ФЕДЕРАЦІЯ ПРОФЕСІЙНИХ СПІЛОК УКРАЇНИ

АКАДЕМІЯ ПРАЦІ, СОЦІАЛЬНИХ ВІДНОСИН І ТУРИЗМУ

ПУБЛІЧНЕ УПРАВЛІННЯ: ПРАВОВІ, ОРГАНІЗАЦІЙНІ ТА СОЦІАЛЬНІ ПРОБЛЕМИ РОЗВИТКУ

Колективна монографія

Київ – 2025

УДК 351.07:35.08+342.9+316.4
П-88

Рекомендовано до друку Вченою радою Академії праці, соціальних відносин і туризму
(протокол № 7 від 25 лютого 2025 року)

Колектив авторів*: Н. Балашова (4.2), Н. Васильєва (3.1), В. Воротін (2.1; 4.1), О. Домбровська (4.3), А. Іванов (4.4), Я. Качан (Вступ; 2.2; 2.5), Д. Костенко (2.3), Д. Красівський (1.4; 2.5), І. Кульчій (4.5; 4.6), М. Лахижа (Вступ; 1.1; 2.2; 4.5), К. Міщенко (1.2; 2.4; 3.4), В. Писаренко (2.7;3.2; 3.3), Г. Старченко (2.6), В. Сухомлин (Вступ; 4.2), М. Шевченко (1.3).*

Рецензенти:
Кравченко Мілена В'ячеславівна, д-р наук держ. упр., проф., професор кафедри публічного управління, адміністрування та соціальної роботи, Національний університет охорони здоров'я України імені П. Л. Шупика (НУОЗ).

Приліпко Сергій Михайлович, д-р наук держ. упр., доц., професор кафедри публічного управління, менеджменту інноваційної діяльності та дорадництва, в. о. завідувача кафедри публічного управління, менеджменту інноваційної діяльності та дорадництва Національного університету біоресурсів і природокористування України.

Ганечко Олена Миколаївна, д-р юрид. наук, доц., викладач Національної школи суддів України, суддя шостого апеляційного адміністративного суду.

П-88 Публічне управління: правові, організаційні та соціальні проблеми розвитку / за наук. редакції д-ра наук держ. упр., проф. М. І. Лахижі; канд. наук держ. упр., доц. Я. В. Качан та канд. наук держ. упр., доц. В. Б. Сухомлина. Київ, 2025. 232 с.
ISBN 978-966-654-697-8

Колективна монографія видається в межах виконання кафедрою публічного управління та публічної служби загальноакадемічної теми «Ринок праці і розвиток профспілкового руху», затвердженої рішенням Вченої ради Академії праці, соціальних відносин і туризму (протокол № 4 від 09.12.2021).

У колективній монографії висвітлено юридичні, організаційні та соціальні аспекти розвитку системи публічного управління. Автори, спираючись на аналіз законодавчих актів, даних соціологічних опитувань, наукової літератури з України та інших країн, а також медійної інформації, розглядають історичні й теоретичні підвалини публічного управління. У праці викладено правові, організаційні та кадрові основи цієї системи, а також представлено механізми і засоби її функціонування. Окрему увагу приділено забезпеченню сталого розвитку та безпеки, а також ролі публічного управління у цих процесах.

Видання рекомендується науковим працівникам, викладачам та студентам закладів вищої освіти, практикам.

Складність, динамічність і перманентне оновлення публічного управління у сфері національної безпеки залежить як від складності і динамічності національної безпеки як явища та необхідності постійних змін у процесі публічного управління та адміністрування.

Розділ 4.6. Публічне управління забезпеченням інформаційної безпеки: досвід ЄС для України

Інна Кульчій

Із зростанням значення інформації в суспільному житті як ресурсу розвитку, з посиленням глобальних впливів на нації та держави актуальним стає проблема збереження та постійного оновлення їх національного інформаційного простору. Під час інформаційної агресії вона є об'єктом первинного ураження та суб'єктом організації захисту сторони, яка зазнала інформаційної агресії. Сучасний національний інформаційний простір як сфера інформаційного обміну має складатися з розгалуженої системи структур, що забезпечують створення нової інформації, зберігання та захист існуючої, а також організацію її використання через мережу засобів у країні та за кордоном для задоволення інформаційних інтересів і потреб громадян і зрештою – інформаційна безпека держави.

