету України; свободу думки, свободу слова та вільного вираження поглядів і переконань [38].

Важливого значення набуває свобода збирання, зберігання, використання і поширення інформації, захист від втручання в особисте і сімейне життя особи, доступ до інформації лише на підставі закону, гармонізація особистих, суспільних і національних інтересів. В ній зроблено акценти на відповідальності всього українського народу та влади за забезпечення інформаційної безпеки, що потребує розмежування повноважень, взаємодії та відповідальності держави і недержавних суб'єктів забезпечення інформаційної безпеки, пріоритетності розвитку та поширення інформаційних технологій, продуктів і послуг, постійне вдосконалення каналів передачі інформації.

Інформаційні ресурси в Доктрині оцінюються з точки зору їх кількості та технічності, використання міжнародних та колективних систем і механізмів безпеки, гармонізації інформаційного законодавства з нормами міжнародного права та нормативно-правовими актами Європейського Союзу, захисту інформаційного суверенітету, національного суверенітету, конституційного ладу і територіальної цілісності України. Зроблено акцент на формуванні української ідентичності в інформаційному просторі, яка є невід'ємною частиною суспільно-політичного процесу [31].

Розбудова дуальної системи суспільного та комерційного мовлення та сприяння розвитку в інформаційному просторі контенту, спрямованого на утвердження та захист загальнолюдських цінностей, а також інтелектуального, духовного і культурного потенціалу українського народу теж є пріоритетами та визначають основні напрями державної політики у сфері інформаційної безпеки України, а саме:

- дотримання балансу між неухильним дотриманням конституційних прав і свобод людини і громадянина в інформаційній сфері, зокрема свободи слова, та виконання державних функцій у частині запобігання, своєчасного виявлення, знешкодження, усунення або нейтралізації загроз в інформаційній безпеці людини і громадянина, суспільства і держави;

- створення нормативно-правової бази для організації розвитку інформаційного простору та його захисту від зовнішніх загроз, а також приведення такої нормативно-правової бази у відповідність з нормами міжнародного права, міжнародними договорами України, вимогами міжнародного співробітництва та стандартами і регламентами ЄС;

- формування та реалізація ефективної державної інформаційної політики, спрямованої на розвиток національного інформаційного простору та гармонізацію системи контролю і координації між суб'єктами національної інформаційної політики та практики;

- налагодження співпраці між урядом, громадським сектором та приватним сектором, сприяння міжнародному співробітництву з метою реалізації національної інформаційної політики та забезпечення інформаційної безпеки, формування якісного національного інформаційного продукту;

- всебічне сприяння, державна підтримка та пріоритетність створення та розповсюдження національного інформаційного продукту, у тому числі за межами України, для популяризації загальнолюдських цінностей у міжнародному інформаційному просторі та інформаційному розвитку людства, зокрема обмін із зарубіжними партнерами України баченням, підходами та механізмами розв'язання сучасних викликів, що постають перед людством [34].

2.3. Особливості інституційного забезпечення управління інформаційними ресурсами

Інформаційна політика в стратегічних документах, її основні положення та цілі реалізуються через корпус нормативних актів, дію урядових структур, органів місцевого самоврядування, які визначають її інституційне забезпечення. Так, відповідальність за розробку та впровадження нормативних актів лежить на фахівцях, які беруть участь у забезпеченні інформаційної політики та стійкого інформаційного розвитку, як це визначено в стратегічних цілях центральних виконавчих органів, що відповідають за виконання національної інформаційної політики, вживають заходів для забезпечення цілісності та послідовності політики щодо забезпечення інформаційної безпеки та захисту інформаційного суверенітету України [35].

Вони розробляють та подають на розгляд Кабінету Міністрів України пропозиції щодо розробки, затвердження та впровадження нормативно-правових актів, що спрямовують і координують інформаційні діяльність Кабінету Міністрів України, Прем'єр-міністра України, членів Кабінету Міністрів України, міністерств та інших центральних органів виконавчої влади та їхніх посадових осіб, а також Антимонопольного комітету України, державного майна Фонду України та їхніх посадових осіб. Також, державні інститути в сфері інформаційної політики, подають на розгляд Ради національної безпеки і оборони України пропозиції щодо розробки, затвердження та впровадження нормативних актів, що спрямовують і координують інформаційну діяльність Президента України, Ради національної безпеки і оборони України, Міністерства оборони України, Верховного Головнокомандування Збройних Сил України, Міністерства закордонних справ України, Служби безпеки України, Національного бюро з протидії корупції України, Державної прикордонної служби України, розвідувальних та іноземних розвідувальних органів, місцевих державних адміністрацій [36].

