МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Харківський національний університет імені В.Н. Каразіна
Навчально-науковий інститут «Інститут державного управління»

До захисту
Завідувач кафедри публічного управління
та державної служби
к.держ.упр., доц. Набока Л.В.
_____

ДЕРЖАВНІ МЕХАНІЗМИ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ У КОНТЕКСТІ ФОРМУВАННЯ ІНФОРМАЦІЙНОГО ПРОСТОРУ В УКРАЇНІ

Кваліфікаційна робота на здобуття освітнього ступеня «магістр»
281 Публічне управління та адміністрування
28 Публічне управління та адміністрування

Виконавець
здобувач 2 курсу, групи ЗПУА-6-23 Тіщенко А.В.

Науковий керівник
к.держ.упр., доц. Білоконь М.В.

Харків – 2024

ЗМІСТ

ВСТУП

Актуальність теми. Інформаційна безпека займає особливе місце в загальній системі національної безпеки держави, оскільки є елементом усіх складових системи безпеки, внаслідок чого одночасно набуває й автономного значення. В умовах активізації реформ в Україні спостерігаємо певні труднощі стосовно реалізації функцій держави в деяких сферах життєдіяльності. Не є винятком і сфера національної безпеки, інформаційних відносин тощо.

Масштаби негативних наслідків цих загроз для держав, організацій, прав і свобод людини і громадянина вже усвідомлені світовою спільнотою, тому найважливішим завданням держави є розробка системи заходів по їх запобіганню і нейтралізації. В умовах російсько-українського конфлікту захист національного інформаційного простору від негативних інформаційно психологічних впливів, операцій та війн, гарантування інформаційної безпеки та інформаційного суверенітету набувають особливого значення і стають чинниками збереження національної ідентичності України та функціонування її як суверенної та незалежної держави.

Питання пов’язанні з державними механізмами забезпечення інформаційного простору у системі національної безпеки досліджували такі науковці як: А. Мінчеков, Г. Черних, О. Калівошко, Д. Хлистун, Т. Федоренко, В. Котляров, Н. Воробець, Є. Кобко, В. Зейкан, О. Радутний, Р. Кукляк, О. Венглінський, І. Дерюгін, І. Батько, О. Мельник, Є. Міненко та інші науковці.

Об'єкт дослідження – система державних механізмів, що забезпечують національну безпеку України в інформаційній сфері.

Предмет дослідження – державні механізми забезпечення національної безпеки у контексті формування інформаційного простору в Україні.

Мета і завдання дослідження. Мета магістерської роботи полягає у аналізі

теоретичних основ і практичних аспектів механізму забезпечення інформаційної безпеки, розкриття сутнісних ознак та особливостей, структури окресленої категорії.

Для досягнення поставленої мети в ході випускної кваліфікаційної роботи треба вирішити наступні *завдання:*

– дослідити сутність та основні компоненти інформаційного простору як елементу системи національної безпеки України;

– вивчити вплив інформаційних загроз на стан національної безпеки України, зокрема в контексті сучасних викликів;

– проаналізувати нормативно-правове забезпечення інформаційної безпеки в Україні, визначивши його сильні та слабкі сторони;

– оцінити інституційні механізми забезпечення інформаційної безпеки держави та їхню ефективність у сучасних умовах;

– розробити рекомендації щодо вдосконалення державних механізмів інформаційної безпеки України, спираючись на міжнародний досвід та сучасні інформаційні технології.

Методи дослідження. Методологічну основу дослідження становить сукупність загальнонаукових та спеціально-наукових методів, зокрема: аналізу, синтезу, дедукції, індукції, абстрагування, узагальнення, системний та структурно-функціональний, порівняльно-правовий, формально-юридичний.

Використання методів аналізу, синтезу, системного та структурно-функціонального методів дало змогу дослідити основні складові механізми забезпечення національної безпеки у інформаційному просторі.

Застосування структурно-функціонального методу сприяло всебічному дослідженню взаємодії компонентів системи.

Порівняльно-правовий метод використано при вивченні зарубіжного досвіду роботи механізмів забезпечення національної безпеки у інформаційному просторі.

Практичне значення роботи полягає в тому, що матеріали та висновки,

наведені в ній, можуть бути використані при написанні наукових, курсових, дипломних та інших робіт, пов'язаних з даною проблематикою. Запропонований матеріал може бути застосований при вивченні формуванні національного інформаційного простору, забезпеченні національної та інформаційної безпеки – у якості підготовчого матеріалу до занять з дисциплін, пов’язаних з публічним та державним управлінням, національною безпекою, інформаційною безпекою, тематичних семінарів, конференцій, виставок тощо.

Апробація результатів роботи. Магістерська кваліфікаційна робота самостійно виконана шляхом аналітичного дослідження та його узагальнення. Усі результати отримані за допомогою самостійного опрацювання та аналізу і синтезу отриманих даних.

Отримані в результаті проведеної роботи теоретичні висновки і практичні пропозиції обговорювалися на засіданні кафедри права, національної безпеки та європейської інтеграції Навчально-наукового інституту «Інститут державного управління» Харківського національного університету імені В.Н. Каразіна та можуть бути використані в науково-дослідній роботі кафедри.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ЗАСАДИ ФОРМУВАННЯ ІНФОРМАЦІЙНОГО ПРОСТОРУ У СИСТЕМІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

1.1 Сутність та основні компоненти інформаційного простору

Інформаційний простір відіграє важливу роль у забезпеченні національної безпеки в сучасних умовах. Його становлення та розвиток суттєво впливають на стабільність держави, включаючи її політичну, економічну, соціальну та культурну сфери. У контексті глобалізації та стрімкого прогресу інформаційно-комунікаційних технологій (ІКТ) національні інформаційні простори стикаються з новими викликами та загрозами, що вимагає ефективних заходів захисту [11].

Інформаційний простір охоплює сукупність інформаційних ресурсів, систем, каналів комунікації та організацій, які забезпечують обмін інформацією та формують суспільну свідомість. Це середовище, де циркулює інформація, формується громадська думка, забезпечується доступ до знань та реалізуються права громадян на свободу слова та інформацію.

Різноманітні підходи до дослідження поняття «інформаційний простір» представлені в роботах багатьох науковців, як вітчизняних, так і зарубіжних. Протягом останніх десятиліть питання захисту та розвитку національного інформаційного простору стало основою для численних наукових дискусій. Серед зарубіжних дослідників, які зробили вагомий внесок у цю тему, відзначаються А. Моль, М. Кастельс, Д. Томпсон, З. Бжезінський, Ф. Вільямс та інші [13].

Рисунок 1.1 – Інформаційний простір

Після проголошення незалежності України дану проблематику активно досліджують і українські науковці, зосереджуючись на питаннях формування інформаційного простору України, його розвитку та перспектив. Особливої уваги заслуговують праці таких дослідників, як А. Москаленко, П. Шевчук, В. Здоровега, І. Михайлін, В. Карпенко, Г. Кривошея та Ю. Горбань. Зокрема, дослідження впливу інформаційних технологій на розвиток засобів масової інформації представлені в роботах О. В. Зернецької, О. Мелещенко та В. Різуна.

Під інформаційним простором зазвичай розуміють сферу поширення інформації через різні елементи інформаційної системи та зв'язку, включаючи як технологічні, так і організаційні аспекти, що забезпечують передачу інформації в різних напрямках. Також важливе значення мають регіональні та міжнародні угоди, оскільки жоден інформаційний процес не може розглядатися лише як локальний

феномен. Параметрами інформаційного простору можуть бути: загальна кількість засобів масової комунікації, обсяг розповсюдженої інформації та фіксовані результати взаємодії аудиторії з контентом ЗМІ [10].

Інформаційне середовище включає в себе комплекс технічних і програмних засобів для зберігання, обробки та передачі інформації, а також політичні, економічні й культурні умови для реалізації процесів інформатизації. Це середовище можна охарактеризувати як ту частину інформаційного простору, яка формує найближче інформаційне оточення індивіда і є сукупністю умов, що сприяють його ефективній діяльності. Завдання, які реалізує людина, визначаються саме тим інформаційним середовищем, яке вона обирає [38].

Надзвичайно важливим аспектом стає правовий статус інформаційного простору України як основа для правового захисту національних інформаційних ресурсів. Сучасні загрози, пов'язані із запереченням можливості керувати інформаційним політичним простором через його відкритість і домінування країн-лідерів у сфері інформаційних технологій, обумовлюють необхідність формування національного інформаційного простору для збереження державного суверенітету [15]. Тому критичним є науково обґрунтоване й юридично точне визначення цього поняття.

Існують різні підходи до його трактування. Зокрема, у монографії О. Литвиненка «Інформаційний простір як чинник забезпечення національних інтересів України» національний інформаційний простір визначено як сукупність національних та іноземних інформаційних потоків, доступних на території країни, які формуються пресою, електронними ЗМІ та циркулюють у мережах зв'язку.

Водночас український дослідник комунікацій Г. Почепцов відзначає, що Україна недостатньо адаптована до нових реалій інформаційного суспільства. Відсутність академічних установ, які б працювали у цьому напрямі, обмежує підготовку фахівців лише в межах журналістики, тоді як суспільство потребує аналітиків, експертів з інформаційних кампаній і спеціалістів з громадських

комунікацій. Інші країни, як-от Болгарія, мають власні профільні журнали з інформаційної безпеки, тоді як у США існує багатий вибір літератури і програм підготовки військових кадрів до реалій інформаційної війни, що змінює підходи до стратегії та тактики, вироблені раніше [14].

Всі дослідники інформаційного простору України сходяться на думці, що для його ефективного розвитку необхідно активно розвивати інформаційну інфраструктуру країни. Це можливо за наявності чіткої, доступної та загальноприйнятої програми розвитку, що повинна бути зафіксована в національній «Концепції реформування інформаційної інфраструктури». Така концепція має ретельно враховувати існуючий досвід, спрямований на оптимізацію власної інфраструктури, адже без її належного функціонування неможливий сталий економічний, політичний та демократичний розвиток України.

При цьому український науковець О. Буньківська зазначає, що підхід до організації інформаційного простору зазнав змін: якщо раніше акцент був на формуванні цього простору, то тепер фокус зміщується на його моделювання та оптимізацію. Це пов’язано зі значними матеріальними витратами на підтримку інформаційного середовища, зокрема на технічне обладнання, підготовку фахівців, розробку і впровадження програмного забезпечення [11].

Розширення інформаційного простору та його зростаюча роль у житті суспільства створює новий життєвий простір – цілісне комунікаційне середовище, в якому взаємодіють люди. Характерною рисою цього простору є відокремленість реального та віртуального вимірів буття, що породжує нові норми існування та сприйняття. З глобалізацією інформаційні технології сприяють поглибленню комунікацій та формуванню єдиного інформаційного простору з особливими правилами взаємодії та світосприйняття.

Серед основних характеристик інформаційного політичного простору виділяють його масштабність (усі громадяни, незалежно від регіону проживання, користуються державними чи контрольованими каналами інформації),

упорядкованість (сукупність текстів національних медіа з регулярною підтримкою основного масиву інформації), а також інтенсивність інформаційних процесів [12]. Однак через нестачу сучасної технічної бази в Україні існує проблема телевізійного впливу ззовні, що ускладнює створення національного інформаційного простору, здатного протистояти іноземній інформаційній експансії та домінуванню потужніших мас-медіа [39].

Інформаційні технології завжди супроводжували розвиток суспільства: будь-які принципові технічні інновації рано чи пізно приводили до значних соціальних і культурних змін. Інформаційні комунікації стали постійним рушієм, який суттєво вплинув на розвиток суспільства.

Основні складові інформаційного простору включають:

1. Інформаційні ресурси – це дані, знання та інформація, створювані й використовувані різними суб’єктами, серед яких держава, громадянське суспільство, приватний сектор та індивіди. Вони можуть бути у вигляді тексту, аудіо, відео та інших форм, поширюючись через інформаційні канали та впливаючи на суспільну думку.

2. Інформаційні системи – це набір технічних засобів, програмного забезпечення, баз даних і мереж, що забезпечують зберігання, обробку та передавання інформації. Вони є критичним компонентом сучасного суспільства, оскільки надають доступ до інформаційних ресурсів і сприяють їх розповсюдженню.

3. Комунікаційні канали – це засоби передачі інформації, включаючи телебачення, радіо, інтернет-ЗМІ, соціальні мережі, телекомунікаційні мережі та друковані видання. Ефективність інформаційного простору залежить від здатності цих каналів забезпечувати швидкий і надійний обмін інформацією.

4. Суб’єкти інформаційного простору – основними учасниками є держава, медіа, громадські організації, приватний сектор та громадяни. Вони взаємодіють через інформаційні системи та канали, створюючи контент і впливаючи на його

сприйняття. Важливою є роль держави у забезпеченні безпечного функціонування інформаційного простору та контролі за загрозами.

5. Інформаційна інфраструктура – це технічна основа, яка включає телекомунікаційні мережі, сервери, дата-центри та платформи, що забезпечують обробку, зберігання та передачу інформації. Стабільність і захищеність інфраструктури є критичними для безпеки інформаційного простору.

Інформаційний простір також охоплює правові, політичні та культурні аспекти, які регулюють роботу інформаційних ресурсів і каналів, забезпечуючи захист національних інтересів і протидіючи зовнішнім загрозам. Таким чином, інформаційний простір складається з багатьох взаємопов'язаних елементів, що формують інформаційне середовище держави. Його розуміння та компонентів є необхідною основою для розробки ефективних механізмів державної інформаційної безпеки, яка є невід'ємною частиною національної безпеки.

Засоби інформаційної взаємодії громадян і організацій, що забезпечують доступ до інформаційних ресурсів, базуються на інформаційних технологіях, які включають програмні засоби та організаційно-нормативні документи. Таким чином, інформаційно-телекомунікаційну інфраструктуру формують організаційні структури та засоби інформаційної взаємодії [14].

Процес створення єдиного інформаційного простору України полягає не лише в розвитку технологій для забезпечення взаємодії виробників і споживачів інформації, але й в інтеграції соціальних, економічних і політичних аспектів у глобальний інформаційний простір. Інформація стає рушієм змін, якщо вона доступна зацікавленим споживачам.

Інформаційна діяльність є важливим елементом економічного потенціалу суспільства. Одним із головних завдань створення єдиного інформаційного простору є забезпечення відкритого доступу до інформаційних ресурсів і подолання інформаційного монополізму. Законодавча підтримка відкритості інформації є ключовою передумовою інтеграції України в світовий інформаційний простір [40].

