

С. Г. Головко,

кандидат історичних наук, доцент

ORCID ID: <https://orcid.org/0000-0003-0795-7166>

Н. М. Головко,

здобувачка вищої освіти першого (бакалаврського) рівня

ORCID ID: <https://orcid.org/0009-0004-2033-9893>

ДЕРЖАВНА ІНФОРМАЦІЙНА ПОЛІТИКА ЯК ІНСТРУМЕНТ ПРОТИДІЇ ГЛОБАЛЬНИМ ВИКЛИКАМ І ЗАГРОЗАМ: МІЖНАРОДНИЙ ДОСВІД ТА ЙОГО ВИКОРИСТАННЯ В УКРАЇНІ

Державний університет «Київський авіаційний інститут»
проспект Любомира Гузара, 1, 03058, Київ, Україна
Київський національний університет імені Тараса Шевченка
вул. Юрія Іллєнка, 36/1, 04119, Київ, Україна
E-mails: golovkos@ukr.net, natalijaholovko123@ukr.net

Мета: актуалізація пріоритетних завдань розбудови державної інформаційної політики України в контексті сучасних викликів і загроз та міжнародного досвіду їх подолання на прикладі США як провідного учасника глобального інформаційного простору. **Методи:** за результатами порівняльно-правового аналізу окреслено пріоритетні завдання, ключові виклики та загрози інформаційної сфери України, механізми та особливості реалізації державної інформаційної політики США; документальний метод застосовано для аналізу законодавчо-нормативного забезпечення реалізації державної інформаційної політики; прогностичний метод використано для визначення перспектив удосконалення державної інформаційної політики України з урахуванням міжнародного досвіду. **Результати:** актуалізовано проблему розбудови державної інформаційної політики України, визначено основні виклики та загрози для інформаційної сфери в умовах воєнного часу; обґрунтовано необхідність удосконалення державної інформаційної політики у контексті інтеграції до європейського та світового інформаційного простору з використанням міжнародного досвіду; проаналізовано механізми та засоби реалізації державної інформаційної політики США в аспекті її стратегічних концептів, законодавчої підтримки, посилення впливу на міжнародний інформаційний простір, реалізації системи заходів з кібербезпеки та регулювання інновацій у галузі розвитку нейромереж та технологій штучного інтелекту. **Обговорення:** співвідношення інтересів держави в галузі інформаційної безпеки як складника національної безпеки та забезпечення дотримання прав і свобод людини як найвищої цінності громадянського суспільства.

Ключові слова: державна інформаційна політика України; інформаційна безпека; досвід США щодо регулювання національного та глобального інформаційного простору.

Постановка проблеми та її актуальність. Державна інформаційна політика є важливим складником інституціонального забезпечення функціонування громадянського суспільства. Забезпечення рівного доступу до достовірної та об'єктивної інформації, ефективний захист від

негативних інформаційних впливів є одним із важливих напрямів реалізації конституційних прав і свобод людини, що гарантуються державою. На тлі глобальної цифровізації усіх галузей суспільного життя інформаційна політика виступає ключовим засобом підтримки не лише

інформаційної, а й національної безпеки держави загалом, оскільки спрямована на запобігання загрозам і подолання викликів в реаліях, коли кардинально змінюються усталені, традиційні підходи щодо джерел, методів і способів отримання та зберігання, опрацювання, аналізу, інтерпретації інформації у часі та просторі, її ролі в житті суспільства та конкретного громадянина.

В умовах воєнного часу для України актуальним завданням є поєднання засобів протидії викликам і загрозам в інформаційному просторі, зумовлених, перш за все, загарбницькою війною, а також інструментів забезпечення прав і свобод в інформаційній сфері для людини як найвищої цінності громадянського суспільства. Встановлення оптимального балансу між інтересами держави у сфері інформаційної безпеки та правами громадян як суб'єктів глобальних міжнародних інформаційних процесів вимагає пошуку нових підходів та стратегій, а також вироблення механізмів їх реалізації з урахуванням тенденцій розбудови міжнародного інформаційного простору.