Центральний виконавчий орган, що відповідає за виконання національної інформаційної політики, розробляє та подає на розгляд Національному банку України та Генеральній прокуратурі України пропозиції щодо розробки, затвердження та впровадження нормативно-правових актів, що регулюють їхню інформаційну діяльність. Кабінет Міністрів України, Рада національної безпеки і оборони України, Національний банк України та Генеральна прокуратура України розглядають пропозиції центрального урядового органу, відповідального за виконання національної інформаційної політики, та ухвалюють відповідні рішення в межах своїх повноважень та компетенції [37].

Виконавчі органи, що діють як практики національної інформаційної безпеки, забезпечують виконання Концепції відповідно до розпоряджень Кабінету Міністрів України та Ради національної безпеки і оборони України, прийнятих на основі пропозицій центрального виконавчого органу, відповідального за виконання національної інформаційної політики. Центральний виконавчий орган, що відповідає за виконання національної інформаційної політики, приймає та розглядає заяви інших державних органів, громадян України та не урядових організацій для їх розгляду в процесі розробки пропозицій Кабінету Міністрів України та інших виконавчих органів.

Висновки до 2 розділу

Розробка та реалізація зазначених програм є невід'ємною частиною обов'язків практиків, які беруть участь у забезпеченні інформаційної безпеки та стійкого інформаційного розвитку України. Контроль за дотриманням виконання зазначених документів та їхньої узгодженості між собою за цілями та напрямками діяльності покладається на органи, відповідальні за координацію та моніторинг стійкого інформаційного розвитку та інформаційної безпеки України відповідно до цієї Концепції.

РОЗДІЛ 3.
НАПРЯМИ УДОСКОНАЛЕННЯ ІНФОРМАЦІЙНОЇ ПОЛІТИКИ ДЕРЖАВИ В УМОВАХ ВОЄННОГО СТАНУ

3.1. Шляхи імплементації зарубіжного досвіду публічного управління у сфері інформаційної безпеки

В сучасному світі, IT-технології інтегровані майже в кожну сферу повсякденного життя, а тому системи підключені до критичних систем, які безпосередньо впливають на наш економічний добробут, заробітки та навіть здоров'я, починаючи від управління особистим ідентифікатором до медичної допомоги. Небезпечна технологія та уразливості в критичних системах можуть приваблювати шкідливі кібер-вторгнення, що призводить до серйозних потенційних ризиків для безпеки. Можна навести приклад, де кібер-порушення призвели до скасування госпіталями операцій та перенаправлення догляду за пацієнтами по всьому світу [32].

Нині, як ніколи раніше, на думку публічних органів США, Канади, Австралії, країн Євросоюзу, технічні виробники повинні зробити «Secure-by-Design» і «Secure-by-Default» центральними точками процесів проектування та розробки продуктів. Деякі постачальники зробили великі кроки вперед, просуваючи галузь у сфері гарантії програмного забезпечення, тоді як інші відстають [21].

Національні агентства наголошують на тому, що кожний технологічний виробник повинен будувати свої продукти таким чином, щоб споживачі не мали постійно виконувати моніторинг, регулярні оновлення та ліквідацію збитків на своїх системах для пом'якшення кібер-вторгнень. Виробникам заохочують взяти на себе відповідальність за поліпшення результатів безпеки своїх клієнтів.

Історично склалося так, що технічні виробники покладалися на виправлення вразливостей, виявлених після розгортання продуктів клієнтами, вимагаючи від клієнтів застосовувати ці патчі за власний рахунок. Лише

шляхом інтеграції практик «Secure-by-Design», зламано порочне коло створення та застосування виправлень. Щоб досягти такого високого стандарту безпеки програмного забезпечення, авторські агентства заохочують виробників пріоритизувати інтеграцію безпеки продуктів як критичну передумову для функцій та швидкості виходу на ринок [38].