Мета формування і розвитку єдиного інформаційного простору України:

– забезпечення прав громадян на інформацію згідно з вимогами Конституції України;

– створення і підтримка необхідного для стійкого розвитку суспільства рівня інформаційного потенціалу;

– підвищення узгодженості рішень, які прийняті центральними органами державної влади, обласними державними адміністраціями та органами місцевого самоврядування;

– підвищення рівня правосвідомості громадян шляхом надання їм вільного доступу до правових і нормативних документів, що визначають їх прав, обов’язки й можливості;

– надання можливості контролю з боку громадян і громадських організацій за діяльністю центральних і місцевих органів державної влади і органів місцевого самоврядування;

– підвищення ділової і суспільної активності громадян шляхом надання рівної з державними структурами можливості користуватися відкритою поштово-технічною, соціально-економічною, суспільно-політичною інформацією, а також інформаційними фондами сфер освіти, культури тощо;

– інтеграція зі світовим інформаційним простором.

Всі цивілізовані країни розглядають побудову інформаційного простору як основу соціально-економічного, політичного і культурного розвитку і проводять продуману національну інформаційну політику. Особливе значення в розвитку інформаційного простору мають геополітичні фактори. Як суб'єкт геополітики, Україна могла б стати природним мостом між Європою і Росією, який з'єднує з країнами Азіатсько-Тихоокеанського регіону. Для цього, перш за все, необхідно розвивати інформаційну інфраструктуру євразійського простору, що дозволить Україні стати важливою ланкою у світовому інформаційному просторі [10].

Формування та розвиток єдиного інформаційного простору в Україні,

зокрема, відповідних державних інформаційних ресурсів, є міжвідомчим та міжрегіональним питанням. Це вимагає вирішення складних організаційних і техніко-впроваджувальних проблем, великих витрат і не може бути вирішено відразу. При цьому необхідно враховувати соціально-економічні, правові та політичні аспекти інформатизації суспільства, всебічне використання організаційного, технічного та нормативно-правового досвіду, накопиченого при розвитку інформаційного простору найбільших країн світу [13].

1.2 Вплив інформаційних загроз на національну безпеку України

Першим термін «інформаційна війна» вжив Томас Рон у звіті за назвою «Системи зброї й інформаційна війна»2 у 1976 р. Він зазначив, що інформаційна складова є невід'ємним компонентом американської економіки і може стати вразливою ціллю в мирний чи воєнний час. Після публікації цього звіту постановка проблеми набула свого поширення в засобах масової інформації, а також серед військових [20]. Після активних обговорювань було досягнуто висновку, що інформація може виступати як ціллю, так і зброєю.

У сучасних реаліях інформаційні загрози стають одними з найсерйозніших викликів для національної безпеки держави. Україна, як і багато інших країн, стикається з масованими та системними інформаційними атаками, спрямованими на дестабілізацію політичної ситуації, підрив суспільної стабільності та ослаблення економічного й оборонного потенціалу. Зі зростанням цифрових технологій, розширенням глобального інформаційного простору і поширенням гібридних методів ведення війни інформаційні загрози набувають дедалі більшої значущості [41].

Україна, що опинилася в складному геополітичному положенні, стала

мішенню інформаційних атак, спрямованих на підрив її суверенітету та національної згуртованості. Російська агресія та інформаційна війна не тільки створили серйозні виклики, але й завдали значної шкоди національній безпеці країни. У цьому контексті важливо глибоко розуміти природу інформаційної війни та дезінформації, досліджувати їх методи і наслідки, а також розробляти стратегії протидії, що є ключовим завданням для забезпечення національної безпеки України [18].

Термін «інформаційна війна» був предметом досліджень багатьох науковців, проте особлива увага до його визначення в науково-правовій сфері почала приділятися в останні сім-вісім років. Це пов'язано з тим, що саме в цей час інформаційна війна набула особливого значення і стала частим компонентом ведення війни, особливо в контексті гібридних конфліктів. Наприклад, Б.С. Льюїс розглядав «інформаційну війну» як у широкому, так і у вузькому значенні. Згідно з його першим підходом, інформаційна війна – це боротьба за контроль над інформаційними та комунікаційними процесами, що бере свій початок з моменту виникнення людського спілкування та конфліктів [16].

В світлі іншого, вузького підходу, інформаційна війна полягає у широкомасштабному використанні руйнівної сили проти різних інформаційних систем та активів, включаючи комп’ютери та комп’ютерні мережі, що використовуються для функціонування основних систем критичної інфраструктури.

Сучасна доктрина інформаційної агресії проти України, будучи складовою частиною воєнної стратегії застосування збройних сил РФ, базується на трьох ключових елементах інформаційного протистояння:

1) інформаційно-психологічна війна;

2) інформаційно-технологічний вплив, що включає кібератаки і втручання в роботу електронних ресурсів державних органів;

3) операції із захисту власного інформаційного простору від зовнішніх

інформаційних атак.

Таким чином, спеціальні інформаційні операції, що проводяться російськими спецслужбами, складаються з багатоступеневих, взаємопов'язаних заходів, метою яких є маніпуляція масовою та індивідуальною свідомістю. Особливістю цих операцій є використання передових технологій і психологічних методик, які разом із можливостями сил безпеки та оборони можуть створювати значний суспільний резонанс [19].

Не заглиблюючись у детальний аналіз усіх складових, що лежать в основі спеціальних інформаційних операцій, доцільно звернути особливу увагу на інформаційно-психологічні впливи. В умовах повномасштабної війни вони є найбільш небезпечними, оскільки спрямовані на реалізацію геноцидних планів РФ проти України. Основною метою таких впливів є ураження національної свідомості українців через формування викривленого сприйняття реальних подій (починаючи з 2014 року) та виправдання збройної агресії, що в кінцевому результаті веде до знищення української ідентичності та державності. Це не випадково, оскільки саме інформаційно-психологічне середовище дозволяє впливати на свідомість і навіть підсвідомість (в тому числі емоційно-вольову сферу) невизначеного кола осіб та встановлення контролю над ними [42].

Найбільш ефективним інформаційно-психологічний вплив стає за умов домінування в інформаційному просторі супротивника, що досягається шляхом обмеження або повного позбавлення цільової аудиторії доступу до правдивої інформації з альтернативних джерел. Це створює сприятливе середовище для нав'язування контрольованих наративів. Така тактика активно використовується ворогом на окупованих територіях України. Очевидно, що протидія інформаційній агресії також повинна включати обмеження доступу до дезінформації та пропаганди на території України. Це передбачає блокування ресурсів, що поширюють деструктивний контент. Правовою основою для таких дій став указ Президента України №133/2017 від 15 травня 2017 року, а також подальші рішення

РНБО, які передбачають заборону користування радіочастотним ресурсом, обмеження або припинення телекомунікаційних послуг та інші санкції відповідно до закону [17].

Однак, незважаючи на низку обов'язкових рішень РНБО щодо блокування інформаційних ресурсів, які містять деструктивний контент, деякі провайдери продовжують безкарно надавати доступ до цих підсанкційних ресурсів, не виконуючи своїх зобов'язань. Основною причиною цього є недостатня правова регламентація механізмів виконання таких рішень, зокрема нечіткість процедур обмеження доступу до шкідливої інформації та механізмів притягнення до відповідальності тих, хто зобов'язаний забезпечувати виконання санкцій. В умовах війни бездіяльність операторів і телекомунікаційних провайдерів становить серйозну загрозу для інформаційної безпеки України. Це вказує на необхідність запровадження кримінальної відповідальності за умисне невиконання спеціальних економічних або інших обмежувальних заходів (санкцій), що дозволить притягати до відповідальності навіть Інтернет-провайдерів. Зокрема, вже зареєстровано законопроект № 8384 від 25 січня 2023 року, який передбачає внесення змін до Кримінального кодексу України щодо встановлення кримінальної відповідальності за порушення законодавства про санкції. Хоча виникають питання стосовно деталей криміналізації порушень, включаючи запропоновану ст. 1113 КК України, впровадження таких норм є критично важливим для захисту інформаційного простору України [2].

Загрози національній безпеці України в інформаційній сфері це – сукупність умов та чинників, які становлять небезпеку життєво важливим інтересам держави, суспільства і особи через можливість негативного інформаційного впливу на свідомість та поведінку громадян, а також на інформаційні ресурси та інформаційно-технічну інфраструктуру [20].

Як зазначає Р. Р. Марутян, найсуттєвішою загрозою національній безпеці України в інформаційній сфері належать дії іноземних держав, спрямовані на

негативний інформаційно-психологічний вплив на суспільну свідомість українців та світову громадськість через проведення інформаційних кампаній і спеціальних операцій. Це включає систематичне поширення тенденційної, неповної або упередженої інформації про Україну та її політичні процеси, що впливає на внутрішню та зовнішню політику, знижує міжнародний імідж країни й має політичні та економічні мотиви. Метою таких операцій є захист національних інтересів інших держав.

Серед інших загроз варто відзначити: обмеження свободи слова та доступу до інформації; викривлення, спотворення або замовчування важливих фактів; несанкціоноване розповсюдження інформації; відкрита дезінформація; інформаційна експансія іноземних держав, яка проявляється в руйнівному впливі на національний інформаційний простір, коли країни з сильнішим інформаційним потенціалом використовують ЗМІ для впливу на населення менш потужної держави. Інші загрози включають появу неконтрольованих інформаційних потоків, поширення культури насильства та жорстокості в медіа, уповільнення інтеграції України у світовий інформаційний простір, недоліки в державній інформаційній політиці та відсутність належної інфраструктури в інформаційній сфері, а також поширення дезінформації в Інтернеті.

У сучасному глобалізованому інформаційному суспільстві, де кіберпростір стає полем боротьби, одними з основних загроз інформаційній безпеці держав (включаючи Україну) є комп'ютерні злочини, кібертероризм і кібервійни. Вони передбачають протистояння національним інтересам у просторі Інтернету через використання комп'ютерних та інтернет-технологій для завдання шкоди супротивнику. Найчастіше такі технології спрямовані на сфери державної безпеки та оборони, становлячи реальну загрозу суверенітету держави [19].

Проти України активно застосовуються сучасні технології негативних інформаційно-психологічних впливів, що загрожують національному інформаційному простору та суверенітету. Забезпечення інформаційної безпеки

України в умовах дестабілізаційних інформаційних атак і агресивної інформаційної політики Російської Федерації потребує об'єднання зусиль на всіх рівнях державної влади та громадянського суспільства.

Основним інструментом ведення інформаційної війни є дезінформація. В цілому, під терміном «дезінформація» розуміють широкий набір методів і засобів, що використовуються для свідомого поширення неправдивих повідомлень, викривленої інформації або неправдивих даних з метою введення в оману суспільства або політичних опонентів [17].

Однак деякі дослідники трактують дезінформацію як поширення публічної інформації, що містить неправдиві дані, які не були перевірені або виявлені як хибні, що може спричинити негативні наслідки для реалізації конституційних прав громадян та становити загрозу національній безпеці [16].

За думкою Таркіна В.П., дезінформація може бути класифікована за тривалістю та рівнем організаційної підготовки як разова та тривала. Ці типи мають різні негативні наслідки і, як правило, використовуються для досягнення різних стратегічних цілей. Так, разова дезінформація, за Таркіним В.П., стосується конкретної події, ситуації або окремої особи, часто розповсюджується у формі чуток або неперевіреної інформації. Тривала або систематична дезінформація виникає тоді, коли проводяться організовані та сплановані заходи для введення в оману великих груп людей або всього населення. Цей вид дезінформації є більш серйозним, оскільки потребує значної підготовки, координації та ресурсів. Вона може використовуватися для спотворення політичних процесів, впливу на державну безпеку та міжнародні відносини [18].

Під час мого аналізу рекламних повідомлень РФ, починаючи з 10 березня 2023 року, вони були направленні на деморалізацію цивільних громадян і українських військових. Служби РФ розповідали про «переваги» перебування в російському полоні, намагалися переконати в тому, що західні партнери більше не підтримують Україну, пророкували безрезультатність опору агресії та поширювали

чутки про масову зраду, корупцію й внутрішні конфлікти у вищих гілках влади.

Найбільша кількість повідомлень з виявленого масиву присвячена ситуації на фронті (тема «Фронт»). Виявлено 136 повідомлень, для яких ця тема була основною, і вони склали майже 23% від загального масиву. Саме ситуація на лінії бойового зіткнення і стала ключовою темою для рекламних публікацій, що з’явилися 11 березня. Першим меседжом, який атакував українську аудиторію Facebook, став «Битву за Бахмут програно».

Слід зазначити, що масований наступ російських військ на це місто в Донецькій області розпочався в грудні 2022 – січні 2023 року. Ціною великих втрат окупантам вдалося захопити майже весь Бахмут лише наприкінці травня. Деморалізуючі повідомлення почали з'являтися в розпал битви за Бахмут, коли російські війська контролювали лише східну частину міста. Пропаганда активно використовувала тему Бахмута до серпня, але влітку, на відміну від весни, акцент змістився з «програної битви» на «катастрофічні втрати» ЗСУ та прогнози про «ще більші втрати» і «другий Бахмут» під час нового наступу на Півдні України.

Публікації про «провал контрнаступу» почали з'являтися з 10 квітня, за кілька місяців до його реального початку. Пік активності щодо цієї теми припав на другу половину вересня, коли українські сили активізували наступальні дії в Херсонській і Запорізькій областях. У повідомленнях знову робився акцент на втрати ЗСУ.

У жовтні та листопаді наратив «проваленого контрнаступу» використовувався вже не для опису ситуації на фронті (після піку в середині жовтня інтенсивність таких публікацій зменшилася), а як інструмент для дискредитації української влади та західних партнерів.

Друга за популярністю тема – формування антизахідних настроїв серед аудиторії («Захід»). Цій темі присвячено 108 повідомлень, що становить 18% від загальної кількості. На відміну від інших тем, вона постійно експлуатувалася протягом усього досліджуваного періоду. Серед ключових меседжів, поширених у Facebook, були такі:

– Захід не довіряє українській владі через її некомпетентність і корумпованість та може припинити підтримку України;

– Захід роздратований постійними проханнями Києва про допомогу;

– Захід корумпує українських посадовців;

– Україна перебуває під зовнішнім управлінням Заходу;

– Сусідні держави мають територіальні претензії до України;

– Громадяни Західних країн зневажливо ставляться до українців та українських біженців.

Пропагандисти переважно приписували територіальні претензії до України Польщі, активно просуваючи наратив «поляки хочуть забрати Львів», хоча також згадували й інших західних сусідів. У жовтні-листопаді до цих меседжів додалося протиставлення України Ізраїлю, із твердженням, що Захід, зокрема США, тепер надаватиме пріоритет Ізраїлю, залишаючи Україну без військової допомоги.

Особливу увагу пропагандисти приділили підриву мобілізаційних процесів в Україні. Тема мобілізації займала 13,8% від загальної кількості публікацій (82 публікації). На початку акцент робився на страху смерті, каліцтва чи полону, а також залякуванні мобілізацією жінок, підлітків та осіб з інвалідністю. Однак з кінця вересня основним наративом стала корумпованість військкоматів («воєнкоми-хабарники»), на тлі реальних корупційних скандалів, таких як справа з арештом керівника Одеського ТЦК Євгена Борисова.