Аналіз досліджень і публікацій з проблеми. Теоретико-методологічну та джерельну базу окресленої проблеми становлять праці дослідників, присвячені удосконаленню державної інформаційної політики в Україні з використанням міжнародного досвіду [10], підвищенню її ефективності в контексті європейської інтеграції [3], подоланню сучасних загроз і викликів в інформаційній безпеці країн з розвинутою демократією [11], питанням державного регулювання забезпечення інформаційної безпеки зарубіжжя [12], застосуванню технологій штучного інтелекту для забезпечення інформаційної безпеки [5] та тенденцій розвитку цього процесу [4], особливостям реалізації внутрішньої та зовнішньої інформаційної політики як ключової умови підтримки інформаційного суверенітету держави [6].

Метою статті є актуалізація пріоритетних завдань розбудови державної інформаційної політики України в контекстах сучасних викликів і загроз та міжнародного досвіду їх подолання на прикладі Сполучених Штатів

Америки як одного з провідних учасників глобального інформаційного простору.

Виклад основного матеріалу дослідження. Зasadничі принципи державної інформаційної політики окреслені Законом України «Про інформацію». Її основними напрямками визначено забезпечення рівних можливостей щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації та забезпеченню доступу до неї; створення умов для формування в Україні інформаційного суспільства; оновлення та зберігання національних інформаційних ресурсів; забезпечення інформаційної безпеки України та входження до світового інформаційного простору тощо [7]. Одним із пріоритетів державної інформаційної політики України виділяють інтеграцію до єдиного європейського та міжнародного інформаційного простору, модернізацію системи нормативно-правового регулювання національного медіапростору, розвиток внутрішньодержавних та міжнародних комунікацій, розбудова культурно-освітнього складника соціального та медіапростору, приділення належної уваги дослідженню проблеми використання штучного інтелекту та досягнень нейронауки [1]. Євроінтеграційний поступ України потребує розроблення механізмів, які передбачають функціонування інформаційного простору за стандартами Європейського Союзу, модернізації законодавчо-нормативної бази, що регулює реалізацію цифрових технологій у міжнародному інформаційному просторі, формування позитивного іміджу країни як умови міжнародної співпраці та залучення інвестицій, удосконалення системи інформування громадян тощо [3].

Пріоритети державної інформаційної політики трансформуються в умовах непрогнозованих викликів. Її особливістю під час війни є спрямування зусиль усіх інститутів громадянського суспільства на регулювання інформаційної сфери в пріоритетах захисту прав громадян та гарантій інформаційної безпеки держави і окремої особистості. Разом із тим, встановлюються певні обмеження на поширення інформації з метою запобігання можливих загроз національній безпеці [10]. Сьогодні державна інформаційна

політика України спрямована на запобігання та подолання сучасних загроз і викликів глобального та національного рівнів. До загроз Стратегією інформаційної безпеки віднесено глобальні дезінформаційні кампанії, впливи на інформаційний простір та соціальні мережі, невідповідність рівня глобальної медіаграмотності та стрімкого розвитку цифрових технологій. Натомість не менш актуальними є й національні виклики, які, перш за все, пов'язані з інформаційним впливом держави-агресорки, обмеженістю ресурсів і можливостей щодо ефективної протидії дезінформаційним кампаніям, недостатньою сформованістю в Україні системи стратегічних комунікацій, недосконалістю організаційно-правового регулювання відносин у сфері інформаційної діяльності та захисту прав її суб'єктів, обмеженістю доступу до інформації на місцевому рівні, недостатнім рівнем інформаційної культури та медіаграмотності в суспільстві як умова протидії маніпулятивним впливам [9]. Одним із пріоритетних завдань держави є забезпечення інформаційного суверенітету України, що є важливим складником державного суверенітету, інструментом національної безпеки та виявляється в здатності держави регулювати зовнішні інформаційні потоки відповідно до національного законодавства [6]. Зауважимо, що Доктрина інформаційної безпеки України передбачає спрямування регулятивних заходів в інформаційній сфері на гарантування національної безпеки та дотримання прав і свобод громадян [2]. Цей принцип є одним із визначальних для функціонування інформаційної сфери. Одним із прикладів його ефективної реалізації є ставлення до проблеми інформаційної безпеки в США як умови гарантування безпеки, прав і свобод американських громадян. Хоча нормативно-правова база підтримки інформаційної безпеки США є різноаспектною та структурується за федеральним рівнем та окремих штатів, що зумовлює суттєві відмінності в законодавчих актах, вона достатньо уніфікована. Це робить її застосування гнучким та достатньо ефективним [12]. Хоча у США формально відсутня цілісна стратегія щодо державної інформаційної політики, її основоположними принципами є