З часом інженерні команди зможуть встановити новий ритм рівноважного стану, в якому безпека дійсно вбудовується та вимагає менше зусиль для підтримки. Відображаючи цю перспективу, Європейський Союз підкреслює важливість безпеки продуктів у Директиві про кіберстійкість, наголошуючи на тому, що виробники повинні реалізовувати безпеку протягом усього життєвого циклу продукту, щоб запобігти введенню виробниками вразливих продуктів на ринок. Щоб створити майбутнє, де технологія та пов'язані з нею продукти є безпечнішими для споживачів, авторські агентства закликають виробників переробити свої програми проектування та розробки, щоб дозволити доставляти лише продукти «Безпека за дизайном» та «Безпека за замовчуванням» [32].

Програма *«Secure-by-Design» («Безпека за дизайном»)* означає, що технологічні продукти розробляються таким чином, щоб захистити їх від успішного доступу зловмисних кіберактрів до пристроїв даних та підключеної інфраструктури. Виробники програмного забезпечення повинні провести оцінку ризиків, щоб ідентифікувати та перелічити поширені кіберзагрози для критичних систем, а потім включити захист у проектні креслення продуктів, які враховують мінливу ситуацію з кіберзагрозами [32].

Програма *«Secure-by-Default» («Безпека за замовчуванням»)* означає, що продукти є стійкими до поширених методів експлуатації без додаткової плати. Ці продукти захищають від найпоширеніших загроз і вразливостей, і кінцевим користувачам не потрібно додатково їх захищати. Продукти Secure-by-Default розроблені так, щоб клієнти чітко усвідомлювати, що коли вони відхиляються від безпечних параметрів за замовчуванням, вони збільшують ймовірність компрометації, якщо не впровадять додаткові заходи [34].

Агентство з кібербезпеки іннфраструктури США (CISA), Національне агентство безпеки США (NSA), ФБР та наступні міжнародні партнери : Австралійський Центр кібербезпеки (ACSC), Канадський центр кібербезпеки (CCCS), Національний центр кібербезпеки Сполученого Королівства (NCSC-UK), Федеральний офіс безпеки інформації Німеччини (BSI), Національний центр кібербезпеки Нідерландів (NCSC-NL), Команда реагування на комп'ютерні надзвичайні ситуації Нової Зеландії (CERT NZ) та Національний центр кібербезпеки Нової Зеландії (NCSC-NZ) надають рекомендації для виробників технологій для забезпечення безпеки їх продуктів [31].

Вказані агентства визнають внесок багатьох приватних партнерів у просуванні безпеки за дизайном і за замовчуванням. Це має на меті просунути міжнародну дискусію про ключові пріоритети, інвестиції та рішення, необхідні для досягнення майбутнього, в яких технологія є безпечною, захищеною та стійкою за дизайном і за замовчуванням. Для цього авторські агентства шукають відгуки на цей продукт від зацікавлених сторін та мають намір провести серію слухань для подальшого уточнення, конкретизації та просування наших рекомендацій для досягнення наших спільних цілей.

3.2. Інструменти удосконалення управління інформаційною політикою в умовах воєнного стану

Управління інформаційною політикою в умовах воєнного стану має ряд особливостей, які вимагають удосконалення існуючих механізмів та розробки нових підходів. Однією з основних особливостей є зростаюча роль інформаційних технологій у веденні війни, так інтернет, соціальні мережі, а також інші цифрові платформи стали важливими інструментами пропаганди та дезінформації. Це вимагає від органів державної влади посилення протидії цим загрозам.

Іншою особливістю є необхідність забезпечення інформаційної безпеки країни, в умовах воєнного стану інформація є цінним ресурсом, який може використовуватися як для захисту, так і для нападу, тому важливо забезпечити захист інформації від несанкціонованого доступу, поширення та використання. Нарешті, необхідно враховувати інтереси всіх суб'єктів інформаційних відносин, зокрема громадян, ЗМІ та органів державної влади. Умови воєнного стану не повинні призводити до обмеження свободи слова та доступу до інформації [38].