Тема корупції посіла четверте місце за кількістю публікацій, становлячи 11,7% загального масиву (70 публікацій). Найпопулярніші наративи включали: розкрадання гуманітарної допомоги, продаж західної зброї на чорному ринку та корумпованість Міністерства оборони. Часто ці теми переплітaлися з антизахідною пропагандою, стверджуючи, що Захід корумпує українську владу, а також використовувалися для дискредитації мобілізації.

Важливим напрямом ворожої пропаганди є дискредитація української влади. Ця група повідомлень була спрямована на підрив довіри до військово-політичного

керівництва країни через різні звинувачення та претензії. Серед найпоширеніших меседжів можна виділити такі:

– влада некомпетентна;

– влада непатріотична і готова зрадити Україну за першої нагоди;

– представники влади свідомо шкодять населенню України та скоюють інші злочини;

– у владних структурах є внутрішні конфлікти, які негативно впливають на простих громадян.

Президент України Володимир Зеленський був найчастішою мішенню цих інформаційних атак, а також неодноразово піддавалися атакам його дружина Олена Зеленська, міністри оборони Олексій Резніков та Рустем Умєров.

За допомогою реклами у Facebook поширювалися неправдиві повідомлення про те, що подружжя Зеленських нібито отримало іноземне громадянство для втечі з України, а також про придбання першою леді дорогоцінностей у США на значну суму [49]. У листопаді пропаганда активно використовувала тему конфлікту між Володимиром Зеленським і головнокомандувачем ЗСУ Валерієм Залужним.

До теми «Деморалізація» включено повідомлення, що містять «свідчення» про моральне падіння українського суспільства, а також експлуатацію різних страхів. Для просування цих ідей використовувалися такі сюжети та меседжі:

– низький бойовий дух військових і добровільна здача в полон;

– аморальна поведінка як цивільних, так і військових, взаємна неповага;

– військові – загроза для цивільних (поза контекстом мобілізації);

– радість жителів окупованих територій через прихід росіян;

– зростання рівня злочинності;

– «чорна» трансплантологія.

Перша реклама «переваг» російського полону з'явилася у Facebook наприкінці березня. В її основу ліг матеріал пропагандистського проєкту «Мама, я в порядке», запущеного восени 2022 року, який публікує відео з українськими

військовополоненими. Метою цього проєкту є деморалізація українських військових через розповіді про «доброту» російського ставлення до полонених, твердження про небажання українських солдатів воювати з «братнім народом», масове залишення ними позицій і втрату віри у перемогу.

Російські ресурси, орієнтовані на жителів РФ та окупованих територій. 14 березня адміністратори проєкту оголосили, що він отримав «нове життя» та планує публікувати більше відео з українськими полоненими.

Автори публікацій використовували поширений пропагандистський прийом, коли окремий інцидент подається як загальноприйнята та постійна практика. Наприклад, для демонстрації «морального занепаду» українців було використано повідомлення про викрадення шевронів з могили військового пілота Андрія «Джуса» Пільщикова, про що 5 вересня у Facebook повідомила Меланія Подоляк. Через місяць, 18 жовтня, з'явилася реклама, проілюстрована фотографією з її допису, де з тексту випливало, що обкрадання могил військових нібито є повсякденною практикою серед українців.

Окремим напрямом стали звинувачення мешканців окупованих територій у масовій зраді. Використовуючи відверто пропагандистський контент, аудиторію намагалися переконати, що всі українські громадяни на окупованих землях нібито є колаборантами і «радіють» приходу росіян. Метою цих маніпуляцій було послаблення суспільства через підрив єдності, деморалізація та формування думки про «непотрібність» відновлення територіальної цілісності і вигнання російських окупантів.

Тема «Турбота про військових» тісно пов'язана з темою «Деморалізація», але акцентується не на аморальності суспільства, а на нібито байдужості держави до військовослужбовців. Основні меседжі цієї теми включають:

– влада залишає поранених бійців напризволяще;

– влада не поважає сім'ї військових, особливо загиблих і зниклих безвісти, і не піклується про них.

Окрім експлуатації природних страхів перед загибеллю чи пораненням (часто використовувалися зображення поранених з ампутаціями), автори також просували ідею, що родичі військових залишаються беззахисними, коли чоловіки йдуть на фронт. Очевидною метою було підрив мобілізації. Типовим прикладом такого наративу став фейк про повідомлення про загибель бійця, нібито надруковане на звороті рекламного буклету продуктового супермаркету.

Теми «Бідність» і «Виплати» також тісно переплітаються. Повідомлення про низький рівень життя соціально незахищених верств населення, чиї основні доходи складаються з пенсій і соціальних виплат, підводили аудиторію до висновку, що «за таку державу не варто боротися».

Отже, інформаційні загрози мають багатовимірний характер і впливають на різні аспекти національної безпеки. Для ефективного протистояння цим викликам необхідне всебічне державне регулювання інформаційного простору, включаючи розробку національної стратегії інформаційної безпеки, зміцнення співпраці з міжнародними організаціями, розвиток кібервійськ і підвищення рівня інформаційної грамотності громадян. Своєчасна та адекватна реакція на інформаційні загрози є ключовою умовою для забезпечення суверенітету й стабільності держави.

РОЗДІЛ 2
ДЕРЖАВНІ МЕХАНІЗМИ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ В ІНФОРМАЦІЙНІЙ СФЕРІ

2.1 Нормативно-правове регулювання інформаційної безпеки в Україні

Нормативно-правове регулювання інформаційної безпеки є важливою складовою національної безпеки України. Воно визначає основи, механізми та інструменти для захисту інформаційного простору від загроз, що можуть порушити політичну, економічну та соціальну стабільність країни. З огляду на зростання ролі інформаційних технологій і глобальної комунікації, правові норми у сфері інформаційної безпеки потребують постійного вдосконалення та адаптації до нових викликів.

По-перше, в умовах створення правової держави та громадянського суспільства діяльність органів державної влади, відповідальних за національну безпеку, повинна регулюватися чітко визначеними правовими нормами, які гарантують конституційні права та свободи громадян.

Правове регулювання в цій сфері спрямоване на нормативне закріплення цілей у боротьбі з загрозами національній безпеці, методів їх досягнення та узгодження дій органів влади.

По-друге, інтеграція України у світову спільноту відкриває додаткові можливості для зміцнення інформаційної безпеки через участь у формуванні міжнародного права та створенні глобальної системи захисту інформаційної сфери як на рівні окремих країн, так і в світовому масштабі.

По-третє, забезпечення прав і свобод громадян та захист національних інтересів України передбачає значне посилення ролі держави у регулюванні

суспільних відносин і розробку відкритої та прозорої державної політики в цій сфері.

У зв’язку з цим останнім часом зростає інтерес з боку державних органів і науковців до обговорення шляхів вдосконалення правового забезпечення інформаційної безпеки України. Це забезпечення складається з правової системи, яка регулює захист інформаційної безпеки, і процесу її формування.

Система правового регулювання інформаційної безпеки включає сукупність правових норм, що регулюють відносини у цій сфері, правовідносини, які виникають на основі цих норм, та відповідні правозастосовчі акти.

Ці правові норми є основою захисту інформаційної безпеки і визначають ефективність діяльності держави, суспільства та громадян у сфері захисту національних інтересів України. До цієї бази належать норми міжнародних договорів України, закони України, акти Президента, постанови уряду та нормативні акти державних органів.

Необхідність правового забезпечення курсу на демократичні зміни в суспільстві та державі визначає потребу в реформуванні всієї правової системи України, зокрема її законодавства, яке наразі має низку суттєвих недоліків [43].

При вертикальній структуризації законодавства в досліджуваній сфері основою ієрархії нормативно-правових актів є Конституція України. Вона встановлює базові правові засади, а наступні рівні включають закони та підзаконні акти, такі як укази Президента України та постанови Верховної Ради України.

Основу правового регулювання у сфері інформаційної безпеки становить Конституція України, яка гарантує громадянам свободу слова, право на доступ до інформації, а також захист від незаконного втручання в особисте життя та комунікації. Конституційні положення створюють базу для подальшого розвитку законодавства, спрямованого на забезпечення інформаційної безпеки як невід’ємної частини національної безпеки.

Конституція України включає понад 20 правових норм, що стосуються

забезпечення інформаційної безпеки, які мають найвищу юридичну силу. Серед основних конституційних норм варто відзначити право на інформацію та положення щодо захисту державної таємниці.

Аналіз конституційних норм, пов'язаних із інформаційною безпекою, вказує на їхню багатогранність і складність. Кожна з цих норм може бути темою окремого наукового дослідження. Проте навіть поверхневий аналіз положень Конституції України, що стосуються захисту інформаційних прав та свобод, свідчить про те, що Основний закон містить значну кількість норм, які є базою для формування законодавства у сфері інформаційної безпеки [1].

Серед нормативно-правових актів у зазначеній сфері важливу роль відіграє Кримінальний кодекс України. У ньому передбачена відповідальність за порушення недоторканності приватного життя (стаття 137), таємниці листування та телефонних розмов (стаття 138), відмову в наданні громадянину інформації (стаття 140), незаконний експорт науково-технічної інформації (стаття 189), розголошення державної таємниці (стаття 283) та інші злочини у цій галузі. Окрема глава Кримінального кодексу вперше в українському законодавстві присвячена злочинам у сфері комп'ютерної інформації (глава 28) [2].

Митний кодекс України (статті 186, 214, 344) і Податковий кодекс України (статті 84, 90, 313) також містять положення, що регулюють захист різних видів конфіденційної інформації [3].

У Законі України «Про національну безпеку України» поняття безпеки визначається як стан захищеності життєво важливих інтересів особи, суспільства та держави від внутрішніх і зовнішніх загроз. Життєво важливими інтересами вважаються ті потреби, задоволення яких забезпечує існування та розвиток особистості, суспільства і держави (стаття 1), а під загрозами безпеки розуміються умови та чинники, що створюють небезпеку цим інтересам (стаття 3) [4].

Як видно з наведених визначень, українське законодавство щодо інформаційної безпеки охоплює широкий спектр суспільних відносин у

інформаційній сфері. Водночас більшість норм у цій сфері стосується саме захисту інформації.

Закон «Про захист інформації в інформаційно-комунікаційних системах» є ключовим нормативним актом у сфері інформації. У ньому визначені основні терміни, такі як:

– Інформація – це відомості (повідомлення, дані) незалежно від форми їх подання.

– Інформаційні технології – процеси та методи пошуку, збору, зберігання, обробки, надання та поширення інформації, а також способи реалізації цих процесів.

– Інформаційна система – сукупність інформації в базах даних, яка забезпечується за допомогою інформаційних технологій та технічних засобів.

– Інформаційно-телекомунікаційна мережа – технологічна система, призначена для передачі інформації через лінії зв’язку, доступ до якої здійснюється за допомогою обчислювальної техніки.

– Власник інформації – особа, яка самостійно створила інформацію або отримала право дозволяти чи обмежувати доступ до неї на підставі закону або договору.

– Доступ до інформації – можливість отримання та використання інформації.

– Конфіденційність інформації – зобов’язання особи, яка отримала доступ до інформації, не передавати її третім особам без дозволу власника.

– Надання інформації – дії, спрямовані на передачу або отримання інформації певним колом осіб.

– Поширення інформації – дії, що дозволяють передати або отримати інформацію невизначеному колу осіб.

– Електронне повідомлення – інформація, передана або отримана користувачем через інформаційно-телекомунікаційну мережу.

– Документована інформація – зафіксована на матеріальному носії інформація з реквізитами, що дозволяють її ідентифікувати або визнати її матеріальний носій відповідно до законодавства.

– Оператор інформаційної системи – фізична або юридична особа, яка здійснює експлуатацію інформаційної системи, включаючи обробку даних, що містяться в її базах [5].

Правове регулювання відносин у сфері інформації, інформаційних технологій та захисту інформації, згідно з цим законом, базується на таких принципах:

1. Свобода пошуку, отримання, передачі, створення та поширення інформації будь-яким законним способом.

2. Обмеження доступу до інформації встановлюються виключно законом.

3. Відкритість інформації про діяльність державних органів та органів місцевого самоврядування, а також вільний доступ до неї, за винятком випадків, визначених законом.

4. Забезпечення безпеки України під час створення, експлуатації та захисту інформаційних систем і даних, що містяться в них.

5. Достовірність та своєчасність надання інформації.

6. Недоторканність приватного життя та заборона збору, зберігання, використання та поширення інформації про особисте життя без згоди особи.

7. Недопустимість надання переваг окремим інформаційним технологіям перед іншими у нормативних актах, якщо закон не передбачає обов’язкове використання певних технологій для державних інформаційних систем.

Особливо актуальним у контексті вдосконалення правового регулювання є питання захисту персональних даних. Важливим аспектом розвитку інформаційного законодавства у сфері забезпечення інформаційної безпеки є його приведення у відповідність до Європейської Конвенції про захист фізичних осіб при автоматизованій обробці персональних даних, яку ратифікувала Україна.

Закон України «Про інформацію» регламентує права та обов’язки суб’єктів

інформаційної діяльності, встановлює принципи прозорості та доступності інформації для громадян, а також передбачає заходи щодо захисту інформації, що становить державну або комерційну таємницю. Цей закон також визначає відповідальність за порушення законодавства в інформаційній сфері, включаючи поширення неправдивої інформації або використання інформаційних ресурсів з метою маніпуляцій громадською думкою [6].

Значну роль у забезпеченні інформаційної безпеки відіграє Закон України «Про електронні комунікації», який регулює діяльність у сфері телекомунікаційних послуг і забезпечує умови для безпечної та надійної роботи інформаційних мереж [7]. Водночас Закон «Про захист персональних даних» спрямований на захист інформації, яка стосується приватного життя громадян. Він встановлює вимоги до обробки персональних даних, гарантує право на конфіденційність інформації та передбачає заходи проти несанкціонованого доступу до даних [9].

Крім того, важливим елементом нормативно-правового регулювання є Закон «Про основні засади забезпечення кібербезпеки України», який закріплює механізми захисту національної інформаційної інфраструктури від кіберзагроз. Він передбачає створення національної системи кібербезпеки, яка охоплює державні установи, приватний сектор та громадянське суспільство. Цей закон визначає принципи співпраці між державними органами та приватними компаніями для захисту критичної інфраструктури від кібератак [8].

Нормативно-правове регулювання інформаційної безпеки також спирається на міжнародні зобов’язання України. Зокрема, країна активно співпрацює з Європейським Союзом у рамках Угоди про асоціацію, яка передбачає гармонізацію національного законодавства з європейськими стандартами в сфері інформаційної безпеки. Україна також є учасницею міжнародних ініціатив, спрямованих на боротьбу з кіберзлочинністю, зокрема Будапештської конвенції про кіберзлочинність.