свобода слова та розмежування урядових повноважень. Перша поправка до Конституції, прийнята 1791 року, утверджує принцип свободи слова та преси й обмежує повноваження федерального уряду щодо їх обмеження. Одним із ключових законодавчих актів, що забезпечують реалізацію права громадян на безперешкодний доступ до інформації, є Закон про свободу інформації 1966 (Freedom of Information Act), який передбачає можливість для кожного американця звертатися до федеральних агентств із запитом щодо інформації, якщо вона не містить даних, які загрожують національній безпеці або порушують конфіденційність приватних осіб. Важливу роль відіграв Закон про відкритість уряду 1974 (Sunshine in Government Act), який визначив принцип прозорого функціонування ключовим у діяльності державних установ. Розбудові інформаційної сфери, адекватної запитам громадянського суспільства, сприяв і Закон про авторське право (United States Copyright Act). Відповідно до нього, всі твори, створені на замовлення держави, стають суспільним надбанням. Це стимулювало розвиток не лише наукових досліджень, а й бізнесу, коли приватні компанії отримали безкоштовний доступ до корисної інформації. Основні принципи управління урядовою інформацією визначає Документ Офісу управління та бюджету Circular A-130 (Office of Management and Budget). Він наголошує, що обов'язком держави є забезпечення громадянам вільного доступу до інформації, усунення бюрократичних бар'єрів. Важливу роль у реалізації державної інформаційної політики США відіграють спеціальні органи. Контроль за дотриманням Закону про свободу інформації покладений на Управління інформаційної політики (Office of Information Policy) Міністерства юстиції США. Офіс управління та бюджету США здійснює координацію інформаційної політики та визначає її основні напрями. Національний архів і адміністрація документації (National Archives and Records Administration) зберігає офіційні документи уряду та гарантує їхню доступність для всіх громадян. Федеральна комісія зі зв'язку (Federal Communications Commission) здійснює супровід норм, пов'язаних зі свободою слова, діяльністю

засобів масової інформації та інтернет-ресурсів. Важливі функції покладено на державні агентства зі збору та поширення науково-технічних даних. Національний науковий фонд (National Science Foundation) фінансує дослідження та контролює впровадження їх результатів у практику. Бібліотека Конгресу США (Library of Congress) як найбільший державний архів знань відкриває доступ до історичних документів та урядових матеріалів. Американські медіа мають значну самостійність та незалежні від держави завдяки Першій поправці до Конституції США, хоча й можуть отримувати певну підтримку на федеральному рівні або рівні штату. Також функціонує громадське некомерційне мовлення, яке підтримується глядачами та донорами. При цьому права засобів масової інформації регулюються Законом про телекомунікації 1966 року. Контроль за функціонуванням радіо-, телевізійного, дрогового, супутникового та кабельного зв'язку здійснює Федеральна комісія зі зв'язку. США мають широку мережу засобів масової інформації для іноземної аудиторії, діяльність яких координує Агентство з глобальних медіа. Воно регулює інформаційну сферу за межами США та реалізує програми для глобальної аудиторії (Голос Америки, Офіс кубинського мовлення, Радіо Вільна Європа/Радіо Свобода, Радіо Вільна Азія, Фонд відкритих технологій тощо). Це дає можливість реалізувати інформаційну політику та здійснювати інформаційні впливи в глобальному масштабі.