Проблема інформаційної безпеки Європейського Союзу розглядається поряд з іншими проблемами інформаційного суспільства. Слід зазначити, що аналіз низки нормативно-правових актів та планів дій у сфері формування інформаційного суспільства ЄС дозволив зробити висновок про значно вужче розуміння поняття «інформаційна безпека» стосовно як до України, так і до України.

Реформування сфери публічного управління забезпечення інформаційної безпеки не є виключенням і передбачає проведення ґрунтовної роботи щодо адаптації національної системи адміністрування забезпечення інформаційної безпеки у відповідності з кращими практиками держав Європейського Союзу. Відповідно, актуальним є науково-практичне завдання щодо узагальнення досвіду забезпечення інформаційної безпеки у розвинених державах світу і, зокрема деяких країн, що входять до Європейського Союзу та США.

Аналізуючи досвід країн ЄС із системи забезпечення інформаційної безпеки, варто зауважити, що пошук певного балансу між повним державним контролем і ринковими законами, тобто поєднанням влади та ринкових сил, є головною ознакою інформаційної політики не лише в Північній Європі, а й в інших країнах Європейського Союзу. У той же час ЄС продовжує приділяти пильну увагу сьогодні приватизації та лібералізації ринку інформаційно-комунікаційних технологій.

Система інформаційної безпеки Франції є складовою національної безпеки, відповідно її основні принципи закріплені в Білій книзі з оборони та національної безпеки. Процес глобалізації та боротьби з тероризмом привели до розробки нової концепції стратегії національної безпеки, яка безперешкодно

поєднує політику оборони, політику внутрішньої безпеки, зовнішню та економічну політику. Ця концепція була закріплена в третій Білій книзі з оборони та національної безпеки в 2008 році.

Цей підхід до формування стратегії національної безпеки Франції, який характеризується розширенням стратегічного мислення окрім оборони, був обумовлений глобалізацією, яка глибоко змінила основи міжнародної системи, ставши більш нестабільними та непередбачуваними, ніж у холодні часи. Війна та створювати нові загрози. різного характеру. З 2009 року це поняття включено до Кодексу оборони Франції.

Ще одна особливість білої книги з національної оборони та безпеки 2008 року полягає у тому, що вона визначає загрози для використання інформаційних систем та засобів масової інформації. Таким чином, характеризуючи загрозу масштабних атак на інформаційні системи, зазначається, що останні проникають через основні системотворчі ланки економічного та соціального життя.

Таким чином, «залежність від комунальних інформаційних систем, транспортної інфраструктури, продовольчої безпеки та навіть управління обороною робить сучасне суспільство та його безпеку вразливими для випадкових пошкоджень та цільових атак з боку комп'ютерних мереж. Загроза шпигунства та стратегічного впливу виправдовується широким використанням (м'якої сили) у міждержавних відносинах, маніпулюванням свідомістю через ЗМІ та Інтернет, досягненням наукового, економічного, оборонного потенціалу Франції та її території, небезпека культурної експансії» [6].

Четверта Біла книга була опублікована у 2013 році під головуванням Франсуа Олланда. П'ятий документ, під назвою «Стратегічний огляд оборони та національна безпека, був опублікований наприкінці 2017 року під головуванням Е. Макрона» [6]. Defense Review приділяє значну увагу «інформаційним загрозам та заходам протидії. Таким чином, зазначається, що в кіберпросторі деякі атаки через їх масштаби і серйозність можуть бути класифіковані як озброєна агресія. Труднощі з розподілом часток та поєднанням прямої дії з методами впливу та пропаганди дозволяють використовувати численні інструментальні сценарії для дестабілізації або підтримки більш простих операцій.