Отже, багатогранність інформаційних відносин дозволяє зробити висновок, що до системи законодавства з питань забезпечення інформаційної безпеки входять норми конституційного, адміністративного, цивільного, кримінального, трудового та інших галузей права.

Аналіз українського законодавства у сфері інформаційної безпеки показує, що його структура значною мірою визначається основними напрямками захисту об'єктів інформаційної сфери, зокрема: захист прав і свобод в інформаційній сфері; захист інформації, інформаційних ресурсів та систем від неправомірного втручання; а також захист інтересів особи, суспільства та держави від шкідливої, небезпечної або недоброякісної інформації.

Проведений системний аналіз законодавства у галузі інформаційної безпеки свідчить про необхідність впорядкування цього законодавства, визначення принципів реалізації державної політики і розробки концепції правових засад інформаційного суспільства.

У Концепції національної безпеки України забезпечення єдності правового простору розглядається як одна із ключових складових захисту конституційного ладу, що є національним інтересом у внутрішньополітичній сфері. На сьогодні суб'єкти України володіють великими інформаційними ресурсами, активно впроваджується інформатизація, а в органах державної влади широко використовуються сучасні інформаційні технології. Прийнято значну кількість нормативних актів, що регулюють ці питання.

У сфері інформаційної безпеки суб'єкти України розробляють концепції з питань інформації, інформатизації, інформаційних технологій та інформаційної безпеки; формують та експлуатують державні інформаційні ресурси, проводять державний облік та реєстрацію баз даних; приймають правові акти для реалізації законів «Про захист інформації в інформаційно-комунікаційних системах» та щодо забезпечення конфіденційності інформації обмеженого доступу, включаючи персональні дані. Також здійснюються заходи для забезпечення доступу до

інформації (включаючи Інтернет) та її захисту від неправомірних дій, таких як несанкціонований доступ, знищення, модифікація або блокування даних.

Отже, нормативно-правове регулювання інформаційної безпеки в Україні є комплексним і охоплює різні аспекти захисту інформаційного простору. Воно постійно розвивається, оскільки потребує адаптації до нових викликів та загроз в умовах інформаційної війни та глобальних змін у сфері інформації.

2.2 Інституційні механізми забезпечення інформаційної безпеки держави

Інституційні механізми забезпечення інформаційної безпеки є важливою складовою державного апарату, що формує норми і правила для регулювання взаємодії різних суб'єктів у інформаційній сфері з метою запобігання загрозам інформаційній безпеці. Інституційні механізми можна розглядати як процес визначення і закріплення норм, правил, статусів і ролей, які спрямовані на вирішення певних суспільних завдань. Це складне і багатовимірне явище, яке в наукових дослідженнях вивчається за різними методологічними підходами [22].

Інституцію можна розглядати як систему, тоді як інститут є її базовим, неподільним елементом. Один із засновників інституціоналізму Дж. Коммонс описує інституції у вузькому сенсі як «систему законів або природних прав, у межах яких діють індивіди, як в'язні», а в широкому сенсі – як «колективну дію, спрямовану на контроль, лібералізацію та розширення індивідуальної діяльності».

Представник неоінституціоналізму Д. Норт визначає інституції як обмеження, що спрямовують людську взаємодію в певному напрямку, зменшуючи невизначеність шляхом встановлення стабільної структури взаємодії. Подібний підхід підтримує Е. Остром, яка вважає інституції набором правил для прийняття рішень у конкретних сферах діяльності.

Українські вчені також продовжують досліджувати інституціоналізм. Т. Гайдай визначає інституції як систему норм і правил, які регулюють соціально-економічну взаємодію суб'єктів і соціальних груп. Узагальнюючи підходи «нового» інституціоналізму, інституції можна описати як систему формальних і неформальних норм, що регламентують відносини між економічними суб'єктами і включають організаційні структури для досягнення конкретних цілей [25].

Інститути є формою прояву інституцій. Їх можна розуміти як юридичні норми та механізми встановлення зв'язків між ними, що дозволяє упорядковувати взаємовідносини між суб'єктами права для надання їм стабільності. Т. Веблен визначав інститути як закріплення звичаїв і порядків у формі закону, а Дж. Коммонс відносив до інститутів корпорації, профспілки та політичні партії, які визначають економічну поведінку суспільства.

Д. Норт вважає інститути основними суб'єктами інституційного механізму, які встановлюють правила гри та забезпечують їх виконання. Дж. Ходжсон називає інститути системами соціальних правил, що структурують соціальні взаємодії. Д. Буркальцева підкреслює, що аналіз інститутів повинен враховувати як мікро-, так і макрорівень: на мікрорівні підприємці організовують роботу фірм, а на макрорівні держава і міжнародні організації координують системи.

Інституційне забезпечення можна визначити як процес формування інституцій (формальні та неформальні норми) і інститутів (юридичні норми), що діють через організації, закони та правила в еволюції ринкового механізму [24].

Інституційне забезпечення інформаційної безпеки – це сукупність державних і недержавних інституцій, які створюють нормативно-правові, організаційні та економічні умови для реалізації ефективної державної політики у сфері інформаційної безпеки [23].

У структурі інституційного забезпечення інформаційної безпеки можна виділити дві основні складові:

– інституційно-правове забезпечення;

– інституційно-організаційне забезпечення.

З огляду на об'єкт інституційно-правового забезпечення, доцільно запропонувати авторське визначення поняття «інституційно-правове забезпечення інформаційної безпеки» як нормативної форми реалізації функцій державних і недержавних інституцій, спрямованих на забезпечення захищеності інформаційного середовища та протидію ризикам і загрозам, викликаним поширенням негативних інформаційних впливів [44].

Одним із підходів є функціональний аналіз інституційного механізму в сфері інформаційної безпеки. Деякі дослідники вважають, що цей механізм може виконувати такі функції: об'єднання агентів в один інститут для спільної діяльності на основі загальних статусів і норм; розмежування норм, статусів і суб’єктів різних інститутів; регулювання взаємодії між інститутом і його агентами; реалізація нових вимог у практичну діяльність; підтримка інноваційних рутин; координація відносин між суб’єктами різних інститутів; інформування суб’єктів про нові норми поведінки; регулювання діяльності суб’єктів і контроль за виконанням норм і правил.

З іншого боку, науковці також досліджують окремі складові (суб’єкти) інституційного механізму інформаційної безпеки і їхній вплив на державну політику в цій сфері. Інституційний механізм може розглядатися як у широкому, так і у вузькому значенні. У вузькому розумінні він включає тільки державні інституції, які відповідають за формування і впровадження політики в галузі інформаційної безпеки.

Навіть коли інституційний механізм розглядається в межах певного формату суб'єктів, це не дає однозначного розуміння щодо інституційного забезпечення інформаційної сфери в наукових колах. Одним із підходів до сприйняття цього механізму є аналіз загальної системи національної безпеки, зосередженої на інформаційній сфері. Наприклад, дослідник О. Стоєцький, посилаючись на офіційні документи, що передували агресії РФ проти України, визначає інституційний

механізм інформаційної безпеки як організовану державою систему суб'єктів: державних органів, громадських організацій, посадових осіб та громадян, які спільно діють для захисту національних інтересів у рамках законодавства України.

Інший погляд на інституційний механізм інформаційної безпеки пропонує О. Твердохліб, який, базуючись на контент-аналізі нормативних актів органів державної влади, розглядає їхні функціональні обов'язки в умовах агресії РФ. Він зазначає, що в Україні державне регулювання та управління інформаційною сферою сьогодні здійснюється за основними напрямами і суб'єктами.

Законодавча гілка влади:

– Комітет Верховної Ради України з питань свободи слова та інформаційної політики займається формуванням державної політики у сфері інформації та інформаційної безпеки, забезпеченням свободи слова, правом громадян на інформацію, а також регулюванням діяльності ЗМІ та Інтернету;

– Комітет Верховної Ради з питань інформатизації та зв’язку відповідає за державну політику у сферах розвитку інформаційного суспільства, інформатизації, електронного урядування, кібербезпеки та інших суміжних сфер.

Виконавча влада:

– Міністерство юстиції України регулює діяльність друкованих ЗМІ та інформаційних агентств, формує політику у сфері архівної справи та діловодства, а також займається створенням і функціонуванням державної системи страхового фонду документації;

– Міністерство культури України відповідає за формування і реалізацію державної політики в галузях культури, мистецтв, кінематографії та державної мовної політики;

– Національна комісія, що здійснює державне регулювання у сфері зв’язку та інформатизації, регулює телекомунікації, інформатизацію, користування радіочастотним ресурсом та надання послуг поштового зв’язку;

– Національна рада України з питань телебачення і радіомовлення

займається регулюванням галузі телерадіомовлення;

– Державний комітет телебачення і радіомовлення України формує і реалізує політику у сфері телебачення, радіомовлення, а також в інформаційній і видавничій галузях;

– Державна служба спеціального зв'язку та захисту інформації України відповідає за політику у сферах криптографічного та технічного захисту інформації, телекомунікацій і користування радіочастотним ресурсом;

– Державна архівна служба України реалізує політику у сфері архівної справи, діловодства та функціонування державної системи страхового фонду документації.

– Державна служба статистики України відповідає за реалізацію державної політики у сфері статистики;

– Служба безпеки України та Міжвідомча комісія з питань інформаційної політики та інформаційної безпеки при Раді національної безпеки і оборони України забезпечують інформаційну безпеку та захист національного інформаційного простору;

– Служба зовнішньої розвідки України здійснює розвідувальну діяльність, зокрема в інформаційній сфері.

Як зазначає дослідник, на центральному, регіональному та місцевому рівнях органи державної влади мають структурні підрозділи, відповідальні за реалізацію інформаційної політики за переліченими напрямами або їх частинами. Ці підрозділи є важливою частиною інституційного середовища, яке формує та реалізує державну інформаційну політику України.

13 серпня 2014 року, на підставі Постанови Кабінету Міністрів (з подальшими змінами), до системи органів, відповідальних за інформаційну політику в умовах агресії РФ, було включено Державний комітет телебачення і радіомовлення. Цей центральний орган виконавчої влади зі спеціальним статусом відповідає за формування та реалізацію державної політики у сфері телебачення, радіомовлення,

інформаційній та видавничій галузях. Відповідно до положення, основні функції Держкомтелерадіо включають:

– аналіз практики застосування законодавства у відповідних сферах, розробка пропозицій щодо його вдосконалення, а також підготовка законодавчих актів та актів Президента України і Кабінету Міністрів для подання Міністру культури та інформаційної політики;

– виконання завдань із забезпечення інформаційної безпеки за дорученням Міністра культури та інформаційної політики з участю інших державних органів;

– розробка пропозицій щодо поліпшення системи державного управління в телебаченні, радіомовленні, інформаційній і видавничій сферах та поліграфії;

– підтримка розвитку національних засобів масової інформації;

– забезпечення дотримання державної мовної політики у сферах телебачення, радіомовлення, інформаційної та видавничої діяльності.

Окремої уваги заслуговує питання розподілу повноважень і визначення рівня відповідальності в системі інформаційної безпеки серед силових структур, таких як Служба безпеки України, Служба зовнішньої розвідки України, Міністерство оборони, Міністерство внутрішніх справ та Національна поліція. До їхніх офіційних функцій у сфері інформаційної безпеки належать проведення розвідувальної діяльності, виявлення і запобігання психологічним диверсійним операціям, забезпечення інформаційної політики в оборонній сфері, підтримання правопорядку з виявленням порушень у системі інформаційної безпеки, а також захист державної таємниці. Важливою особливістю цих структур є не тільки їхня автономність від міністерств, зосереджених на гуманітарних питаннях, але й проблеми міжвідомчої взаємодії, що ускладнює обмін інформацією і скоординовану протидію викликам у сфері інформаційної безпеки.

Одним із ключових факторів для покращення функціонування інституційного механізму забезпечення інформаційної безпеки є підвищення рівня координації всіх

його складових, як гуманітарних, так і силових відомств. Загальноприйнятою є думка, що ця координаційна функція належить Раді національної безпеки і оборони України (РНБО), яка діє при Президентові України і відповідає за питання національної безпеки й оборони. Повноваження РНБО закріплені в Конституції України (ст. 107) [1] та Законі України «Про Раду національної безпеки і оборони» від 5 березня 1998 року, з наступними змінами, що враховують вимоги часу (2014–2019 роки).

У сфері інформаційної безпеки до компетенцій РНБО входить:

– визначення стратегічних національних інтересів України та концептуальних підходів до забезпечення національної безпеки й оборони в політичній, економічній, соціальній, військовій, науково-технологічній, екологічній, інформаційній та інших сферах;

– удосконалення системи національної безпеки, реорганізація, створення або ліквідація органів виконавчої влади в цій сфері;

– впровадження політичних, економічних, соціальних, військових, науково-технологічних, інформаційних та інших заходів для протидії реальним і потенційним загрозам національним інтересам України.

Компетенції РНБО передбачають її ключову роль у координації відомств, залучених до системи інформаційної безпеки. Одним із прикладів такого впливу стала діяльність Міжвідомчих комісій з питань інформаційної політики та безпеки при РНБО (2002 та 2009 роки), до складу яких входили міністерства і відомства як гуманітарного, так і силового блоків виконавчої влади.

У квітні 2014 року, в умовах агресії РФ, за указом Президента України був створений інформаційно-аналітичний центр при РНБО, завданням якого стало аналітичне та прогнозне забезпечення діяльності Ради в питаннях координації органів виконавчої влади в інформаційній сфері. Проте діяльність цього центру виявилася короткостроковою (указ втратив чинність 28 травня 2015 року) та обмеженою через його громадську природу.

14 квітня 2017 року, в результаті чергової реорганізації, в структурі РНБО було створено Службу з питань інформаційної безпеки, а 18 жовтня 2019 року – Службу з питань інформаційної безпеки та кібербезпеки. Однак, попри ці внутрішні підрозділи РНБО, існує потреба у створенні постійно діючої міжвідомчої координаційної структури для інформаційної безпеки, подібної до Національного координаційного центру кібербезпеки, який був заснований відповідно до рішення РНБО «Про Стратегію кібербезпеки України» від 27 січня 2016 року.

Основними завданнями такого Центру повинні бути узгодження та координація дій суб’єктів безпеки і оборони, що відповідають за інформаційну безпеку. Діяльність Центру передбачає визначення національних інтересів України в цій сфері, стратегічних підходів до державної інформаційної політики, а також розподіл повноважень і рівня відповідальності залучених структур.