Міжнародна інформаційна політики США є важливим складником Стратегії національної оборони 2022 (National Security Strategy) [15]. Згідно з нею, найбільшою загрозою національній безпеці є політика Китаю в інформаційній, цифровій, космічній сферах як представника авторитарних геополітичних об'єднань. З огляду на це, пріоритетним завданням державної інформаційної політики визначено підтримка інформаційної незалежності, кібербезпека та зміцнення зовнішнього інформаційного простору. Тому серед найбільш важливих механізмів гарантування державою інформаційної безпеки США відзначають дієву систему реагування на процеси в інформаційному просторі та протидії

загрозам у сфері інформаційної безпеки, розвинуту систему підготовки фахівців із кібербезпеки, ефективний захист управлінських інформаційних систем, активну міжнародну співпрацю задля підтримки інформаційної безпеки, формування відповідального ставлення громадян до інформаційної безпеки держави [10]. Натомість до ключових проблем у галузі сучасної державної інформаційної політики США дослідники відносять зростання кількості шкідливого програмного забезпечення та його поширення, а також отримання особистих конфіденційних даних користувачів шляхом несанкціонованого доступу до їх акаунтів.

Актуальним для США є також розроблення ефективних механізмів інформаційної протидії урядовим та іншим організаціям країн, що мають відповідні технологічні ресурси і діють поза межами міжнародного правового поля [11]. Ключові виклики та напрями подолання загроз інформаційній сфері США відображено в Національній стратегії кібербезпеки 2023 [14], яка продовжила реалізацію системи заходів, визначених Комплексною національною ініціативою з кібербезпеки 2008 [16]. Зокрема, запроваджується програма багаторівневої перевірки доступу до інформаційних систем та вдосконалених методів шифрування інформації для її захисту «Zero Trust Architecture» [17]. Одним із контекстів проблеми інформаційної безпеки та державної інформаційної політики, що актуалізується в США та країнах Європейського Союзу, є потенційна можливість використання інформаційних систем зі штучним інтелектом для ухвалення стратегічних управлінських рішень національного та міжнародного рівнів, часткової або повної заміни в цих процесах представників публічної влади, а також дослідження ризиків, що їх супроводжують. З огляду на це, одним із ключових принципів застосування систем ШІ є прозорість цього процесу на всіх його етапах: від проектування відповідних алгоритмів до їх використання та оцінки впливів. Саме зважаючи на глобальні ризики, національна стратегія використання технологій ШІ в усіх сферах суспільного життя США формується на федеральному рівні, хоча регіональні нормативно-правові акти, що регу-

люють окремі її аспекти, достатньо широко представлені [5]. У січні 2025 року Президент США підписав новий виконавчий указ «Усунення бар'єрів для лідерства Америки в галузі штучного інтелекту», що вносить значні зміни в стратегію розвитку технологій штучного інтелекту. Нові підходи спрямовані на скасування попередніх обмежень для розвитку та використання інновацій ШІ, декларуючи принцип «неупередженого та вільного розвитку систем ШІ». Одночасно було оголошено про старт компанії Stargate, яка об'єднає провідних технологічних гігантів OpenAI, SoftBank та Oracle для розвитку інфраструктури штучного інтелекту та передбачає початкову інвестицію в обсязі \$100 млрд зі збільшенням вкладень до \$500 млрд [13]. Можемо зауважити, що ці кроки підтверджують спрямування державної інформаційної політики США на посилення позицій у галузі створенні та розвитку неймереж. Зосередження на технологічному лідерстві та зменшенні регулятивних функцій держави щодо використання технологій штучного інтелекту можуть мати серйозні наслідки. Тому важливою тенденцією інформаційної політики США та інших держав у недалекій перспективі є зміщення акцентів із пріоритету захисту персональних даних користувачів та їх безпечного використання на ефективну протидію неконтрольованого використання технологій ШІ та їх впливу на порушення прав і свобод громадян.