На основі цих особливостей можна виділити наступні шляхи удосконалення управління інформаційною політикою в умовах воєнного стану:

- посилення протидії дезінформації та пропаганді, що передбачає розробку та реалізацію ефективних механізмів виявлення та протидії поширенню дезінформації та пропаганди, зокрема в соціальних мережах та інших цифрових платформах;

- забезпечення інформаційної безпеки країни, через розробку та реалізацію заходів щодо захисту інформації від несанкціонованого доступу, поширення та використання, зокрема інформації про оборону, державну таємницю та інших важливих об'єктів;

- балансування інтересів всіх суб'єктів інформаційних відносин, шляхом створення умов для реалізації свободи слова та доступу до інформації, а також для захисту прав і свобод громадян, ЗМІ та органів державної влади [39].

Конкретизуючи ці заходи, які можуть бути реалізовані в рамках визначених шляхів, ми вважаємо за необхідне вдосконалити нормативно-правове регулювання інформаційної сфери, через уточнення та доповнення існуючих нормативно-правових актів, а також розробку нового, адаптованого до сучасних реалій законодавства. На нашу думку, є гостра потреба у створенні єдиного центру протидії дезінформації та пропаганді, діяльність якого може об'єднати зусилля різних органів державної влади, ЗМІ та громадських організацій.

Необхідно створити принципово нову систему захисту інформації від несанкціонованого доступу, поширення та використання, вона повинна включати в себе як технічні, так і організаційні заходи в напряму посилення інформаційної безпеки. Розробити механізми громадського контролю за діяльністю органів державної влади в інформаційній сфері, що дозволить забезпечити прозорість і відповідальність органів державної влади за свою діяльність. Реалізація цих заходів дозволить підвищити ефективність управління інформаційною політикою в умовах воєнного стану та забезпечити захист інформаційної безпеки країни [40].

Сучасний розвиток галузі кібербезпеки свідчить про необхідність розробки нових та модифікації існуючих програмних документів, які визначають діяльність державних органів, відповідальних за інформаційну безпеку, вони повинні бути зосереджені на напрямах:

- забезпечення сталого розвитку інформаційного простору України таким чином, щоб такий інформаційного простору України з тим, щоб такий простір був здатний протидіяти зовнішнім і внутрішнім загрозам;

- створення та функціонування системи захисту інформаційного простору України від загроз;

- забезпечення сталого розвитку інформаційного простору України з метою протидії зовнішнім і внутрішнім загрозам інформаційного простору України від загроз [41].

Інформаційна політика України має діяти в напряму задоволення життєво важливих для інформаційного простору України інтересів і потреб громадянина, суспільства та держави. Розробка стратегічного контенту, як національного інформаційного продукту має бути спрямована на підтримку політичної, культурної та духовної цілісності та розвитку політичної нації. Стратегічно важливі національного рівня документи, наприклад Концепція інформаційної безпеки повинні бути також спрямовані на створення передумов для розвитку інформаційного потенціалу України з метою забезпечення

швидкого зростання без негативних зовнішніх ефектів, що не створюють реальних ризиків національній інформаційній безпеці [35].

Основною завданням системи інформаційної безпеки є підтримання такого розвитку, який сприятиме запобіганню негативних наслідків втручання третіх сторін. На нашу думку, такий підхід може бути реалізований на практиці лише за умови залучення всіх внутрішніх учасників інформаційних відносин та ефективної співпраці між державою, громадянським суспільством, приватним сектором та окремими громадянами задля розвитку інформаційного простору та його спільного захисту від зовнішніх загроз [40].

Метою наших рекомендацій є інноваційне забезпечення інформаційного суверенітету та визначення підходів до захисту національного інформаційного простору. Оскільки інформаційна безпека – це захищеність життєво важливих інтересів людини, громадянина суспільства і держави, потрібно унеможливливити заподіяння шкоди від надання неповної, недостовірної, застарілої інформації, порушення цілісності та доступності інформації, несанкціонованого поширення інформації з обмеженим доступом, а також негативного інформаційно-психологічного впливу та умисне заподіяння негативних наслідків застосування інформаційних технологій [41].