«Облік кіберзагроз та його еволюції тим паче складний, що «він може обмежуватися периметром захисту через заплутані питання та участі державних і приватних суб'єктів. У зв'язку з цим підкреслюється, що армії повинні повністю планувати та проводити операції у цифровому просторі до тактичного рівня в ланцюжку планування та проведення кінетичних операцій. Операції в цифровому просторі розширюють діапазон традиційних ефектів, доступних політичній владі, і використовують цифровість опонентів Франції, що зростає, як державних, так і недержавних. Ця здатність вимагає покращених та дуже гнучких людських ресурсів, а також постійної розробки конкретних технічних рішень» [15].

Крім того, для забезпечення безпеки інформації Defense Review допускає кібервійну, що означає оборонну або наступальну боротьбу у всьому цифровому середовищі проти урядових чи неурядових супротивників.

Стратегії національної безпеки, викладені у Білій книзі, становлять основу законів про військове планування. Сьогодні діє закон Франції «Про військове планування на 2019-2025 роки та інші оборонні положення» №2018-607 від 13.07.2018. Для Франції так званий «кіберджихадизм» залишається серйозною загрозою її інформаційному простору, який складається з використання інтернет-технологій та послуг, особливо соціальних мереж, для пропагування джихадистського насильства. Це робиться шляхом злому урядових веб-сайтів, корпоративних веб-сайтів або організацій, захисту інтересів та найму. Заходи протидії: блокування сайтів та облікових записів, створення сайтів контрпропаганди тощо.

Система інформаційної безпеки у Франції складається з таких спеціальних структур «Національного агентства з безпеки інформаційних систем (ANSSI)», «Аудіовізуальної служби (Audiovisual), Міжвідомчого управління інформаційних систем та комунікацій (DISIC)», «Управління розвитку ЗМІ)» та інші деякі.

Національне агентство безпеки інформаційних систем (ANSSI) – це «французька служба з національною компетенцією, створена указом у липні 2009 року під егідою Генерального секретаріату оборони та національної безпеки». ANSSI відповідає за просування національних технологій, систем та досвіду для просування цифрової економіки. При цьому основні зусилля фахівців ANSSI спрямовані на реалізацію заходів, передбачених у стратегії національної безпеки та оборони. «Основними завданнями агенції є підвищення ефективності управління та координації органів державної влади, критичної інфраструктури, суспільства з погляду комп'ютеризації; забезпечення промислової безпеки, організація захисту національної розвідувальної та телекомунікаційної інфраструктури в умовах військової загрози, у тому числі кібервійни; підтримка технічних засобів, необхідних для виконання завдань, поставлених перед Агентством у його нинішньому вигляді. У його повноваження входять» [14]:

- «формування державної політики у сфері захисту та безпеки інформаційних систем»;
- «розробка організаційних, правових та технічних заходів щодо захисту державних інформаційних систем та контроль за їх впровадженням»;
- «моніторинг, виявлення, повідомлення та реагування на кібератаки, спрямовані на державні інформаційні та телекомунікаційні системи»;
- виявлення та реагування на вірусні атаки, реалізація механізмів адаптивного захисту від них;
- «запобігання загрозам шляхом сприяння розробці надійного програмного та апаратного забезпечення»;
- «консультації та підтримка об'єктів критичної інфраструктури»;
- «систематичне інформування громадськості про загрози, зокрема через урядовий веб-портал з питань ІБ»;
- «розробка та придбання товарів, призначених для захисту найбільш уразливих ділянок міжвідомчої державної мережі»;

- «здійснення контролю та комунікацій з питань національної оборони та безпеки»;

- «сертифікація інтегрованих систем захисту інформації»**.**

Аудіовізуальна служба, яка діє під головуванням президента, також бере участь у реалізації інформаційної політики у Франції. Служба розробляє аудіовізуальні технічні платформи Президента Республіки, організує його виступи та забезпечує їх поширення по всій країні та за кордоном».