Отже, аналіз інституційного механізму забезпечення інформаційної безпеки в сучасних умовах показує, що його ефективне функціонування можливе за таких умов: розробка та ухвалення Концепції інформаційної безпеки; оновлення законодавства, зокрема внесення змін до законів і положень, що регламентують діяльність суб'єктів інформаційної безпеки, з узгодженням їхніх завдань і функцій; створення механізмів управління, контролю та нагляду з чітким розподілом ролей і повноважень; запровадження відповідальності за недотримання вимог внутрішньої інформаційної безпеки; впровадження системи загальної підготовки суб'єктів до виконання завдань; посилення взаємодії та інформаційного обміну між суб'єктами інформаційної безпеки для ефективного виконання їхніх функцій. Дотримання цих умов сприятиме реалізації ефективної політики інформаційної безпеки, як ключової частини національної безпеки [21].

РОЗДІЛ 3
НАПРЯМКИ УДОСКОНАЛЕННЯ ДЕРЖАВНИХ МЕХАНІЗМІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В КОНТЕКСТІ СУЧАСНИХ ВИКЛИКІВ

3.1 Міжнародний досвід забезпечення інформаційної безпеки та його імплементація в Україні

Наразі міжнародні організації активно співпрацюють для протидії інформаційним ризикам, спільно формуючи політику, адже інформаційна безпека стає важливою складовою міжнародних відносин. З розвитком цифрових технологій зросла необхідність скоординованих зусиль для забезпечення безпеки у цьому напрямі.

Зростання ризиків, пов’язаних із використанням інформаційних технологій подвійного призначення, вимагає узгодженого міжнародного підходу до контролю та регулювання. Країни й міжнародні організації розробляють спільні стратегії, спрямовані на попередження використання таких технологій у військових цілях та для інших загрозливих дій [26].

Міжнародне співробітництво у сфері інформаційної безпеки потребує не лише реагування на загрози, а й проактивного планування, координації та врахування динаміки технологічного розвитку.

Сучасні виклики вимагають об'єднаних зусиль, і такі організації, як ООН, НАТО та ОБСЄ, відіграють ключову роль у формуванні міжнародної інформаційної безпеки. Прийняті рішення базуються на принципах міжнародного права, що визначають стратегії та механізми реагування на новітні загрози. Завдяки участі різних міжнародних гравців створюються механізми колективних дій для забезпечення безпеки у глобальному масштабі, сприяючи миру та стабільності [31].

Також важливо відзначити, що на сесіях Генеральної Асамблеї ООН обговорюються важливі питання інформаційної безпеки. Резолюції, як-от «Роль науки і техніки в контексті міжнародної безпеки і роззброєння» і «Досягнення у сфері інформатизації і телекомунікації», заклали основу для сучасної політики інформаційної безпеки. Вони передбачають контроль за використанням інформаційних технологій у цивільних і військових сферах та протидію деструктивним впливам. Це свідчить про розуміння необхідності створення міжнародних стандартів у сфері інформаційної безпеки й застосування сучасних технологій для захисту.

Обговорення проєкту Конвенції з міжнародної інформаційної безпеки на сесії Генеральної Асамблеї ООН продемонструвало різні підходи держав до визначення понять, оцінки інформаційних загроз і організації міжнародної співпраці у цій сфері. З метою досягнення консенсусу щодо формулювання Конвенції було створено Групу урядових експертів, яка мала провести детальний аналіз проблем інформаційної безпеки та розробити міжнародні принципи регулювання комунікаційних мереж, враховуючи можливість використання сучасних технологій для атак на критично важливі державні та громадські системи [27].

Проте через розбіжності між країнами щодо основних принципів Конвенції її ухвалення відклали, перенісши обговорення на пізніший час. Відмінності у поглядах на регулювання міжнародної інформаційної безпеки ускладнили узгодження тексту документу.

Резолюція «Заохочення відповідальної поведінки держав у кіберпросторі в контексті міжнародної безпеки», ухвалена Генеральною Асамблеєю ООН за підтримки більшості країн-членів, підкреслює необхідність створення безпечного та стабільного кіберсередовища. Вона наголошує на важливості довіри між державами та необхідності розширення можливостей для співпраці з метою зниження ризиків кіберконфліктів.

Аналіз політики НАТО у сфері інформаційної безпеки свідчить про активну

роль Естонії у співпраці з країнами Східного партнерства, включаючи Україну та Грузію. Спільні заходи включали підготовку кадрів, технічні консультації та забезпечення обладнанням для протидії інформаційним загрозам. У зв'язку з агресією РФ, у тому числі під час конфлікту на Сході України та окупації Криму, Естонія закликала союзників по НАТО надати фінансову допомогу Україні у відповідь на кібератаки з боку Росії. Естонія також перерахувала 100 тисяч євро у трастовий фонд НАТО для підтримки інформаційної безпеки України та організувала навчання українських фахівців із кіберзахисту [29].

Україна може стати цінним партнером НАТО, поділившись досвідом протидії російським кіберзагрозам і негативним інформаційним впливам, що становлять загрозу демократичним процесам не лише у Європі, а й на міжнародному рівні.

Приєднання України до ініціативи «Партнерства розширених можливостей НАТО» є важливим кроком для посилення співпраці у сфері інформаційної безпеки. Це розширює можливості для раннього планування в умовах конфліктів, обміну розвідувальною інформацією та участі у навчаннях з кібероборони. Також це відкриває доступ до посад у Міжнародному військовому штабі НАТО та інших командних структурах для здобуття досвіду управління в сфері інформаційної безпеки.

Співпраця України з НАТО через Комплексний пакет допомоги сприяє підвищенню стандартів військово-політичної організації країни. Пакет включає підтримку через трастові фонди та реалізацію Річної національної програми як інструменту для здійснення реформ.

У межах цього практичного співробітництва було затверджено Указ про Річну національну програму під егідою Комісії Україна-НАТО на 2022 рік. Крім того, було прийнято План заходів для реалізації Концепції підвищення інформування суспільства з питань євроатлантичної інтеграції України. Ці ініціативи передбачають роботу спільних груп Україна-НАТО у сфері військової реформи, оборонно-технічної співпраці та інформаційної безпеки, а також

взаємодію в галузі науки та екології [27].

ОБСЄ (Організація з безпеки та співробітництва в Європі) виступає ключовим майданчиком для обговорення питань безпеки в Європі, Північній Америці та в державах, що утворилися після розпаду СРСР. Спочатку ця організація була створена для забезпечення безпеки, прав людини, демократії, розвитку медіа в зонах конфліктів та моніторингу кризових ситуацій.

ОБСЄ наголошує на актуальності інформаційних загроз і закликає зацікавлені сторони до пошуку рішень у сфері кібербезпеки, підкреслюючи важливість міжнародного права як основи для регулювання кіберпростору. Конференція «Загальний підхід до кібербезпеки: визначення майбутньої ролі ОБСЄ» стала вагомим кроком для формування стратегії ОБСЄ в галузі інформаційної безпеки. На ній обговорювалися проблеми зловживання кіберпростором та аналізувалися заходи з боку міжнародних і регіональних організацій, що впливають на безпеку у регіоні ОБСЄ. Основними темами конференції були розробка комплексного підходу ОБСЄ до кібербезпеки, обмін досвідом між країнами, формування правил поведінки держав у кіберпросторі та прийняття рішень для посилення кібербезпеки.

За підсумками конференції були ухвалені новаторські рекомендації щодо заходів зі зміцнення довіри у сфері інформаційної безпеки, які включали взаємодію ОБСЄ з приватним сектором і ключовими інфраструктурними провайдерами, розробку спільних підходів до управління кібербезпекою для підвищення прозорості та безпеки у регіоні ОБСЄ [31].

Політика Європейського Союзу у сфері інформаційної безпеки передбачає впровадження передових цифрових, квантових технологій і систем штучного інтелекту, а також удосконалення інформаційного озброєння. Основні завдання цієї політики – використовувати комунікаційні інструменти та протистояти деструктивним інформаційно-психологічним впливам у сучасному геополітичному контексті.

Експерти відзначають, що інформаційна безпека Європи визначається

рішеннями та стратегічними документами ЄС, а також національними стратегіями країн із значним економічним і технологічним потенціалом, таких як Франція та Німеччина. Особливу увагу приділяють новим викликам у сфері інформаційної безпеки, що виникають у зв'язку зі змінами в регіональній безпеці.

Сучасні підходи ЄС і ключових країн Європи спрямовані на захист інформаційного суверенітету держав і боротьбу з новими інформаційними загрозами. Реформування національних стратегій стає необхідним через нестабільність міжнародного інформаційного середовища та стрімке впровадження інноваційних технологій у захист критичної інфраструктури.

Політика інформаційної безпеки у провідних європейських країнах, таких як Велика Британія, Франція та Німеччина, спрямована на захист критично важливих секторів та протидію зовнішнім загрозам, зокрема інформаційно-психологічним операціям, кібертероризму, кіберзлочинності й деструктивним інформаційним впливам.

Для вирішення цих питань необхідно посилити координацію між наднаціональними інститутами ЄС і державами-членами, розробити спільні стратегії протидії кіберзлочинності та ворожій пропаганді. Ці дії мають стати частиною стратегічного бачення європейської громадськості щодо посилення оборонних можливостей і реформування європейських механізмів колективної безпеки з урахуванням національних інтересів [29].

Інформаційна безпека розглядається як стратегічна концепція, що охоплює всі аспекти життя суспільства [45].

Сучасні дослідження у сфері інформаційної безпеки в європейських країнах зосереджені на аналізі доктрин і практичних підходів, що використовуються для захисту інформації. Особлива увага приділяється забезпеченню конфіденційності інформаційних ресурсів та питанням державно-приватного партнерства в інформаційній безпеці.

Як зазначають дослідники тенденції й проблеми підтверджують наявність

суперечностей у політиці інформаційної безпеки в сучасних міжнародних відносинах. Експерти наголошують на необхідності врахування національними стратегіями інформаційної безпеки швидких змін у політичній ситуації, а також еволюції концепцій сили в міжнародних відносинах. У цьому контексті важливо впроваджувати механізми, що забезпечують національну інформаційну безпеку як невід'ємну частину зовнішньої і безпекової політики [31].

Згідно з дослідженням RAND Corporation , визначе тенденції у сфері інформаційної безпеки, які можуть вплинути на міжнародну співпрацю та викликати нові типи інформаційних загроз. Уряди європейських країн, враховуючи ці тенденції, вносять корективи в національні стратегії інформаційної безпеки для адаптації до поточних викликів.

Основною проблемою інформаційної безпеки в міжнародному контексті визнано можливі порушення конфіденційності державних, корпоративних і приватних інформаційних ресурсів. Ці порушення здатні завдати серйозної шкоди функціонуванню критичної інфраструктури та поставити під загрозу стандарти правового захисту інформаційної безпеки.

Глобальне дослідження стану інформаційної безпеки наголошує, що інформаційна безпека, конфіденційність даних та етичні стандарти є тісно взаємопов'язаними аспектами, які потребують ефективного управління ризиками. У зв'язку з цим компанія PricewaterhouseCoopers розробила нову платформу для захисту інформаційної безпеки та конфіденційності, яка допомагає у протидії загрозам, підтримці трансформаційних процесів та стимулюванні зростання. Платформа передбачає інтеграцію заходів з інформаційної безпеки та методів захисту даних, зокрема застосування сучасних технологій шифрування, протидію кібератакам та контроль доступу до даних.

Європейське агентство з мережевої та інформаційної безпеки (ENISA) координує зусилля ЄС і європейських країн у галузі мережевої та інформаційної безпеки. Агентство було створено для забезпечення захисту інформаційного

суверенітету та інфраструктури Європи, а також розвитку співпраці з представниками приватного сектора. Німеччина, Франція та Велика Британія активно співпрацюють з ENISA, розробляючи національні стратегії інформаційної безпеки. Наприклад, Німеччина ухвалила «Національний план захисту інформаційної інфраструктури» для посилення кібербезпеки. Франція спрямовує зусилля на захист від кіберзлочинності, а Велика Британія акцентує увагу на інноваціях та покращенні сервісів у сфері інформаційних технологій.

ENISA також підтримує розробку практичного посібника для формування національної політики інформаційної безпеки, який містить рекомендації для підвищення ефективності заходів з кібербезпеки та протидії загрозам. Крім того, посібник включає стратегії для попередження й реагування на можливі загрози з метою покращення загального рівня безпеки.

Регламент ЄС про захист персональних даних (GDPR), що набув чинності у 2018 році, є основним нормативним актом, який регулює захист персональних даних в ЄС. Дослідження показують, що 67% опитаних знають про існування GDPR, але лише 36% обізнані з його змістом, що вказує на потребу в додатковій освіті.

У зв’язку зі зростанням загроз від деструктивної пропаганди, фейкових новин та дезінформації ЄС ухвалив рішення посилити заходи протидії пропаганді, зокрема російській. У Великій Британії ці функції виконує Національний підрозділ Ради нацбезпеки, у Франції – спеціалізовані державні установи, а в Німеччині діють програми проти дезінформації. Координація таких дій на рівні ЄС має стратегічне значення, підтверджуючи роль організації як лідера у сфері європейської інформаційної безпеки.

Європейські стандарти інформаційної безпеки підтримуються всіма країнами-членами ЄС, що підтверджує єдність підходів до оцінки інформаційних загроз. Однак слід зазначити, що провідні європейські держави демонструють відмінності у своїх підходах через національні пріоритети у сфері безпеки [32].

Інформаційна стратегія Великої Британії враховує як міжнародні, так і внутрішні інтереси у створенні системи захисту від сучасних інформаційних загроз. У документі «Стратегія національної безпеки» визначено критичні виклики, серед яких кібератаки з боку іноземних держав, злочинних та екстремістських угруповань, кібершпигунство і хакерство, що можуть поставити під загрозу критично важливу інфраструктуру, розглядаються як основні загрози для безпеки країни.

У рамках реалізації цієї стратегії уряд Великої Британії запровадив такі проєкти, як створення громадсько-приватних «хабів» для обміну інформацією про кіберзагрози між державними структурами та приватними компаніями з метою протидії кібератакам. Крім того, стратегія передбачає формування спеціалізованих кіберпідрозділів для боротьби з інформаційними злочинами та застосування чинних санкцій щодо кіберзлочинців.

Для Франції поняття «цифровий суверенітет» є ключовим пріоритетом у сфері інформаційної безпеки, що означає здатність країни самостійно приймати рішення щодо захисту національної безпеки, інформаційної інфраструктури та інформаційного середовища. Вплив проросійської пропаганди та зовнішні маніпуляції громадською свідомістю створюють загрози для інформаційної безпеки уряду і суспільства Франції.

Особливу увагу приділяють кіберзагрозам, таким як кіберзлочинність, кібершпигунство та хакерські атаки на інфраструктурні об’єкти, які розглядаються як напади на критично важливі сфери країни і вимагають правового регулювання на національному рівні [46].