Україні спільно з зарубіжними партнерами, в сфері інформаційної безпеки, потрібно протидіяти сучасним викликам, спровокованим деструктивною політикою інших країн, спрямованою на підрив в країні демократичних цінностей та свободи вираження поглядів в інформаційному просторі. На даний час, загрозами інформаційній безпеці України є наступні:

- загрози у сфері комунікацій, пов'язані із забезпеченням потреб людини і громадянина, суспільства і держави у виробництві, споживанні, поширенні та розвитку національного стратегічного контенту та інформації;

- технологічні загрози, пов'язані з функціонуванням та безпекою кібернетичних телекомунікаційних та інших автоматизованих комп'ютерних систем, що утворюють інфраструктурну (технічну, інструментальну) основу національного інформаційного простору [39].

Загрозами у сфері комунікацій, які пов'язані із забезпеченням потреб людини, громадянина, суспільства та людини, громадянина, суспільства і держави у виробництві, споживанні, поширенні та розвитку національного стратегічного контенту та інформації є :

а) зовнішній негативний інформаційний вплив на свідомість людини і суспільства через засоби масової інформації та мережу Інтернет, що здійснюється на шкоду державі з метою намагання змінити психічний або емоційний стан людини, її психологічні та фізіологічні характеристики;

б) впливу на свободу вибору шляхом культивування культури насильства та жорстокості, зухвалості та неповаги до людської та національної гідності, розпалювання релігійної, расової, національної ненависті та дискримінації за будь-якою ознакою - етнічним походженням, мовою, релігією тощо заклики до сепаратизму, повалення конституційного ладу або порушення територіальної цілісності до сепаратизму, повалення конституційного ладу або порушення територіальної цілісності країни;

в) інформаційний вплив на населення України, у тому числі на військовослужбовців та мобілізаційного резерву, з метою зниження обороноздатності та підриву іміджу служби в армії;

г) поширення суб'єктами інформаційної діяльності викривленої, недостовірної та упередженої інформації з метою дискредитації органів державної влади інформаційної діяльності з метою дискредитації органів державної влади та дестабілізації суспільно-політичної ситуації, що суттєво ускладнює прийняття політичних рішень обстановку, істотно ускладнює прийняття політичних рішень, завдає шкоди національним інтересам або створює негативний імідж України [37].

Загрози свободі слова полягають у наступному:

- втручання власників ЗМІ у редакційну політику;

- відсутність законодавчої бази для посилення ролі творчих колективів та редакцій у здійсненні редакційної політики ЗМІ, як державних, так і приватних;

-медіа-монополізм, що дозволяє здійснювати цілеспрямований вплив на споживачів інформації;

- адміністративні та регуляторні передумови, створені для обмеження свободи слова та маніпулювання громадською думкою як під зовнішнім впливом, так і громадською думкою як під зовнішнім впливом, так і з боку внутрішніх політичних організацій, бізнесу та окремих осіб;

- створення, поширення, передача та зберігання інформації з метою підтримки або інтенсифікації злочинної або терористичної діяльності [34].

Технологічними загрозами, які пов’язуються з функціонуванням та безпекою кібернетичних, телекомунікаційних та інших автоматизованих комп'ютерних систем, що утворюють інфраструктурну (технічну, інструментальну) основу національного інформаційного простору, є:

а) застосування іноземними державами кібернетичних сил, кібернетичних підрозділів, нових видів інформаційної зброї та кібернетичних засобів ураження на шкоду національному інформаційному простору України;

б) акти кіберзлочинності, тероризму або військової кіберагресії, що створюють загрозу стабільному функціонуванню національних інформаційно-телекомунікаційних систем, вчинені шляхом втручання, несанкціонованого доступу або порушення функціонування телекомунікаційних, кібернетичних та автоматизованих комп'ютерних систем, державних або приватних, з метою здійснення актів саботажу або тероризму підтримки або активізації злочинної, екстремістської або терористичної діяльності здійснення деструктивного інформаційного впливу перехоплення телекомунікацій;

в) радіоелектронне придушення або блокування інформаційних систем, засобів зв'язку та управління з використанням програмних і математичних засобів, що порушують функціонування інформаційних систем;

г) додавання до програмних і технічних засобів прихованих шкідливих функцій;

д) нерозвиненість національної інформаційної інфраструктури, зокрема залежність національної інформаційної інфраструктури від іноземних виробників високотехнологічної продукції;

е) використання контрафактного та несертифікованого програмного забезпечення та обладнання для обробки інформації;

ж) невідповідність норм, що регулюють відповідальність за вчинені правопорушення, сучасним викликам і загрозам інформаційній безпеці;

з) недостатній рівень захисту об'єктів критичної інформаційної інфраструктури України [32].