Крім того, Служба підтримує фотовідділ про діяльність президента та життя Єлисейського палацу, керує фотобанком та взаємодіє із засобами масової інформації та громадськістю. Важливою функцією цієї служби є аудіовізуальний моніторинг ЗМІ та формування адекватного архіву матеріалів. Загалом його діяльність спрямована на формування іміджу президента.

«У зв'язку з активною комп'ютеризацією органів державної влади у Генеральному секретаріаті уряду (SGG), що належить прем'єр-міністру, на початку 2011 року було створено Міжвідомче управління інформаційних систем та комунікацій (Постанова № 2022-193 від 21 лютого). 2011). (ДІСІК). Він відповідає за роботу інформаційних та телекомунікаційних систем для обміну інформацією між різними агенціями та з громадянами. Основними завданнями підрозділу є проектування державної інформаційної та телекомунікаційної інфраструктури з урахуванням потреб діяльності та оптимізації ресурсів, організація закупівель інформаційного обладнання, програмного забезпечення та послуг, розподіл електронних комп'ютерів між міністерствами, впровадження нових інформаційних систем» [6].

Метою створення DISIC є «відстеження тенденцій в інформаційних технологіях, оптимальне використання інформаційних ресурсів через загальні бази даних, запобігання ризикам інформаційної безпеки, пов'язаним з реалізацією великомасштабних проектів, покращення інформаційних систем обслуговування клієнтів» [6].

Основним законом у галузі інформаційної безпеки у Німеччині є Закон «Про посилення безпеки систем інформаційних технологій» (Information Security Law) від 25.07.2015. Закон відводить Федеральному управлінню інформаційних технологій (BSI) центральну роль захисту критично важливої інфраструктури у Німеччині.

Критичні інфраструктури – це установки, установки або їх частини, які «належать до секторів енергетики, інформаційних технологій та телекомунікацій, транспорту та дорожнього транспорту, охорони здоров'я, водопостачання, продовольства, фінансів та страхування. Такі об'єкти важливі для функціонування спільноти, оскільки їх закриття або погіршення стану спричинить значний брак матеріалів або створить загрозу громадській безпеці. 27 березня 2019 року Федеральне міністерство внутрішніх справ також опублікувало законопроект щодо безпеки інформаційних технологій, який містить цілісний підхід до безпеки у цій сфері.

Серед іншого, «передбачається запровадити простий у використанні ярлик комп'ютерної безпеки для комерційних продуктів, а також посилити компетенцію BSI та розширити список порушень кібербезпеки та пов'язаних із

ними слідчих дій. Законопроект також збільшує кількість отримувачів звітів та зобов'язань. Загалом очікується, що закон створить певні економічні труднощі для підприємств та органів державної влади» [15].

«Інформаційна безпека у Німеччині забезпечується Федеральними збройними силами Німеччини (Бундесвер), зокрема, Відділом комп'ютерних мереж та інформаційних операцій Командування стратегічної розвідки. Командування стратегічної розвідки також керує системою розпізнавання супутників SAR-Lupe, яка була запущена у грудні 2008 року» [3].

Завдяки п'яти супутникам SAR-Lupe, які вважаються одними з найпередовіших систем у своєму роді, може передаватися зображення з роздільною здатністю менше одного метра, незалежно від денного світла та погоди. Таким чином, можна прояснити практично будь-яку точку Землі. Система збирає та оцінює інформацію про військово-політичну ситуацію в окремих країнах та альянсах потенційного чи поточного супротивника та його збройних сил.

Отже, проаналізувавши досвід Країни ЄС щодо системи інформаційної безпеки варто відмітити, що на сьогодні немає універсального підходу чи єдиної моделі управління інформаційної безпекою. У кожного регіону світу та країни є свої внутрішні особливості, які надалі визначають специфіку цього процесу. Системи інформаційної безпеки у Франції та Німеччині засновані на усвідомленні ризиків та загроз, пов'язаних із швидким розвитком інформаційних та комунікаційних технологій. Наприклад, одним з основних гравців у системі інформаційної безпеки у Франції є Національне агентство безпеки інформаційних систем (ANSSI), а в Німеччині – Управління інформаційних та комп'ютерних мереж Бундесверу.