Занепокоєння щодо юридичної й технічної беззастережності використання нових інструментів інформаційної політики (зокрема, інтернету), що може посилити загрозу для державних таємниць, особистої конфіденційної інформації громадян, а з іншого, збільшити залежність національного інформаційного простору України від зарубіжної продукції, чужої інформаційної політики, наголошувалося ще в рекомендаціях парламентських слухань 1997 року [8]. Це актуалізує проблему розроблення та запровадження адміністративно-правових механізмів регулювання застосування штучного інтелекту, забезпечення контролю та відповідальності за результати такої діяльності як складника інформаційної безпеки сучасного громадянського суспільства [4].

Висновки. В умовах глобальних викликів та загроз, зумовлених війною, державна інформаційна політика є важливим складником національної безпеки України, забезпечуючи реалізацію прав і свобод людини в інформаційній сфері як невід'ємний складник сучасного громадянського суспільства. Аналізуючи міжнародний досвід, насамперед США як лідера інновацій у підтримці незалежності та протидії сучасним загрозам національного та глобального інформаційного простору, можемо окреслити основні аспекти його використання як чинника розбудови інформаційної сфери України. Зауважимо, що одним із ключових чинників, що визначають особливості інформаційної політики США, можна виділити концепт свободи слова. З одного боку, його акцентуація є ознакою громадянського суспільства та гарантує прозорість державної інформаційної політики, діяльність урядових інституцій та масмедіа, а з іншого, ускладнює оперативну протидію інформаційним загрозам, зокрема поширенню дезінформації.

Інформаційна політика в США є важливим складником внутрішньої та зовнішньої політики країни, потужним інструментом забезпечення впливу на світовій арені та збереження статусу наддержави. Попри значні геополітичні, географічні, соціально-економічні відмінності України та США, доцільним є врахування американського досвіду формування та реалізації державної інформаційної політики, зокрема й в умовах воєнного часу. Актуальним завданням для вітчизняних реалій є забезпечення балансу між контролем інформаційного простору з боку держави та свободою слова. Попри те, що Конституція та Закони України проголошують свободу слова, на практиці спостерігається значний вплив держави на висвітлення інформаційних процесів, що стосуються політичного життя країни, зокрема виборчого процесу, окремих політичних постатей тощо, тоді як протидія поширенню дезінформації та наративів держави-агресора потребує системного підходу, розроблення ефективних механізмів та нормативно-правового забезпечення їх реалізації. Беручи до уваги те, що Україна постійно перебуває під загрозою інформаційних атак, актуальним є ство-