Франція здійснила значні зміни в політиці безпеки та оборони, визначивши інформаційну безпеку одним із пріоритетів національної безпеки у своїх стратегічних документах, що відображає постійний акцент на модернізацію у цій галузі. Національне агентство ANSSI (Agence nationale de la sécurité des systèmes d'information), створене у 2009 році, стало центральним відомством Франції з

питань захисту інформаційних систем і критичної інфраструктури. У Міністерстві оборони також сформовано Генеральний директорат з інформаційного захисту, що ініціював розробку стратегії інформаційної безпеки, яка враховує досвід інших європейських країн, зокрема у створенні резервних мереж. Ця стратегія передбачає підтримку проєктів державно-приватного партнерства у сфері інформаційної безпеки, що залучають державні установи, великі промислові компанії, приватний сектор, наукові й освітні організації.

У Франції розвиток доктрини та практики інформаційної безпеки був спрямований на реалізацію національної цифрової стратегії. Основними цілями цієї стратегії були: захист національних інформаційних систем і критично важливої інфраструктури, охорона приватного життя та персональних даних громадян, підтримка місцевих компаній у секторі цифрових технологій і зміцнення впливу Франції на міжнародній арені, зокрема в наданні підтримки менш захищеним державам і загальному зміцненні кібербезпеки.

Для посилення інформаційного захисту Франція планувала збільшити штат Агентства мережевої та інформаційної безпеки, а також Міністерства оборони та внутрішніх справ. Серед додаткових заходів – забезпечення кібербезпеки для суспільно важливих недержавних інформаційних систем та підтримка розробок систем виявлення і захисту від кібератак для малого та середнього бізнесу. Це підкреслює прагнення Франції до підвищення рівня інформаційної безпеки та захисту своїх цифрових ресурсів.

Важливу роль у забезпеченні інформаційної безпеки Німеччини відіграє Федеральна служба інформаційної безпеки (BSI). Ця служба є частиною Федерального міністерства внутрішніх справ, яке, окрім іншого, відповідає за внутрішню безпеку країни, захист конституційного ладу, а також протидію тероризму, екстремізму, шпигунству і саботажу. Згідно із Законом «Про Федеральне відомство безпеки інформаційних систем», BSI займається збором та аналізом інформації про кіберзагрози, виявляє нові види кібератак і розробляє

відповідні заходи протидії. Крім того, BSI спільно з НАТО та ЄС виконує такі функції, як оцінка ризиків від впровадження інформаційних технологій; розробка критеріїв, методів і засобів тестування для перевірки захищеності національних комунікаційних систем; оцінка рівня захищеності інформаційних систем та видача відповідних сертифікатів; надання дозволів на впровадження інформаційних систем у важливих державних об’єктах тощо.

Основна відповідальність за забезпечення кібербезпеки Польщі лежить на Агентстві внутрішньої безпеки (ABW). У 2013 році Агентство розробило Стратегію кібербезпеки Польщі та ініціювало створення Центру криптології при Міністерстві національної оборони для захисту інформації, кібероборони та проведення наступальних кібероперацій. ABW також створило урядову команду реагування на комп'ютерні інциденти (CERT), мета якої – посилення можливостей державних органів у захисті від кіберзагроз, зокрема атак на інфраструктуру IT-систем та мереж, збій у яких може становити серйозну загрозу для життя, здоров'я людей, національного багатства, навколишнього середовища, а також призвести до фінансових втрат та порушення роботи органів влади.

Зростання інформаційних гібридних загроз, таких як пропаганда, дезінформація та психологічне залякування, спричинених як державними, так і недержавними структурами (зокрема, терористичними організаціями), спонукало Бюро національної безпеки Польщі (BBN) у 2015 році розробити національну Доктрину інформаційної безпеки. Для протидії цим загрозам доктрина рекомендує ідентифікувати інформаційне середовище та визначати дружні, нейтральні й ворожі суб’єкти. Доктрина інформаційної безпеки Польщі вважається робочим документом на підтримку Стратегії національної безпеки країни

Ізраїль є ще одним прикладом країни з розвиненою системою кіберзахисту. Національне бюро кібербезпеки Ізраїлю тісно співпрацює з державними структурами та приватним сектором, щоб захищати критичну інфраструктуру та інформаційні системи. Важливою особливістю ізраїльської моделі є її здатність

швидко й гнучко реагувати на загрози, а також активне залучення приватних компаній до розробки засобів кіберзахисту. В Україні цей досвід застосовується через посилення співпраці держави з ІТ-компаніями та підтримку стартапів, що займаються розробкою рішень у сфері кібербезпеки.

Крім того, вагомим аспектом міжнародного досвіду є протидія дезінформації, яку активно впроваджують країни Північної Європи, зокрема Швеція та Фінляндія. Ці держави розробили національні стратегії, що включають заходи з протидії дезінформації в освітню систему та підвищення рівня медіаграмотності населення. Громадяни навчаються критично оцінювати інформацію та розпізнавати фейкові новини. Україна також рухається в цьому напрямі, співпрацюючи з міжнародними організаціями для створення програм медіаграмотності та боротьби з дезінформацією, особливо серед молоді та державних службовців.

Кібертероризм розглядається як серйозна загроза: злочинні організації та терористичні групи використовують інтернет для пропаганди, вербування, фінансування та організації терактів, що вимагає посилення заходів безпеки [27].

Стратегії інформаційної безпеки Сполучених Штатів залежать від політичних і геополітичних пріоритетів кожної адміністрації, що впливає на національні інтереси, зовнішню політику та загальні підходи до безпеки. США розробляють комплексні стратегії, що включають міжнародну співпрацю, дипломатію, військові можливості й захист кіберпростору. З розвитком інтернету та поширенням технологій у стратегіях США зростає компонент інформаційної безпеки, включаючи боротьбу з кібератаками, дезінформацією та втручаннями, а також співпрацю з іншими країнами для забезпечення глобальної кібербезпеки [50].

Інформаційна безпека в сучасному світі стала одним із центральних аспектів, що привертає увагу вчених, політологів і дослідників. Стрімкий розвиток інформаційних технологій і їхній вплив на різні сфери суспільного життя, включаючи військовий і цивільний сектори, створює нові виклики й загрози, які потребують ретельного аналізу та прогнозування.

Американські дослідники і політологи активно займаються вивченням питань інформаційної безпеки, розробкою захисних стратегій і дослідженням впливу інформаційно-комунікаційних технологій на сучасне суспільство. Вони аналізують розвиток концепцій інформаційної безпеки, визначають ключові підходи до використання різних видів впливу та оцінюють зміни у сфері безпеки як важливий фактор для формування міжнародних відносин і світового порядку. Ці наукові напрацювання допомагають формувати стратегії й політики у галузі інформаційної безпеки, сприяючи більш обґрунтованому підходу до подолання викликів у сучасному інформаційному середовищі.

Стратегії інформаційної безпеки в США за останні десятиліття еволюціонували, що позначилося на формуванні сучасної міжнародної системи. У цьому контексті використовувався підхід «жорсткої сили», який полягає у здатності держави впливати на політику інших країн через економічний і військовий тиск.

Концепція «жорсткої сили» бере свій початок у роботах таких мислителів, як Нікколо Макіавеллі в «Державці» та Томаса Гоббса у «Левіафані», які розглядали її як вплив через військову та економічну перевагу. Ганс Моргентау трактував «жорстку силу» як одну з форм політичної влади, а Колін Грей – як здатність до застосування військової сили в політиці XXI століття.

У Стратегії національної безпеки США визначалися основні напрями адаптації збройних сил до нових умов і викликів, зумовлених стрімким розвитком технологій і змінами в міжнародному середовищі. Було виділено кілька ключових аспектів:

1. Розширення можливостей. Стратегія спрямовувалася на підвищення військових можливостей, виходячи за межі звичайних методів стримування для ефективного реагування на нові загрози.

2. Національна спеціалізація. Особлива увага приділялася розвитку оборонних сфер, таких як ядерні, космічні та передові технології, що впливали на формування наступальних і оборонних програм.

3. Глобальна орієнтація. Стратегія передбачала створення меншого за чисельністю, але більш гнучкого і глобально орієнтованого військового складу, здатного оперативно реагувати на зміни, пов'язані з інформаційними технологіями та непередбачуваними ситуаціями.

Ці напрями заклали основу для змін у військовій сфері з метою адаптації до нових викликів, спричинених швидким технологічним прогресом і геополітичними зрушеннями.

Під час президентства Б. Обами особлива увага приділялася посиленню інформаційного аспекту в стратегіях національної безпеки та оборони США. Інформаційні операції стали ключовим інструментом у міжнародних відносинах, включаючи психологічний вплив, дезінформацію, кібератаки та електронні військові дії, спрямовані на підрив інформаційних систем противника.

Значну увагу також приділили захисту критично важливої інфраструктури США та вдосконаленню систем протидії кібератакам і загрозам цифрової безпеки. Концепція «Більш розумна, більш безпечна Америка», розроблена Центром американського прогресу, стала основою зовнішньої і безпекової політики адміністрації Обами. Вона пропонувала «розумну силу» як альтернативу до попередніх стратегій силового втручання, зосереджуючи увагу на невійськових інструментах захисту національних інтересів.

У рамках цієї концепції, яку підтримував і розвивав Ф. Вонг-Діаз, підкреслювалося, що стратегія не обмежує дії США на світовій арені та не передбачає значного скорочення військових витрат, а натомість стимулює міжнародну співпрацю для забезпечення безпеки із застосуванням високих технологій.

Кібербезпека була визначена одним із ключових напрямів стратегії національної безпеки, поряд із захистом від ядерних і біологічних загроз. Обама підкреслював значення кібербезпеки як важливого елементу національної оборони, де захист інформаційної інфраструктури та цифрового простору розглядався як

пріоритет національної безпеки [30].

Підхід до інформаційної безпеки, який формувався у період президентства Б. Обами, передбачав трансформацію ролі кіберпростору в стратегії національної безпеки США, що включало його як специфічну сферу захисту національних інтересів в умовах зростання міжнародних загроз. У своїй промові у Вест-Пойнті у 2014 році Обама наголосив на потребі нових принципів зовнішньої та безпекової політики США, що відповідають сучасним геополітичним реаліям і викликам. Особливу увагу було приділено ситуації з агресією Росії проти України, яку Обама та його адміністрація підтримували як ключового партнера для зміцнення безпеки в Європі та в світі. Хоча Будапештський меморандум не згадувався, США і ЄС висловили готовність надати Україні політичну, військову та фінансову підтримку, а також допомогти в реформах, боротьбі з корупцією та протистоянні інформаційним загрозам.

Підтримка України стала частиною зовнішньополітичної стратегії адміністрації Обами, спрямованої на розвиток демократії і безпеки в регіоні. У період президентства Д. Трампа було прийнято Національну кіберстратегію США, яка зосередилася на захисті мереж, інформації та критично важливої інфраструктури від кіберзагроз. До пріоритетів стратегії увійшли боротьба з кіберзлочинністю та реагування на кіберінциденти, а також міжнародна ініціатива з кіберстримування, спрямована на координацію з іншими країнами у протидії кіберзагрозам. Ініціатива включала обмін розвідданими, підтвердження претензій щодо кібератак, публічні заяви та спільні заходи проти кіберзлочинців. Крім того, стратегія передбачала розширення американського впливу для забезпечення відкритого та безпечного Інтернету, а також нарощування міжнародного інформаційного потенціалу.

Ці заходи підкреслюють значення інформаційної безпеки для США, особливо з огляду на те, що інформаційні технології дедалі частіше розглядаються як новий вид глобальної загрози. Для гарантування національної безпеки США формують

стратегії протидії інформаційній агресії та підтримки міжнародних і національних безпекових механізмів. До стратегій входять створення захисних механізмів від інформаційних загроз, зміцнення критичної інфраструктури, розробка ефективних механізмів реагування на кіберінциденти та боротьба з дезінформацією. Реалізація таких стратегій є ключовим елементом забезпечення стабільності й безпеки у державному, міжнародному та кіберпросторі.

Отже, міжнародний досвід у сфері інформаційної безпеки надає Україні важливі інструменти для створення ефективної системи захисту інформаційного простору. Впровадження цих підходів сприяє зміцненню національної стійкості перед інформаційними загрозами, покращує координацію між державними установами та приватним сектором і підвищує рівень захисту критично важливих інформаційних систем у контексті глобальних викликів.

3.2 Інформаційні технології та їх роль у протидії інформаційним загрозам

З часів XX століття, коли ЕОМ займала цілу кімнату, магнітофон був розміром з шафу, а про мобільний зв'язок ніхто й не мріяв, минуло чимало часу. Однак система комунікацій зазнала кардинальних змін. Змінилися також методи розвідки у всіх країнах світу, як і цінність інформації. Сьогодні ми частіше купуємо і продаємо інформацію, і наше життя значною мірою залежить від інтернету, телебачення та мобільного зв'язку. Ця залежність тільки зростає. У таких умовах забезпечити конфіденційність будь-якої інформації стає практично неможливим [33].

У світі тривають перегони за технологіями, доступом до конфіденційної та компрометуючої інформації, а також за захист комунікаційних систем. Наймогутніші держави вкладають у ці сфери величезні кошти, що сягають

мільярдів доларів. Пентагон (США) визнав інформаційний простір однією з арен для ведення бойових дій нарівні з землею, водою, повітрям і космосом. Інформаційні війни стали реальністю навіть у мирних країнах.

В умовах повномасштабного вторгнення РФ в Україну, яке почалося 24 лютого 2022 року, особливу актуальність набуло питання захисту демократії як у країнах з усталеними демократичними традиціями, так і в країнах, які переживають перехід до демократії. Це стосується, зокрема, держав Вишеградської групи (Польща, Словаччина, Угорщина, Чехія), що пройшли етап інтеграції до ЄС та захистили свої інформаційні простори від гібридних загроз, таких як інформаційно-психологічні операції та поширення дезінформації. Досвід цих країн у впровадженні новітніх інформаційних технологій для забезпечення свободи слова є позитивним прикладом і для України, яка також розвиває інформатизацію та цифровізацію у сфері публічної діяльності. Це сприяє прозорості роботи державних органів, зокрема парламенту, який є єдиним законодавчим органом влади. Важливими інноваційними технологіями стали такі інструменти, як:

– хмарні послуги та сервіси;
– Інтернет речей (The Industrial Internet of Things – IIoT);
– технології доповненої реальності (Augmented Reality – AR);
– технології Big Data;
– блокчейн і біткойн (Blockchain, Bitcoin).

Сучасна публічна політика та управління стикаються з новими викликами, пов’язаними з необхідністю вивчення позитивного досвіду інших країн у застосуванні новітніх інформаційних технологій у політико-управлінській діяльності. [37]

Дослідження політичних змін в інформаційному просторі України та її сусідів, зокрема країн Вишеградської групи, стає особливо важливим в умовах гібридних війн. Адже сьогодні український парламент та інші органи державної влади стикаються з низкою складних політико-правових викликів, що впливають як

на їхню ефективність, так і на стабільність політичної системи в цілому.