Аналізуючи напрямки вдосконалення забезпечення інформаційної безпеки та організації доступу до публічної інформації, варто зауважити, що Інформаційна безпека України, на жаль, стикається з значними загрозами, викликами, які створюють загрозу функціонуванню держави, її політичному та економічному розвитку, інтеграції в європейські та євроатлантичні структури.

Загрози інформаційній безпеці України в інформаційній сфері – це «сукупність умов і факторів, які загрожують життєво важливим інтересам держави, суспільства та особи через можливість негативного інформаційного впливу на свідомість і поведінку громадян, а також інформаційні ресурси. та інформаційна інфраструктура» [10, с. 90].

Доктрина інформаційної безпеки України визначає такі загрози інформаційній безпеці країни «поширення у глобальному інформаційному просторі спотвореної, небезпечної та необ'єктивної інформації, яка завдає шкоди національним інтересам України», «Зовнішня деструктивна інформація впливає на суспільну свідомість через ЗМІ, а також через Інтернет»; «Деструктивний інформаційний вплив, спрямований на підрив конституційного ладу, суверенітету, територіальної цілісності та недоторканності України»; «Прояви сепаратизму в ЗМІ, а також в Інтернеті на етнічному, мовному, релігійному та іншому ґрунті» [12].

За словами Р. Р. Марутяна, «найсерйознішою загрозою національній безпеці України в інформаційній сфері є реалізація іноземними державами негативного інформаційного та психологічного впливу на суспільну свідомість громадян України та світової спільноти за допомогою інформаційних кампаній та спеціальних розвідувальних операцій. Це пов'язано з систематичним поширенням необ'єктивної, неповної або необ'єктивної інформації про Україну та політичні процеси, що відбуваються на її території. Все це впливає на зовнішню та внутрішню політику нашої держави, знижує її міжнародний імідж, має політичну та економічну основу. Метою цих інформаційних операцій є забезпечення національних інтересів інших держав» [9, с. 163].

Загрози інформаційної безпеки України у сфері інформації також мають включати «прояви обмежень свободи слова та доступу до інформації для громадян», «Спотворення, спотворення, блокування, неявно упереджене та необ'єктивне висвітлення інформації», «Несанкціоноване поширення, відкрита дезінформація», «Поширення інформації іншими державами та деструктивне інформаційне вторгнення до національного інформаційного простору, коли країни з сильнішим інформаційним потенціалом мають можливість через ЗМІ розширювати свій вплив на населення та громадськість менш могутньої держави», «Виникнення та функціонування у національному інформаційному просторі стану неконтрольованих та інформаційних потоків тощо» [2].

Проти України широко використовуються сучасні технології негативного інформаційно-психологічного впливу, які стають загрозою для українського національного інформаційного простору та державного суверенітету. Забезпечення інформаційної безпеки України перед дестабілізуючим негативним інформаційним та психологічним впливом та агресивною інформаційною політикою рф вимагає активізації зусиль на всіх рівнях влади та громадянського суспільства.

«Для протидії широко поширеним негативним інформаційним та психологічним впливам, операціям та війнам необхідно визначити пріоритетні напрямки державної інформаційної політики та важливі кроки з боку української влади» [5]:

1) «Інтеграція України в європейський глобальний та регіональний інформаційний простір»;

2) «інтеграція в міжнародні інформаційно-розвідувальні та телекомунікаційні системи та організації»;

3) «створення власної національної моделі інформаційного простору та забезпечення розвитку інформаційного суспільства»;

4) «модернізація всієї державної системи захисту інформації, формування та реалізація ефективної інформаційної політики»;

5) «вдосконалення законодавства у сфері інформаційної безпеки, приведення національного законодавства у відповідність до міжнародних стандартів та ефективне регулювання інформаційних процесів»;

6) «розвиток національної інформаційної інфраструктури»;

7) «підвищення конкурентоспроможності внутрішніх інформаційних товарів та послуг тощо».