рення та супровід державної системи моніторингу дезінформації, подібної до американського cisa.gov/rumorcontrol, де буде розміщуватися релевантна інформація. Це забезпечить дотримання свободи слова та протидію потенційним інформаційним загрозам. Актуальним є створення багаторівневої системи кібербезпеки як інструменту захисту критичної інфраструктури від гакерських атак інших держав. Зважаючи на постійні загрози, важливим механізмом посилення інформаційної безпеки та забезпечення обороноздатності країни може стати впровадження ініціативи «Zero Trust Architecture», що реалізує сучасні удосконалені методи захисту інформації. За прикладом США, Україні слід підтримувати розвиток технологій ІІІ з метою їх подальшого використання для протидії інформаційним і воєнним загрозам та посилення обороноздатності держави. Варто інвестувати у створення та навчання нейромереж, які збиратимуть та аналізуватимуть великі обсяги важливої інформації, зокрема військової, формуватимуть стратегії дій, об'єктивно оцінюватимуть фізичний та психологічний стан людини в критичних умовах та кризових ситуаціях, забезпечуватимуть безперервний зв'язок та захист від кібератак. Також потрібно зробити стратегію розвитку інформаційного впливу, зокрема, мовлення на віддалені регіони частиною своєї інформаційної політики. Маємо констатувати практично відсутність у цих регіонах спеціалізованих українських засобів масової інформації, які б висвітлювали актуальні новини про події в Україні, створювали та пропонували якісний освітній контент про українську історію, культуру та роль країни на міжнародній арені. Водночас тут активно функціонують засоби масової інформації, які поширюють анти-українську пропаганду, формують негативний образ України. Відтак, необхідно розробляти технології та шукати засоби для залучення глобальної аудиторії, зокрема шляхом створення державних агентств, які б забезпечували організацію телебачення, радіомовлення, друку преси та оформлення новинних сайтів арабською, китайською, корейською та іншими мовами, орієнтовані на населення Близького Сходу, Азії та інших регіонів світу. Не вичерпали свої

ресурси й засоби «м'якої сили» – поширення впливу через мистецтво. Україна має значний потенціал для створення фільмів, музики й художніх творів, які репрезентуватимуть особливості нашої історії та культури, національні інтереси з метою поширення впливу у міжнародній спільноті та формування національного бренду. Маємо достатньо потужну ІТ-індустрію, тому доцільно інвестувати у створення україноцентричного програмного забезпечення за прикладом офісних програм Microsoft, орієнтованого на глобальну аудиторію.

Література

1. Голованова Н. Інформаційна політика України в умовах війни (архетипний підхід). *Наукові перспективи*. 2022. № 6(24). С. 57-70. URL: [https://doi.org/10.52058/2708-7530-2022-6\(24\)-57-70](https://doi.org/10.52058/2708-7530-2022-6(24)-57-70).
2. Доктрина інформаційної безпеки України: Указ Президента України від 25 лют. 2017 р. № 47/2017. URL: <https://www.president.gov.ua/documents/472017-21374>.
3. Лешик С.В. Особливості інформаційної політики в процесі євроінтеграції України. *Політологічний вісник*. 2024. № 92. С. 198-210. URL: <https://doi.org/10.17721/2415-881x.2024.92.198-211>
4. Лисенко С. Майбутні тенденції інформаційної безпеки відповідно до технологій штучного інтелекту. *Публічне урядування*. 2020. № 5(25). С. 151-163. URL: [https://doi.org/10.32689/2617-2224-2020-3\(23\)-151-163](https://doi.org/10.32689/2617-2224-2020-3(23)-151-163).
5. Лопатченко І.С. Застосування досвіду США у використанні штучного інтелекту в забезпеченні національної інформаційної безпеки України. *Державне будівництво*. 2024. № 1(35). С. 247-257. URL: <https://doi.org/10.26565/1992-2337-2024-1-18>.
6. Олейніков Д. Зміст та складові інформаційного суверенітету як об'єкта кримінально-правової охорони. *Геополітичні пріоритети України*. Збірник наукових праць. 2021. Вип. 1(26). С. 60-69.
7. Про інформацію: Закон України від 02 жовт. 1992 р. № 2657-XII. *Відомості Верховної Ради України*. 1992. № 48. Ст. 650. URL: <https://zakon.rada.gov.ua/laws/show/2657-12#Text>.
8. Про рекомендації учасників парламентських слухань «Свобода слова в Україні: стан,

проблеми, перспективи»: Постанова Верховної Ради України від 25 квіт. 1997 р. № 236/97-ВР. *Відомості Верховної Ради України*. 1997. № 22. Ст. 162. URL: <https://zakon.rada.gov.ua/laws/show/236/97-%D0%B2%D1%80#Text>.

9. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки»: Указ Президента України від 28 груд. 2021 р. № 685/2021. URL: <https://www.president.gov.ua/documents/6852021-41069>.

10. Ржевська Н. Сучасна інформаційна політика: досвід США для України. *Політичні дослідження*. 2024. № 1(7). С. 68-85.

11. Черновол І.О., Чарських І.Ю. Інформаційна безпека США: проблеми та виклики в добу Дональда Трампа. *Вісник студентського наукового товариства ДонНУ імені Василя Стуса*. 2020. Т. 1 № 12. С. 110-115.

12. Яковлев П.О. Досвід державного регулювання забезпечення інформаційної безпеки зарубіжних держав (на прикладі Сполучених Штатів Америки, Канади, Німеччини, Франції). *Вісник Харківського національного університету імені В.Н. Каразіна. Серія «ПРАВО»*. 2020. Вип. 30. С. 106-113.

13. Announcing The Stargate Project. URL: <https://openai.com/index/announcing-the-stargate-project/>

14. National Cybersecurity Strategy. URL: <https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf>

15. National Security Strategy. URL: <https://bidenwhitehouse.archives.gov/wp-content/uploads/2022/11/8-November-Combined-PDF-for-Upload.pdf>

16. The Comprehensive National Cybersecurity Initiative. URL: <https://obamawhitehouse.archives.gov/node/233086>

17. Zero Trust Architecture. URL: <https://www.commerce.gov/ocio/key-initiatives/zero-trust-architecture>

References

1. Holovanova N. Informatsiina polityka Ukrainy v umovakh viiny (arkhetypnyi pidkhid). *Naukovi perspektyvy*. 2022. № 6(24). С. 57-70. URL: [https://doi.org/10.52058/2708-7530-2022-6\(24\)-57-70](https://doi.org/10.52058/2708-7530-2022-6(24)-57-70).

2. Doktryna informatsiinoi bezpeky Ukrainy: Ukaz Prezydenta Ukrainy vid 25.02.2017 № 47/2017. URL: <https://www.president.gov.ua/>

[documents/472017-21374](https://www.president.gov.ua/documents/472017-21374).

3. Leshyk S.V. Osoblyvosti informatsiinoi polityky v protsesi yevrointehratsii Ukrainy. *Politolohichni visnyk*. 2024. № 92. С. 198-210. URL: <https://doi.org/10.17721/2415-881x.2024.92.198-211>

4. Lysenko S. Maibutni tendentsii informatsiinoi bezpeky vidpovidno do tekhnolohii shtuchnoho intelektu. *Publichne uriaduvannia*. 2020. № 5(25). С. 151-163. URL: [https://doi.org/10.32689/2617-2224-2020-3\(23\)-151-163](https://doi.org/10.32689/2617-2224-2020-3(23)-151-163).

5. Lopatchenko I.S. Zastosuvannia dosvidu SShA u vykorystanni shtuchnoho intelektu v zabezpechenni natsionalnoi informatsiinoi bezpeky Ukrainy. *Derzhavne budivnytstvo*. 2024. № 1(35). С. 247-257. URL: <https://doi.org/10.26565/1992-2337-2024-1-18>.

6. Olieinikov D. Zmist ta skladovi informatsiinoho suverenitetu yak obiekta kryminalno-pravovoi okhorony. *Neopolitychni priorytety Ukrainy*. Zbirnyk naukovykh prats. 2021. Vyp. 1(26). С. 60-69.

7. Pro informatsiiu: Zakon Ukrainy. *Vidomosti Verkhovnoi Rady Ukrainy*. 1992. № 48. Ст. 650. URL: <https://zakon.rada.gov.ua/laws/show/2657-12#Text>.