Досвід країн Вишеградської групи (Польща, Словаччина, Угорщина, Чехія) показує, що їхнє об'єднання у 1991 році для тіснішої співпраці в питаннях європейської та євроатлантичної інтеграції дало позитивні результати. Уже в 2004 році ці країни стали членами ЄС, успішно протидіяли інформаційним загрозам і забезпечували надійну інформаційну безпеку. Це стало можливим завдяки чіткому визначенню пріоритетних цілей «Вишеградської четвірки» – інтеграції до ЄС і НАТО. Україна ж пройшла складний шлях до вибору свого геополітичного курсу, і лише в 2023 році отримала дозвіл на консультації з країнами-членами ЄС щодо майбутнього вступу [35].

Відмінність процесу інтеграції Вишеградських країн у ЄС полягає в тому, що вони вступали в мирний час, тоді як Україна розпочала цей шлях у 2019 році, після тимчасової анексії Криму Росією. Тоді парламент ухвалив Закон «Про внесення змін до Конституції України», ініційований Президентом України, який закріпив стратегічний курс держави на вступ до ЄС та НАТО. Так, Конституція України закріпила незворотність цього курсу в умовах російської агресії, яка супроводжується численними інформаційними загрозами, що деструктивно впливають на суспільну свідомість громадян.

В Україні процеси впровадження інноваційних технологій у державне управління перебувають на етапі становлення та розвитку. Наприклад, практична реалізація проєкту «Дія» розпочалася лише після 2019 року, ставши успішною ініціативою сучасної влади, яка втілює концепцію «Держава в смартфоні. Держава, орієнтована на людину».

На нинішньому етапі розвитку України, під впливом змін в політичному інформаційному просторі, формується нова система суспільних і політичних цінностей та нові завдання для органів публічної влади, які відповідають вимогам єдиного інформаційно-комунікаційного простору, де важливими стають діалог культур, суспільний консенсус і толерантність. Основою цих цінностей є

узгодженість між суб'єктами публічної влади в питаннях розвитку держави, територіальних громад та громадянського суспільства загалом. Це стає можливим за умов надання органам влади сучасних інформаційних і інноваційних технологій [36].

Аналіз застосування інноваційних інформаційних технологій як засобу політичної комунікації показав, що «розвиток суспільства без інформаційно-комунікаційного простору неможливий. Переходячи до інформаційного суспільства, держава розгортає інформаційну інфраструктуру в мережі, що дозволяє виконувати широкий комплекс державних функцій». Процес формування електронної державності успішно відбувається в багатьох країнах, а інноваційні медіатехнології, які забезпечують постійну взаємодію між державою і суспільством, отримали назву «електронний уряд».

За результатами аналізу сайтів народних депутатів України IX скликання встановлено, що більшість із них мають особисті вебсайти та використовують різні цифрові канали (Telegram, Instagram, чат-боти тощо) для інформування своїх виборців і громадян.

Аналіз проблеми показав, що сучасна масова комунікація постійно розвивається, збільшуючи кількість каналів для розповсюдження інформації. При цьому нові ЗМІ не замінюють попередні засоби комунікації, а займають своє місце, маючи специфічні функції в інформаційно-комунікаційному просторі [47].

Сучасні інноваційні технології виводять публічне управління на новий рівень: вони забезпечують прозорішу комунікацію між владою (зокрема, парламентом) і громадянським суспільством, сприяють зменшенню бюрократії, скорочують паперовий документообіг і оптимізують контроль за діяльністю чиновників [34].

Проведений аналіз трансформацій в інформаційному просторі України і країн Вишеградської групи свідчить про необхідність першочергових кроків:

– створення умов для розвитку незалежних ЗМІ без цензури, підтримки

інноваційного сектору та електронної взаємодії в органах публічної влади, міжнародної співпраці та обміну досвідом з країнами ЄС;

– підвищення інформаційної компетентності державних службовців, зокрема парламентарів і їхніх помічників;

– посилення прозорості діяльності державних органів, підтримка громадських медіаорганізацій, що представляють інтереси громадян;

– активної протидії дезінформації.

Політична трансформація інформаційного простору відбувається завдяки сучасним інформаційно-комунікаційним і інноваційним технологіям, зокрема:

– засобам масової комунікації, телекомунікаційним мережам, супутниковим і мобільним комунікаціям, Інтернету та іншим соціальним комунікаційним засобам (інформаційні технології);

– технопаркам, кластерам, інноваційним інкубаторам, спільним лабораторіям, хмарним обчисленням, штучному інтелекту, Інтернету речей і блокчейну (інноваційні технології).

Більшість з цих технологій вже застосовується в органах публічної влади України, однак частина з них потребує подальшого впровадження і навчання державних службовців, парламентарів та їхніх помічників для забезпечення оперативності та об'єктивності ухвалення політичних рішень, що мають спиратися на достовірні дані.

У сучасному світі глобалізації кіберзагрози набувають транснаціонального характеру, що вимагає від держав та міжнародних організацій тісної координації для ефективної протидії викликам в області інформаційної безпеки. Досвід різних країн у створенні національних стратегій кібербезпеки, вдосконаленні законодавства, розбудові відповідних структур і розвитку міжнародного співробітництва є важливим для покращення підходів до забезпечення інформаційної безпеки. Таким чином, вивчення світового досвіду стає невід’ємним елементом у розробці ефективної системи інформаційної безпеки, здатної

своєчасно реагувати на сучасні загрози і захищати національні інтереси в глобальному інформаційному просторі [48].

Сучасний етап інформаційної боротьби показав, що український інформаційний простір потребує додаткового захисту від зовнішнього інформаційно-психологічного впливу. Відтак, забезпечення інформаційної безпеки України передбачає розширення телекомунікаційних технологій та захист державних інформаційних ресурсів від несанкціонованого доступу.

На основі проведеного дослідження можна виділити шляхи імплементації міжнародного досвіду в українську практику забезпечення інформаційної безпеки, а саме:

1. Прийняття міжнародних стандартів. Україна має впроваджувати міжнародні стандарти інформаційної безпеки, як-от ISO/IEC 27001, що визначають вимоги до створення, реалізації, підтримки й удосконалення систем управління інформаційною безпекою.

2. Міжнародна співпраця. Поглиблення співробітництва з міжнародними організаціями, такими як ЄС, НАТО та ООН, для обміну інформацією щодо кіберзагроз, кращими практиками та спільної розробки заходів протидії кіберзлочинності. Спільні тренінги та участь у міжнародних ініціативах і програмах з кібербезпеки сприятимуть підвищенню національної безпеки та інтеграції України в глобальну систему кіберзахисту.

3. Розвиток законодавчої бази. Україні слід вдосконалювати законодавство у сфері інформаційної безпеки, орієнтуючись на міжнародний досвід і стандарти. Це передбачає оновлення чинних законів, створення нових нормативних актів та правових механізмів, які забезпечать ефективний захист інформації в державному і приватному секторах, а також належну відповідальність за порушення в цій сфері.

4. Розвиток державно-приватного партнерства. Забезпечення інформаційної безпеки вимагає тісної співпраці між державою і приватними

компаніями. Таке партнерство сприятиме обміну інформацією щодо кіберзагроз, спільній розробці технологічних рішень та впровадженню інноваційних методів захисту інформації.

5. Забезпечення доступу до сучасних технологій. Для ефективної реалізації заходів з інформаційної безпеки важливо забезпечити доступ до новітніх технологій на всіх рівнях, що включає розвиток інфраструктури, підтримку і модернізацію державних та приватних інформаційних систем.

6. Впровадження технічних засобів захисту. Ключовим аспектом інформаційної безпеки є застосування сучасних технічних засобів захисту, зокрема, систем шифрування, брандмауерів, систем виявлення та запобігання вторгненням.

Запропоновані заходи сприятимуть підвищенню рівня інформаційної безпеки в Україні та допоможуть ефективно адаптувати найкращі міжнародні практики до національних умов.

Основними елементами успішної практики є формування комплексної правової бази для регулювання інформаційного простору, впровадження сучасних технологій захисту, а також активна взаємодія між державними органами, приватним сектором і громадянським суспільством. У міжнародному досвіді значущу роль відіграє співробітництво на рівні міждержавних угод, участь у міжнародних організаціях та обмін інформацією між країнами для підвищення ефективності заходів протидії глобальним кіберзагрозам.

Досвід інших країн свідчить, що для України важливо адаптувати найкращі практики з урахуванням національних потреб і викликів. Інтеграція міжнародних стандартів, розвиток власної правової бази, посилення співпраці між державними та приватними структурами, а також підвищення рівня інформаційної грамотності населення є ключовими напрямками для забезпечення надійної інформаційної безпеки держави в сучасних умовах.

ВИСНОВКИ

В результаті виконання магістерського кваліфікаційної роботи було проведено аналіз теоретичних основ і практичних аспектів механізму забезпечення інформаційної безпеки; розкрито сутнісні ознаки та особливості, структури окресленої категорії. Таким чином, це дозволило зробити наступні висновки:

1. Досліджено сутність та основні компоненти інформаційного простору як елементу системи національної безпеки України.

Сутність, зміст і функції інформаційного простору варто розглядати як складову частину соціального простору. Інформаційний простір спрямований на поширення інформації в межах соціального простору, що сприяє розвитку процесів у соціальній реальності. Завдяки цьому інформаційний простір, об’єднуючи різні сфери людської діяльності, виступає як засіб передачі знань, інструмент для комунікації, взаємодії та формування прийнятих соціальних норм мислення та поведінки.

Зміст інформаційного простору визначають характеристики суб'єктів, які діють у цій сфері соціальної реальності. Цими суб'єктами можуть бути окремі особи, групи, соціальні спільноти, соціальні інститути та організації з різними статусами та цілями. До інформаційних ресурсів, якими користуються активні суб’єкти, належать засоби масової інформації, інтернет-ресурси та бібліотеки різних напрямів. Функціонування інформаційного простору створює передумови для його соціальної ролі, виконуючи інтеграційну, комунікаційну, соціальну, геополітичну та інформаційну функції.

Доцільно також розширити уявлення про функціональність інформаційного простору, додавши безпекову функцію, що стосується захисту інформаційних процесів, забезпечення безпеки та запобігання загрозам у соціальній реальності.

2. Вивчено вплив інформаційних загроз на стан національної безпеки

України, зокрема в контексті сучасних викликів.

Необхідність глибшого дослідження та розробки чіткого визначення поняття «загроза» є актуальною і спрямована на формування ефективної системи моніторингу та управління загрозами й іншими ризиками для інформаційної безпеки держави.

Для запобігання й протидії існуючим та потенційним загрозам у сфері інформаційної безпеки стратегічне завдання держави полягає у створенні механізму забезпечення інформаційної безпеки. Цей механізм передбачає системну діяльність, комплекс заходів та державно-правових інституцій, які мають забезпечити реалізацію національних інтересів у інформаційній сфері, захист прав громадян та суспільства, попередження інформаційних конфліктів та оперативне реагування на них. З огляду на зростання глобалізації інформаційно-комунікаційних мереж, важливо, щоб не лише держави, а й міжнародні організації сприяли співпраці у протидії різним формам інформаційної агресії.

3. Проаналізовано нормативно-правове забезпечення інформаційної безпеки в Україні, визначивши його сильні та слабкі сторони.

Українське законодавство забезпечує базовий рівень регулювання інформаційної безпеки через Конституцію України, закони «Про національну безпеку України», «Про захист інформації в інформаційно-комунікаційних системах» та інші. До сильних сторін можна віднести комплексність правових норм та їх спрямованість на захист інформаційних прав громадян. Водночас недоліками є відсутність узгодженості між законодавчими актами, недостатня адаптація до сучасних викликів у сфері кібербезпеки та слабкість механізмів реалізації існуючих норм.

4. Оцінено інституційні механізми забезпечення інформаційної безпеки держави та їхню ефективність у сучасних умовах.

Розробка інституційного механізму з чітко визначеними установами, які відповідають за інформаційну політику, та одночасне вдосконалення системи

координації цього механізму є важливими завданнями для керівництва країни – Президента України, Верховної Ради та Кабінету Міністрів – у контексті забезпечення інформаційної безпеки та протидії загрозам. За наявності політичної волі, ефективний інституційний механізм може стати значущим політичним, силовим та гуманітарним засобом боротьби з антидержавними інформаційними впливами і стримування агресії в умовах гібридної війни.

Подальші дослідження мають зосередитися на визначенні шляхів для встановлення двосторонньої та багатосторонньої співпраці між міністерствами та відомствами, як на горизонтальному, так і на вертикальному рівнях у системі інформаційної безпеки. Крім того, важливо окреслити інструменти координації учасників реалізації та захисту державної інформаційної політики на рівні РНБО, щоб сформувати стратегічний підхід держави до інформаційної сфери і максимально ефективно використовувати існуючий інституційний потенціал для протидії інформаційним впливам агресора.

Отже, враховуючи глобальний масштаб інформаційних загроз, Україна активно інтегрує кращі міжнародні практики у свою національну систему інформаційної безпеки. Це охоплює як нормативно-правові зміни, так і інституційні заходи, серед яких створення нових структур для координації кіберзахисту, співпраця з міжнародними партнерами та впровадження сучасних технологій для захисту критичної інформаційної інфраструктури.

Таким чином, міжнародний досвід у сфері інформаційної безпеки надає Україні цінні інструменти для створення ефективної системи захисту інформаційного простору. Використання цих практик допомагає зміцнити національну стійкість до інформаційних загроз, покращити координацію між державними органами та приватним сектором, а також підвищити рівень захисту критично важливих інформаційних систем в умовах глобальних викликів.

5. Розроблено рекомендації щодо вдосконалення державних механізмів інформаційної безпеки України, спираючись на міжнародний досвід та сучасні

інформаційні технології.

Функціонування механізму для протидії злочинам у сфері інформаційних технологій відбувається з урахуванням таких тенденцій: зростання потреби в ефективній міжнародній співпраці; посилення значущості правових основ міждержавної взаємодії та можливостей правоохоронних органів; зв'язок інформаційних злочинів з транснаціональною організованою злочинністю; необхідність узгодження положень щодо криміналізації, процесуальних повноважень правоохоронних структур, визначення юрисдикції та збору цифрових доказів; зростаюча актуальність оперативного реагування на запити про взаємну правову допомогу; активне впровадження практичних заходів для зменшення загроз, пов'язаних із безпекою дітей у сфері інформаційних технологій.