З метою запобігання розповсюдженню інформації державна діяльність в інформаційному просторі має здійснюватися за такими напрямками:

1) «реалізація превентивних стратегій та тактик (превентивних заходів)»;

2) «реалізація стратегії реагування (швидке реагування на атаки розвідки супротивника та активний наступ)»;

3) «захист національного інформаційного простору. Основна мета – забезпечити домінування та перевагу ЗМІ в інформаційному просторі».

Слід зазначити, що для захисту національного інформаційного простору, для створення ефективної системи захисту інформації українська влада вживає певних заходів. Зокрема, 14 січня 2015 року Кабінет Міністрів України ухвалив Постанову про створення Міністерства інформаційної політики України, пріоритетними завданнями якої є протидія інформаційної агресії з боку Російської Федерації; розробка ефективної державної стратегії інформаційної політики та Концепції інформаційної безпеки України; злагодженість та узгодженість функціонування та діяльності органів державної влади та інформаційної сфери» [15].

З метою протидії негативним наслідкам інформаційної пропаганди та інформаційних воєн, нейтралізації та запобігання реальним та потенційним загрозам в інформаційному просторі України Рада національної безпеки та оборони України ухвалила рішення «Про заходи щодо вдосконалення навчання та реалізації державна політика інформаційної безпеки України».

У документі йдеться, що Рада національної безпеки та оборони, враховуючи необхідність удосконалення нормативно-правової бази та запобігання та нейтралізації потенційних та реальних загроз національній безпеці в інформаційній сфері, ухвалила іноземні держави, які передбачають, зокрема, визначення механізму протидії негативному інформаційному та психологічному впливу, зокрема заборона на ретрансляцію телеканалів, посилення контролю за дотриманням законодавства про інформаційну безпеку, психологічну та кібербезпеку, вжити заходів щодо того, щоб об’єктивна інформація про соціально-політичну ситуацію в Україні поширювалася по всьому світу» [1].

«Необхідність створення національної системи інформаційної безпеки очевидна, коли нею займатимуться відповідні підрозділи СБУ, кіберзахисту - відповідні підрозділи Державної служби спеціального зв’язку та захисту інформації та боротьби з кіберзлочинністю - відповідні підрозділи. Міністерства внутрішніх справ. Ефективну координацію та взаємодію забезпечуватиме відповідний підрозділ Ради національної безпеки та оборони» [2].

Національна система інформаційної безпеки створюється та розвивається відповідно до Конституції України та інших правових норм, що регулюють суспільні відносини у сфері національної безпеки, зокрема: Закон України «Про основи національної безпеки України», Концепція безпеки. та Національний координаційний центр розвитку оборонного сектору з кібербезпеки, Стратегії національної безпеки України, Стратегії кібербезпеки України, Військової доктрини України, Доктрини інформаційної безпеки України та ін.

Кібервійна породжує нові кіберзагрози. Кіберзагрози – це «існуючі та потенційно потенційні явища та фактори, які ставлять під загрозу життєво

важливі інтереси людини та громадянина, суспільства та держави, реалізація яких залежить від належного функціонування інформаційних, телекомунікаційних та інформаційних та телекомунікаційних систем [8].

Створення національної системи інформаційної безпеки забезпечується Стратегією кібербезпеки для безпечної експлуатації кіберпростору, його використання на користь особистості, суспільства та держави.

Організаційне забезпечення системи захисту інформації також можна розглядати як умисну діяльність суб'єкта захисту інформації, пов'язану з:

- «створення та оптимізація (розвиток) організаційних структур, що найбільш підходять для забезпечення кібербезпеки»;
- «оптимізація (коригування) процесу управління у сфері безпеки у кіберпросторі, забезпечення найкращих умов прийняття та реалізації відповідних управлінських рішень».