Висновки до 3 розділу

Таким чином, порушення порядку доступу, поводження, збирання, оброблення, зберігання поширення або передачі інформації, що охороняється державою (державна таємниця, конфіденційна інформація, персональні дані, об'єкти авторського права та інтелектуальної власності) або операцій з інформаційними ресурсами, що містять таку інформацію є актуальною загрозою реалізації інформаційної політики держави в умовах воєнного стану. Потрібно впровадити інноваційні інструменти управління і технології державного контролю за діяльністю суб'єктів забезпечення інформаційної безпеки, практиків, безпекою національної інформаційної інфраструктури та інформаційного простору.

ВИСНОВКИ

Аналіз механізмів державної інформаційної політики України в умовах воєнного стану дозволяє зробити наступні висновки:

1. Нормативно-правове регулювання інформаційної сфери в Україні є достатнім для забезпечення ефективного функціонування інформаційного простору країни в умовах воєнно-політичної кризи, але разом з тим, ряд нормативно-правових актів потребує уточнення, доповнення та приведенні у відповідність до міжнародних стандартів та вимог часу.

2. Фінансування розвитку інформаційної сфери в Україні є недостатнім для забезпечення реалізації всіх завдань і пріоритетів державної інформаційної політики враховуючи економічно-фінансову кризу в країні і велику потребу у зовнішніх запозиченнях, тому необхідно максимально залучити усі зацікавлені сторони до пошуку нових джерел фінансування, в першу чергу, за рахунок розвитку державно-приватного партнерства.

3. Вимоги воєнного часу вимагають посилення адміністративного регулювання інформаційною сферою України та ефективного застосування норм міжнародного законодавства в інформаційній сфері, необхідно посилити контроль за дотриманням законодавства в соціальних мережах та інших цифрових платформах.

4. Інформаційна політика держави в Україні спрямована на розвиток інформаційного суспільства та забезпечення інформаційної безпеки країни, однак, необхідно більш детально визначити цілі, завдання та пріоритети державної інформаційної політики. Для цього потрібно підвищити ефективність механізмів державного управління інформаційними ресурсами України.

5. Інформаційні ресурси є важливим об’єктом інформаційної політики держави, вони є основою для розвитку інформаційного простору та забезпечення національної безпеки. Тому, механізми публічного управління в сфері інформації, в умовах воєнних загроз, мають бути зосереджені на

підтримці національних інтересів, прав та свобод людини, ефективне функціонування органів державної влади та інститутів громадянського суспільства, які є регуляторами інформаційних відносин.

6. Вимоги сьогодення вимагають впровадження нових технологій управління на засадах партисипації, оновлення інформаційної стратегії та політики на всіх рівнях адміністрування, забезпечення більшого ступеня конфіденційності у використанні інформаційних ресурсів. Управлінські новації мають передбачати ефективні заходи кіберзахисту, розробки інструментів безпеки та розвиток інфраструктури.

6. Зарубіжний досвід публічного управління інформаційним середовищем держави показав важливість поєднання технологічних інновацій, стратегічного планування та ефективних політичних рішень для забезпечення стійкості національної кібер-інфраструктури.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Довгань О.Д. Інформаційні ресурси: національні та державні, зміст, поняття. *Інформація і право*. 2015. №3. С. 85–91.

2. Єрменчук О. П. Складові національної інфраструктури. Науковий вісник ДДУВС. 2017. № 4. С. 109–115.

3. 8. Єрменчук О.П. Основні підходи до організації захисту критичної інфраструктури в країнах Європи: досвід для України: монограф. Дніпро: Дніпроп. держ. ун-т внутр. справ, 2018. 180 с.