У сучасному інформаційному суспільстві, з огляду на зростання загроз, у тому числі інформаційних, поширення комп'ютерних злочинів та штучного інтелекту, використання інформаційних технологій у правоохоронній, економічній та регуляторній сферах стає необхідним, неминучим і надзвичайно перспективним напрямом для забезпечення безпеки особистості, суспільства й держави. У зв'язку з цим питання національної безпеки в умовах інформатизації набуває особливої актуальності. Зокрема, доцільним буде впровадження системи моніторингу інформаційного простору на основі сучасних технологій штучного інтелекту для оперативного виявлення загроз. Також рекомендовано створити єдиний національний центр координації дій у сфері кібербезпеки, спрямований на об'єднання зусиль державних органів та приватного сектору. Задля підвищення правової регламентації необхідно гармонізувати українське законодавство з європейськими стандартами у сфері кіберзахисту та інформаційної безпеки.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Конституція України від 28 червня 1996 року. *ВВРУ*. 1996. №30. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96%D0%B2%D1%80#Text (дата звернення: 21.11.2024).

2. Кримінальний кодекс України. *Відомості Верховної Ради України (ВВР)*, 2001, № 25-26, ст.131. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text (дата звернення: 21.11.2024).

3. Митний кодекс України. *Відомості Верховної Ради України (ВВР)*, 2012, № 44-45, № 46-47, № 48, ст.552 URL: https://zakon.rada.gov.ua/laws/show/4495-17#Text (дата звернення: 21.11.2024).

4. Закон України «Про національну безпеку України». URL: https://zakon.rada.gov.ua/go/2469-19 (дата звернення: 21.11.2024).

5. Закон України «Про захист інформації в інформаційно-комунікаційних системах». *Відомості Верховної Ради України (ВВР)*, 1994, № 31, ст.286 URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text (дата звернення: 21.11.2024).

6. Закон України «Про інформацію». *Відомості Верховної Ради України (ВВР)*, 1992, № 48, ст.650. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 21.11.2024).

7. Закон України «Про Електронні комунікації». URL: https://zakon.rada.gov.ua/laws/show/1089-20#Text (дата звернення: 21.11.2024).

8. Закон України «Про основні засади забезпечення кібербезпеки України». *Відомості Верховної Ради (ВВР)*, 2017, № 45, ст.403 URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 21.11.2024).

9. Закон України «Про захист персональних даних». *Відомості Верховної Ради України (ВВР)*, 2010, № 34, ст. 481. URL:

https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 21.11.2024).

10. Мінчеков А. Сутність поняття інформаційна безпека в сучасній науці публічного управління. *Наукові перспективи (Naukovì perspektivi)*, 2024, 4 (46). URL: http://perspectives.pp.ua/index.php/np/article/download/10972/11031 (дата звернення: 21.11.2024).

11. Черних Г. Соціологія інформаційного суспільства : навч. посібник. Київ, 2024. 162 с. URL: https://library.megu.edu.ua:9443/jspui/handle/123456789/4292 (дата звернення: 21.11.2024).

12. Калівошко, О., Хлистун, Д. Сутність та основи класифікації інформаційної інфраструктури. *Український економічний часопис*, 2024, (5), 65–74. URL: https://doi.org/10.32782/2786-8273/2024-5-12 (дата звернення: 21.11.2024).

13. Федоренко, Т В., Федоренко, в. В. Основні положення кіберпростору: поняття та сутність. *Сучасний науковий журнал*, 2023. 2(2), 68-72. URL: https://doi.org/10.36994/2786-9008-2023-2-9 (дата звернення: 21.11.2024).

14. Котляров В. Теоретичні засади сутності та концепції інформаційної безпеки. *Наукові перспективи (Naukovì perspektivi),* 2023, 6 (36). URL: https://doi.org/10.52058/2708-7530-2023-6(36)-131-142 (дата звернення: 21.11.2024).

15. Воробець, Н.Р. Теоретико-методологічні аспекти дослідження інформаційного суспільства в інформаційно безпековому вимірі theoretical and methodological aspects of the research of the information society in the information. *Регіональні студії*, 2023, 15. URL: http://regionalstudies.uzhnu.uz.ua/archive/33/2.pdf (дата звернення: 21.11.2024).

16. Кобко Є.В. Інформаційна війна та дезінформація: вплив на Національну безпеку України. *Правові новели*, 2023, 141. URL: http://legalnovels.in.ua/journal/20_2023/20_2023.pdf#page=141 (дата звернення: 21.11.2024).

17. Зейкан, В. В. Інформаційна безпека як елемент національної безпеки України. 2023. URL: https://er.dduvs.edu.ua/bitstream/123456789/11196/1/259.pdf

(дата звернення: 21.11.2024).

18. Радутний О.Е. Феномен великих даних та національна безпека України. *Національна безпека України в умовах інформатизації та глобалізації суспільних процесів: сучасні загрози та кримінально-правове регулювання* : матеріали VII Міжнар. наук.-практ. конф. (м. Харків, 11 трав. 2023 р.) / редкол.: Л. М. Демидова (голов. ред.), Н. В. Шульженко, Д. О. Куковинець, О. С. Попович ; Нац. юрид. ун-т ім. Ярослава Мудрого ; НДІ вивч. проблем злочинності ім. акад. В. В. Сташиса Нац. акад. прав. наук України ; Громад. орг. «Всеукр. асоц. кримін. права». Харків : Право, 2023. URL: https://ivpz.kh.ua/wpcontent/uploads/2023/07/%D0%95%D0%BB%D0%B5%D0%BA%D1%82%D1%80_%D0%B2%D0%B5%D1%80%D1%81%D1%96%D1%8F_%D0%9A%D0%BE%D0%BD%D1%84_%D0%9D%D0%B0%D1%86%D1%96%D0%BE%D0%BD%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0-%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0-%D0%A3%D0%BA%D1%80%D0%B0%D1%97%D0%BD%D0%B8.pdf#page=214 (дата звернення: 21.11.2024).

19. КУКЛЯК, Роман. Інформаційна безпека як складова національної безпеки України. *Наукові інновації та передові технології*, 2023, 4 (18). URL: http://perspectives.pp.ua/index.php/nauka/article/download/4271/4294 (дата звернення: 21.11.2024).

20. Венглінський, О.О. Інформація як об’єкт Національної безпекової політики України. *Редакційна колегія*, 2024, 42. URL: https://appjournal.in.ua/wpcontent/uploads/2024/06/APP_03_2024.pdf#page=42 (дата звернення: 21.11.2024).

21. Виздрик В., Мельник О. Інформаційна безпека в Україні: сучасний стан. *Grail of Science*, 2023, (24), 196–202. URL: https://doi.org/10.36074/grail-of-science.17.02.2023.034 (дата звернення: 21.11.2024).

22. Міненко Є. Організаційно-правовий аналіз забезпечення інформаційної безпеки як фактор суспільно-політичної стабільності. 2023. URL:

https://enpuir.npu.edu.ua/handle/123456789/43809 (дата звернення: 21.11.2024).

23. Домбровський, Л.В. Інформаційна безпека держави у системі національної безпеки України. 2024. URL: http://repositsc.nuczu.edu.ua/handle/123456789/20339 (дата звернення: 21.11.2024).

24. Руснак О. Стратегія національної безпеки в контексті публічного управління: інституційні рівні забезпечення та функціональна структура. *Věda a perspektivy*, 2024, 9 (40). URL: http://perspectives.pp.ua/index.php/vp/article/download/15031/15101 (дата звернення: 21.11.2024).

25. Дерюгін І.К., Батько І.І. Інформаційно-психологічні атаки як загроза державній безпеці. *Редакційна колегія*, 2023, 315. URL: https://appjournal.in.ua/wpcontent/uploads/2023/10/APP_05_2023.pdf#page=315 (дата звернення: 21.11.2024).

26. Йовенко К. Механізми протидії російській інформаційній агресії. *Політ. Сучасні проблеми науки*, 2024, 27. URL: https://nau.edu.ua/site/variables/docs/docsmenu/studnauka/polit2024/polit_2024_NNINO.pdf#page=27 (дата звернення: 21.11.2024).

27. Лопатченко І.С. Національна інформаційна безпека та штучний інтелект: світовий досвід та виклики для України. *Публічне управління XXI століття: Нові виклики і трансформації*, 461. URL: https://lib.lntu.edu.ua/sites/default/files/202408/%D0%97%D0%B1%D1%96%D1%80%D0%BD%D0%B8%D0%BA_%D0%9A%D0%BE%D0%BD%D0%B3%D1%80%D0%B5%D1%81_2024.pdf#page=462 (дата звернення: 21.11.2024).

28. Любиченко О. Взаємодія державних і недержавних суб'єктів забезпечення інформаційної безпеки: досвід країн люблінського трикутника. *Наукові інновації та передові технології*, 2024, 3 (31). URL: http://perspectives.pp.ua/index.php/nauka/article/download/9709/9762 (дата звернення: 21.11.2024).

29. Буряк, А.А. Пріоритети ОНН у напрямі удосконалення міжнародної інформаційної безпеки. 2024. PhD Thesis / Національний університет «Полтавська політехніка імені Юрія Кондратюка». URL: https://reposit.nupp.edu.ua/bitstream/PoltNTU/17032/1/9.pdf (дата звернення: 21.11.2024).

30. Ржевська Н. Сучасна інформаційна політика: досвід США для України. *політичні*, 2024, 68. URL: https://ipiend.gov.ua/wp-content/uploads/2024/06/4_Rzhevska.pdf (дата звернення: 21.11.2024).

31. Федотова О.О. Впровадження зарубіжного досвіду у процесі формування та реалізації державної інформаційної політики України. *Сучасні аспекти модернізації науки: стан, проблеми, тенденції розвитку*, 464. URL: http://perspectives.pp.ua/public/site/conferency/conf-45.pdf#page=465 (дата звернення: 21.11.2024).

32. Козир, М.А. Роль міжнародних організацій у системі забезпечення міжнародної інформаційної безпеки. 2024. URL: https://reposit.nupp.edu.ua/handle/PoltNTU/15131 (дата звернення: 21.11.2024).

33. Гринчишина В. Інформаційні технології в контексті міжнародних відносин: кібербезпека як один із викликів сучасної цифрової епохи. 2024. URL: https://ekmair.ukma.edu.ua/bitstreams/4705dd156aa14493b2062c2e94b7553d/download (дата звернення: 21.11.2024).

34. Ковалів С., Єсімов С. Механізм співробітництва держав щодо протидії злочинам у сфері інформаційних технологій. *Аналітично-порівняльне правознавство*, 2023, 1: 573-578. URL: http://journal-app.uzhnu.edu.ua/article/view/279385 (дата звернення: 21.11.2024).

35. Прокопенко О.С., Лашин, Я.О., Сівоха, І.М. Роль сучасних систем моніторингу у протидії інформаційним загрозам. 2023. URL: http://dspace.megu.edu.ua:8080/jspui/handle/123456789/4462 (дата звернення: 21.11.2024).

36. Даниленко Л., Марутян Р. Роль інноваційних технологій у політичній трансформації інформаційного простору країн вишеградської групи та України. *Наукові перспективи (Naukovì perspektivi),* 2024, 2 (44). URL: http://perspectives.pp.ua/index.php/np/article/download/9456/9509 (дата звернення: 21.11.2024).

37. Лавров В.В., Дудатьєв А.В. Інформаційна війна та її вплив на контент: методи оцінки ризиів та шляхи протидії. *In: The VII International Scientific and Practical Conference» Problematic questions of science and problems of development»*, October 30-November 01, 2023, Berlin, Germany. 350 p. p. 333. URL: https://euconf.com/wpcontent/uploads/2023/10/PROBLEMATICQUESTIONS-OF-SCIENCE-AND-PROBLEMS-OF-DEVELOPMENT.pdf#page=334 (дата звернення: 21.11.2024).

38. Ткачук Т.Ю. Правове забезпечення інформаційної безпеки в умовах Євроінтеграції України. Дисертація на здобуття наукового ступеня д.ю.н. / ДВНЗ «Ужгородський національний університет». Ужгород, 2019.

39. Золотар О.О. Правові основи інформаційної безпеки людини. Дисертація на здобуття наукового ступеня д.ю.н.. К., 2018.

40. Валюшко І.О. Інформаційна безпека України в контексті російсько-українського конфлікту. Кандидатська дисертація на здобуття наукового ступеня к.політ.н. К., 2018.

41. Зозуля О.С. Державне управління забезпеченням інформаційної безпеки України в умовах інформаційно-психологічного протиборства. Дисертація на здобуття наукового ступеня к.держ.упр. К., 2017.

42. Лісовська Ю.П. Адміністративно-правове забезпечення інформаційної безпеки в Україні. Автореферат дисертації на здобуття наукового ступеня к.ю.н. К., 2017.

43. Леоненко Н.А., Поступна О.В. Інформа-ційна безпека України: механізми, сучас-ні виклики та загрози в умовах інформа-ційного глобалізму.

Вісник Національного університету цивільного захисту України. Сер.: Державне управління. 2022. Вип. 2 (17). URL: http://repositsc.nuczu.edu.ua/handle/123456789/16883 (дата звернення: 21.11.2024).

44. Шемчук В.В. Забезпечення інформаційної безпеки як функція сучасних держав: по-рівняльно-правовий аналіз: монографія. Київ: Ліра-К, 2020. 352 с.16.

45. Ткачук Т.Ю. Забезпечення інформаційної безпеки в умовах євроінтеграції України: правовий вимір: монографія. Київ : Вид. дім «АртЕк», 2018. 411 с. РОЗДІЛ VII. Адміністративне право і процес; фінансове право; інформаційне право.

46. Нестерович В. Забезпечення інформаційної безпеки як функція держав в умовах сучасних викликів і загроз. *Fìlosofsʹkì ta metodologìčnì problemi prava*. 2020. No 1 (19). С. 136–137.

47. Гаврильців М. Т. Інформаційна безпека держави в системі національної безпеки України. *Юридичний науковий журнал*. 2020. No 2. С. 200–203.

48. «Україна – на вістрі гібридної атаки РФ у світі» – на міжнародній конференції в Академії СБУ обговорили досвід протидії інформаційним операціям РФ / Вебсайт Національної академії Служби безпеки України. 2021. 15 черв. URL: https://academy.ssu.gov.ua/ua/news-1-8-136-ukraina-–-na-vistri-gibridnoi-ataki-rf-u-sviti-–-na-mizhnarodniy-konferencii-v-akademii-sbu-obgovorili-d (дата звернення: 21.11.2024).

49. Харченко О. Центр протидії дезінформації - це побудова страткому, а не самоціль. URL: https://detector.media/infospace/article/185683/2021-03-lltsentr-protydii-dezmformatsii-tse-pobudova-stratkomu-a-ne-samotsil/ (дата звернення: 21.11.2024).

50. U. S. National Strategy for Public Diplomacy and Strategic Communication. URL: http://www.au.af.mil/au/awc/awcgate/state/natstrat_strat_comm.pdf (last accessed: 21.11.2024).