Національна система інформаційної безпеки має насамперед «забезпечувати взаємодію в галузі інформаційної безпеки державних органів, органів місцевого самоврядування, військових формувань, правоохоронних органів, наукових установ, навчальних закладів, громадських об'єднань, підприємств, установ та організацій, незалежно від форми власності, що здійснюють діяльність у галузі електронних комунікацій, інформаційної безпеки та/або є власниками (адміністраторами) критичної інформаційної інфраструктури. Основою національної системи захисту інформації є Міністерство оборони України, Державна служба спеціального зв'язку та захисту інформації України, Служба безпеки України, Національна поліція України, Національний банк України [13].

Аналізуючи системи захисту інформації провідних країн світу, ми приходимо до висновку, що на сьогоднішній день не існує єдиної моделі побудови національної системи захисту інформації.

Стратегія кібербезпеки Канади «визначає кібертероризм і кіберворожі дії в інших країнах (кібершпигунство та кібервійни) як основні загрози кібербезпеці країни та ключовий орган, відповідальний за координацію та моніторинг реалізації цієї стратегії. І координацію кібербезпеки і протидія кібербезпеки» [4].

Австрійська стратегія кібербезпеки Центр кіберзлочинності Федерального міністерства внутрішніх справ Австрії був призначений національним координатором та центральним органом у галузі інформаційної безпеки. Крім того, на нього покладено основні функції правоохоронних органів у галузі інформаційної безпеки та боротьби з кіберзлочинністю.

«Агентство внутрішньої безпеки відіграє ключову роль у забезпеченні інформаційної безпеки Польщі (AVB) – «польський орган контррозвідки. Так, у 2013 році AVB розробила Польську стратегію інформаційної безпеки та ініціювала створення Центру криптології при Міністерстві національної оборони Польщі, завданням якого є захист інформації, кіберзахист та наступальні кібероперації (активний кіберзахист)». «Аналіз нормативно-правових та організаційних засад системи інформаційної безпеки у провідних країнах світу свідчить про домінуючу роль спецслужб у забезпеченні кібербезпеки держави у зв'язку з характером сучасних кіберзагроз. органи контррозвідки держави» [13].

«У світлі міжнародного досвіду та для того, щоб ефективно вирішувати питання державної кібербезпеки, агентство, яке координує діяльність усіх суб'єктів у галузі кібербезпеки (Національна система інформаційної безпеки), рекомендується призначити Службу безпеки України, яка є спеціально уповноваженим органом у галузі контррозвідки, а також протидії внутрішнім та зовнішнім загрозам, у тому числі в інформаційній сфері (кібернетика). Також з урахуванням світової практики пропонувалося створити Національний центр кібербезпеки, який мав бути підпорядкований Службі безпеки України» [7, с. 77].

Особливу увагу приділено «Національній системі інформаційної безпеки України» від Української служби реагування на надзвичайні ситуації – спеціалізованого підрозділу Державного центру захисту інформації та телекомунікаційних систем Державної служби спеціального зв'язку та захисту інформації України, створеного у 2007 році. UA полягає у забезпеченні захисту державних інформаційних ресурсів та інформаційно-телекомунікаційних систем від несанкціонованого доступу, неправомірного використання та порушення їх конфіденційності, цілісності та доступності. Діяльність CERT-AU передбачена Законом України «Про державну службу спеціального зв'язку та захисту інформації» та Положенням.

Україна має створити ключові механізми публічного управління інформаційною безпекою перед кіберзагрозою у вигляді спеціалізованих центрів, інститутів та експериментів з операціями інформаційної війни, фінансувати спеціалізовані дослідження в галузі розвідувальних операцій та створювати структури для досліджень та розробок.

На порядку денному – завдання «поступового становлення індустрії програмного забезпечення», «прискорити роботи зі створення Української національної мережі супер комп'ютерних комплексів, поєднаних із високошвидкісними оптоволоконними каналами передачі даних», «формувати чітку інформаційну політику щодо просування місцевих ІТ-компаній за кордоном, об'єднати інтереси освіти, науки та ІТ-бізнесу», «визначення базових вузів, на основі яких формуються кластери для вирішення питання підготовки ІТ-кадрів» [8].