4. Клочко А. Забезпечення інформаційної безпеки в умовах сучасного суспільства. *Наукові праці Міжрегіональної Академії управління персоналом. Політичні науки та публічне управління*. 2022. №3(63). С. 38–42. URL: https://doi.org/10.32689/2523-4625-2022-3(63)-6 (дата звернення: 29.11.2023).

5. Конституція України, прийнята на п’ятій сесії Верховної Ради України 28 червня 1996 р. / Верховна Рада України. Київ: Преса України, 1997. 80 с.

6. Концепція створення та функціонування інформаційної системи електронної взаємодії державних електронних інформаційних ресурсів : Розпорядження Кабінету Міністрів України від 05.09.12 р. № 634-р. URL : http://zakon2.rada.gov.ua/laws/show/634-2012-%D1%80 (дата звернення: 24.11.2023).

7. Кормич Б.А. Організаційно-правові основи політики інформаційної безпеки України : дис. … д-ра юрид. наук: спец. 12.00.07. Одеса, 2004. 427 с.

8. Кулицький С.П. Основи організації інформаційної діяльності у сфері управління: навч. посібник. Київ: МАУП, 2002. 224 с.

9. Марутян Р. Національні інформаційні ресурси як першооснова інформаційного суверенітету України. *Актуальні проблеми міжнародної безпеки : український вимір.* Київ : ВД «Стилос», 2020. 496 с.

10. Нестеренко Г. Інформаційна безпека: курс лекцій. Київ: НАУ, 2022. 102 с.

11. Нижник Н., Ситник Г., Нижник В. Національна безпека України (методологічні аспекти, стан і тенденції розвитку) : навчальний посібник. Ірпінь, 2000. 234 с.

12. Новородовський В. Інформаційна безпека України в умовах Російської агресії. *Соціум. Документ. Комунікація*. 2020. Вип. 9. С. 150-179

13. Олійник О. Принципи забезпечення інформаційної безпеки України. *Юридичний вісник повітряне і космічне право*. 2016. № 4(41). С. 72–78.

14. Онищенко О., Горовий В., Попик І. Національні інформаційні ресурси як інтегративний чинник вітчизняного соціокультурного середовища : монографія. Національна бібліотека України ім. В. І. Вернадського. Київ, 2014. 324 с.

15. Офіційний сайт ЖОВА. URL : https://oda.zht.gov.ua/ . (дата звернення: 23.11.2023).

16. Приймак Ю.Ю. Національні інформаційні ресурси – джерело державних інформаційних продуктів та послуг. *Державне управління : теорія та практика.* 2019. № 2. URL: www.academy.gov.ua/ej/ej10/doc_pdf/Priymak.pdf (дата звернення: 23.11.2023).

17. Порядок оцінки стану захищеності державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах : наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 02.12.14 р. № 660. URL : http://zakon.rada.gov.ua/go/z0090-15 (дата звернення: 23.11.2023).

18. Про власність : Закон України від 7 лютого 1991 р. № 697-X11 URL : http://zakon4.rada.gov.ua/laws/show/697-12. (дата звернення: 24.11.2023).

19. Про Державну службу спеціального зв'язку та захист інформації України : Закон України. URL : http://zakon2.rada.gov.ua/laws/show/3475-15. (дата звернення: 24.11.2023).

20. Про інформацію: закон України від 02.10.1992 р. URL : https://zakon.rada.gov.ua/laws/main/2657-12#Text (дата звернення: 22.11.2023).

21. Про Концепцію Національної програми інформатизації : Закон України від 1998 р. *Відомості Верховної Ради України (ВВР).* 1998. № 27–28. Ст. 182.

22. Про науково-технічну інформацію : Закон України №3322-X11 від 25 червня 1993 р. URL : http://zakon4.rada.gov.ua/laws/show/3322-12. (дата звернення: 23.11.2023).

23. Про Національну програму інформатизації : Закон України від 4 лютого 1998 р. № 74/98-ВР. URL : http://zakon4.rada.gov.ua/lawws/74/98-%D0%B2%D1%80. (дата звернення: 10.05.2023).