8. Pro rekomendatsii uchashnykiv parlament-skykh slukhan «Svoboda slova v Ukraini: stan, problemy, perspektyvy»: Postanova Verkhovnoi Rady Ukrainy. *Vidomosti Verkhovnoi Rady Ukrainy*. 1997. № 22. Ст. 162. URL: <https://zakon.rada.gov.ua/laws/show/236/97-%D0%B2%D1%80#Text>.

9. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 15 zhovtnia 2021 roku «Pro Stratehiiu informatsiinoi bezpeky»: Ukaz Prezydenta Ukrainy vid 28.12.2021 № 685/2021. URL: <https://www.president.gov.ua/documents/6852021-41069>.

10. Rzhavska N. Suchasna informatsiina polityka: dosvid SShA dlia Ukrainy. *Politychni doslidzhennia*. 2024. № 1(7). С. 68-85.

11. Chernovol I.O., Charskykh I.Iu. Informatsiina bezpeka SShA: problemy ta vyklyky v dobu Donalda Trampa. *Visnyk studentskoho naukovoho tovarystva DonNU imeni Vasylya Stusa*. 2020. Т. 1. № 12. С. 110-115.

12. Yakovliev P.O. Dosvid derzhavnogo rehuliuвання zabezpechennia informatsiinoi bezpeky zarubizhnykh derzhav (na prykladi Spoluchenykh Shtativ Ameriky, Kanady, Nimechchyny, Frantsii). *Visnyk Kharkivskoho natsionalnogo universytetu imeni V.N. Karazina. Seriia «PRAVO»*. 2020.

Vyp. 30. S. 106-113.

13. Announcing The Stargate Project. URL: <https://openai.com/index/announcing-the-stargate-project/>

14. National Cybersecurity Strategy. URL: <https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf>

15. National Security Strategy. URL:

<https://bidenwhitehouse.archives.gov/wp-content/uploads/2022/11/8-November-Combined-PDF-for-Upload.pdf>

16. The Comprehensive National Cybersecurity Initiative. URL: <https://obamawhitehouse.archives.gov/node/233086>

17. Zero Trust Architecture. URL: <https://www.commerce.gov/ocio/key-initiatives/zero-trust-architecture>

Svitlana Holovko, Nataliia Holovko

STATE INFORMATION POLICY AS A TOOL FOR COUNTERING GLOBAL CHALLENGES AND THREATS: INTERNATIONAL EXPERIENCE AND ITS IMPLEMENTATION IN UKRAINE

State University «Kyiv Aviation Institute»

Liubomyra Husara Avenue, 1, 03058, Kyiv, Ukraine

Taras Shevchenko National University of Kyiv

Yuriia Illienka St, 36/1, 04119, Kyiv, Ukraine

E-mails: golovkos@ukr.net, natalijaholovko123@ukr.net

Purpose: to actualize the priority tasks for developing the state information policy of Ukraine in the context of modern challenges and threats and international experience in overcoming them using the example of the USA as a leading actor in the global information space. **Methods:** based on the results of comparative legal analysis, priority tasks, key challenges and threats to the information sphere of Ukraine, mechanisms and features of the implementation of the state information policy of the USA are outlined; the documentary method is used to analyze the legislative and regulatory support for the implementation of the state information policy; the prognostic method is used to determine the prospects for improving the state information policy of Ukraine, taking into account international experience. **Results:** the problem of developing the state information policy of Ukraine is actualized, the main challenges and threats to the information sphere in wartime conditions are identified; the need to improve state information policy in the context of integration into the European and global information space using international experience is substantiated; the mechanisms and means of implementing the US state information policy are analyzed in terms of its strategic concepts, legislative support, strengthening the influence on the international information space, implementing a system of cybersecurity measures and regulating innovations in the field of development of neural networks and artificial intelligence technologies. **Discussion:** the balance of state interests in the field of information security as a component of national security and ensuring compliance with human rights and freedoms as the highest value of civil society.

Key words: state information policy of Ukraine; information security; US experience in regulating the national and global information space.

Стаття надійшла до редакції 11.03.2025