З метою забезпечення інформаційної безпеки необхідно створити національну систему інформаційної безпеки як формат співпраці державних органів, установ, організацій, приватного сектору, науково-дослідних установ та організацій, професійних асоціацій та неурядових організацій у сфері інформаційної безпеки.

Вбачається доцільним вирішення таких актуальних питань:

Розробити засадничий документ із регулювання інформаційного простору – Концепцію інформаційної політики України, в «якій передбачити засади, методи та засоби формування та провадження державної інформаційної політики» (зокрема щодо реалізації системи державної пропаганди, спрямованої як на внутрішнє, так і на зовнішнє інформаційне середовище; забезпечення достатнього рівня присутності якісного національного інформаційного продукту в українському та міжнародному інформаційному просторі тощо).

Оптимізувати публічне управління інформаційною сферою у спосіб: – «утворення Національної ради України з питань комунікацій – конвергентного

незалежного органу з регуляторними й наглядовими повноваженнями в інформаційній сфері (на базі Національної ради та НКРЗІ), до компетенції якої віднести регулювання діяльності у сфері телекомунікацій, користування радіочастотним ресурсом, телерадіомовлення, а також іншої діяльності, пов'язаної з використанням телекомунікаційної інфраструктури, зокрема в мережі Інтернет тощо»; «утворення Міністерства з комунікацій, інформації та інформатизації України – центрального органу виконавчої влади з провадження комплексної загальнодержавної інформаційної політики та політики в інформаційній сфері, передбачивши серед його повноважень, зокрема, формулювання та трансляції в українському суспільстві й назовні державних інформаційних пріоритетів, найважливіших повідомлень з базових аспектів життя держави, а також координацію діяльності органів виконавчої влади щодо виконання загальнодержавних програм і проектів інформатизації тощо».

Унормувати діяльність в інформаційній сфері відповідно до міжнародних правових норм і сучасних викликів, зокрема у спосіб: «доопрацювання розробленого Міністерством юстиції України Проекту закону «Про внесення змін до деяких законів України щодо забезпечення прозорості відносин власності щодо засобів масової інформації», спрямованого на недопущення монополізації медіа (в тому числі Інтернет-ЗМІ) та їх використання у маніпулятивних цілях»; «розроблення обов'язкового для виконання Кодексу етичної поведінки журналістів, найважливішим у якому має бути розділ «Відповідальність», що міститиме вказівку: хто, за що і як відповідає, порушуючи ту чи іншу етичну норму»; визначення у нормативно-правовому полі України таких понять, як «державна інформаційна політика», «інформаційно-психологічна безпека», «інформаційно-психологічні впливи» тощо.

Отже, проаналізувавши напрямки вдосконалення забезпечення інформаційної безпеки та організації доступу до публічної інформації, варто зауважити, що деякі країни почали просувати проекти стратегій інформаційної безпеки, і Україна не є винятком. Система національної безпеки є багатокомпонентною, національна система інформаційної безпеки є її особливою підсистемою, метою якої є забезпечення функціонування та розвитку цієї системи. Забезпечення належного рівня інформаційної безпеки є необхідною умовою розвитку інформаційного суспільства. У дещо спрощеному вигляді під національною системою інформаційної безпеки пропонується розуміти сукупність специфічних для певної нації чи держави суб'єктів інформаційної безпеки, які взаємодіють з метою забезпечення незахищеності особи, суспільства та країни в цілому. Очевидною є потреба у створенні Національної системи інформаційної безпеки, коли цим займатимуться відповідні підрозділи Служби безпеки України, відповідні підрозділи Державної служби безпеки та Міністерства внутрішніх справ. Координацію та ефективну взаємодію забезпечуватиме відповідний підрозділ РНБО. Одним із ключових питань організації ефективного функціонування національних систем інформаційної безпеки є налагодження взаємодії між компетентними державними органами, які є суб'єктами інформаційної безпеки, та координація такої діяльності.