24. Про рішення Ради національної безпеки і оборони України від 15.10.2021 р. «Про Стратегію інформаційної безпеки» : указ Президента ННІНО НАУ Інформаційна безпека України від 28.12.2021 р. URL : https://zakon.rada.gov.ua/laws/show /685/2021#n14 (дата звернення: 21.11.2023).

25. Романов І.В., Рижов І.М., Тонконог І.О. Методологія комплексного оцінювання розвитку національних інтересів України в секторі економічної та державної безпеки. *Інформаційна безпека людини, суспільства, держави.* 2019. № 3 (27). URL: http://academy.ssu.gov.ua/ua/page/page_1581426025.htm (дата звернення: 12.12.2023).

26. Саган О.В. Протидія медіа-інформаційному тероризму як питання національної безпеки України : автореф. дис. … канд. політ. наук: 21.01.01. Київ, 2021. 22 с. URL: https://niss.gov.ua/sites/default/files/2021-04/06.04.2021_1-avtorefer_pidpis.-sagan_sig.pdf (дата звернення: 09.12.2023).

27. Семенець-Орлова І., Клочко А., Амро, Т. Публічне управління у сфері інформаційної безпеки для забезпечення розвитку демократії в Україні (контекст воєнного стану). 2022. № 5 (33). С. 73–82. DOI: https://doi.org/10.32689/2617-2224-2022-5(33)-10

28. Соснін О.В. Національні інформаційні ресурси : проблеми визначення і розуміння. *Стратегічна панорама*. 2014. № 4. С. 141–146.

29. Стратегії розвитку України : теорія і практика; за ред. О.С. Власюка. Київ : НІСД, 2002. 864 с.

30. Стратегія інформаційної безпеки: затверджена Указом Президента України від 28 грудня 2021 року № 685/2021.

31. Хорошко В., Хохлачова Ю., Пірцхалава Т., Іванченко І. Інформаційна зброя як інструмент інформаційної війни. *Захист інформації.* 2022. Том 24, № 2. С. 50–58. URL: https://jrnl.nau.edu.ua/index.php/ZI/article/view/16930 (дата звернення: 25.11.2023).

32. Хоффман Л. Дж. Сучасні методи захисту інформації / пер. з англ. Київ : Світанок, 1983. 57 с.

33. Цимбалюк В.С., Гавловський В.Д., Гриценко В.В. та ін. Основи інформаційного права України [навч. посіб.]. Київ: Знання, 2004. 274 с.

34. Шпакова О. Политика информационной безопасности в Украине : правовой базис. *Актуальні проблеми міжнародних відносин*. 2018. Вип. 65 (Ч. 1). С. 242–249.

35. Юдін О.К., Бучик С.С. Концептуальний аналіз уразливості державних інформаційних ресурсів. *Наукоємні технології*. 2019. № 3(19). 299–304.

36. Яковлєв П. О. Досвід державного регулювання забезпечення інформаційної безпеки зарубіжних держав (на прикладі Сполучених Штатів Америки, Канади, Німеччини, Франції). *Вісник Харківського національного університету імені В. Н. Каразіна. Серія «Право»*. 2020. №30. С. 106–113. URL: https://doi.org/10.26565/2075-1834-2020-30-13

37. Chala N.D., Poplavska O.M. Transforming the Relations between State and Society in the Context of the 4th Industrial Revolution: Ukraine's Experience. *Public Policy and Administration*. 2020. Vol 19. № 1. P. 89–98.

38. Chulitskaya T., Matonyte I. Social security discourses in a non-democratic state: Belarus between Soviet paternalistic legacies and neo-liberal pressures. *Public Policy and Administration*. 2020. Vol 17. № 4. P. 539–554.

39. Melnyk I. Principles of Formation of Information Policy of Ukraine In the Conditions of Hybrid War. *Krakowskie Studia MałopolskieIssue*. 2020. № 2 (26).

P. 136–149. URL: https://doi.org/10.15804/ ksm20200209 (дата звернення: 12.12.2023).

40. http://www.president.gov.ua/documents/472017-21374

41. (https://rm.coe.int/doctrine-of-information-security-of-ukraine-developments-in-member-sta/168073e052)