УДК 327.8:[004:007](73:477)
DOI: https://doi.org/10.53317/2786-4774-2024-1-4

Сучасна інформаційна політика: досвід США для України

Ніна Ржевська,
доктор політичних наук, професор,
Національний авіаційний університет

Nina Rzhevska,
Doctor of Political Science, Professor,
National Aviation University

ORCID 0000-0003-0963-1311
rzhevskanina@ukr.net

Анотація. У статті обґрунтовано необхідність оптимізації сучасної інформаційної політики України, виокремлено можливі напрями підвищення її ефективності завдяки впровадженню в практику досвіду США. Важливо розуміти, що інформаційна політика держави має спрямовуватися на формування державного інформаційного простору, розширення і вдосконалення правової бази регулювання суспільних відносин залежно від конкретних обставин, поширення та використання інформації, поглиблення політичної стабільності та гарантування інформаційної безпеки суспільства.

Інформаційна політика забезпечує інформаційні ресурси скоординованим технологічним супроводом, надає вільний доступ до них, забезпечує користувачів інструментами ефективного пошуку, використання та передачі інформації. Важливо, що дієвість інформаційної політики можна забезпечити лише шляхом консенсусу, залучивши всі зацікавлені сторони.

Слід наголосити, що в умовах війни інформаційна політика є системою заходів, здійснюваних державою разом із інститутами громадянського суспільства, скерованих на регулювання інформаційних процесів, формування та розвиток інформаційного суспільства, де пріоритетними є оборонні цілі. З огляду на це, серйозною проблемою є відсутність законодавчої бази, що регулює захист інформації, забезпечує протидію новим загрозам в інформаційному просторі й упроваджує заходи щодо відповідальності за дії або організовану діяльність, що завдають шкоди інформаційній безпеці Збройних сил України.

Державі та громадянському суспільству запропоновано практичні рекомендації з формування умов створення оптимальної моделі державної інформаційної політики, адаптивної до різних ситуацій, зокрема, до умов воєнного стану.

Ключові слова: Україна, США, інформаційна політика, інформаційна безпека, захист інформації, інформаційний простір, ефективна інформаційна політика.

Modern Information Policy: The US Experience for Ukraine

Abstract. The article argues for the need to enhance Ukraine's state modern information policy, identifying potential avenues for improvement of its effectiveness by drawing upon the experience of the United States. It is important to understand that the information policy of the state should be aimed at the formation of the state information space, at expanding and refining the legal framework for regulating social relations based

on specific circumstances, dissemination and utilization of information, deepening of the political stability, and ensuring societal information security.

Information policy ensures that information resources receive coordinated technological support, offers unrestricted access to them, and provides users with tools for effective information search, use, and transfer. It is essential that the effectiveness of information policy can only be achieved through consensus, involving all interested parties.

It is crucial to understand that information policy in times of war entails a set of measures implemented by the state in collaboration with civil society institutions, aimed at regulating information processes and fostering the development of an information society where defense goals take priority. Consequently, a significant challenge arises from the absence of a legislative framework regulating information protection and counteracting new threats in the information sphere, and implements measures regarding responsibility for actions or organized activities that harm the information security of the Armed Forces of Ukraine.

The state and civil society are provided with practical recommendations for creating conditions conducive to the development of an optimal model of state information policy, adaptable to various situations, including those under martial law.

Key words: Ukraine, USA, information policy, information security, information protection, information space, effective information policy.

Постановка проблеми та актуальність дослідження. Інформаційна політика, як окрема дослідницька площина, опинилася в центрі уваги лише по завершенні минулого, XX століття, що промовисто засвідчило про перехід до інформаційного суспільства. Раніше споживання інформації можна було розумно нормувати потребою набуття знань, наслідки від чого не були значними. В інформаційному ж суспільстві доступ до інформації стає необхідністю, а інформація є не лише суспільним благом, а й суспільним ресурсом. Як особливий продукт виробничих відносин, інформація потребує ретельного контролю за її використанням і запровадженням інформаційної політики з боку держави як відповідального суб'єкта за її імплементацію.

Запроваджувана державою інформаційна політика є важливим чинником функціонування інформаційного суспільства, що сприяє і залучає різні соціальні групи до політичного життя, забезпечує доступ до влади та розвиток пріоритетних напрямів внутрішньої й зовнішньої політики [Сірий та Турченко, 2012, с. 238].

Слід розуміти, чому в інформаційному суспільстві важливо запроваджувати інформаційну політику на державному рівні. На нашу думку, ця потреба викликана тим, що це є важливою умовою формування інформаційної свідомості населення, зміцнення засад громадянського суспільства, задоволення інтересів його суб'єктів і захисту їхніх прав і свобод.

У своїх цілях інформаційна політика спрямовується на розв'язання загальнодержавних завдань; формування інформаційного простору держави та її входження до світового інформаційного простору; розвиток галузі інформаційних послуг; розширення правової бази, що регулює суспільні відносини, зокрема, пов'язані з отриманням, поширенням і використанням інформації; підвищення політичної стабільності в країні та гарантування

інформаційної безпеки суспільства і держави. Досягнення означених цілей потребує ефективного менеджменту всіма видами інформаційних ресурсів, елементами інформаційно-телекомунікаційної інфраструктури, а ще — державної підтримки вітчизняного ринку інформаційних технологій, засобів, продуктів і послуг та регулювання діяльності державних електронних і друкованих медіа [Rzhevska & Feshchenko, 2022, p. 249].

Незважаючи на значну кількість дослідницьких напрацювань щодо державної інформаційної політики, зокрема в Україні, вивчення інформаційної сфери суспільства залишається актуальним, враховуючи зростаючі всебічні виклики, що неспинно постають перед нею. Зокрема, актуальним залишається пошук шляхів підвищення ефективності інформаційної політики в умовах воєнного стану, що, частково, є можливим завдяки дослідженню і впровадженню досвіду найкращих світових практик із розвитку інформаційної сфери.

Аналіз досліджень і публікацій. Уже понад півстоліття проблема створення дієвої моделі інформаційної політики перебуває в центрі зарубіжних дослідницьких ініціатив. Про це засвідчують праці Н. Вінера, Д. Белла, Е. Бредлі, П. Бурдьє, Б. Гунтера, М. Дженіса, М. Кастельса, Р. Кея, М. Мая, М. Маклюена, Т. Пітерсона, Ф. Сіберта, У. Шрамма та багатьох інших.

Світові зразки моделей державної інформаційної політики, її концептуальне обґрунтування, проблеми управління інформаційними ресурсами в державі та організаційно-правові аспекти представлені в наукових працях українських дослідників: О. Ляшенко [2015], І. Дацків [2019], О. Токар [2009], М. Пахніна [2014], І. Арістової [2000], В. Брижка [2009], І. Панової [2014]. Окремо варто відзначити праці Г. Бондар та Л. Ракутіної [2020], О. Солодкої [2013], у яких ідеться про співвідношення інформаційної політики та інформаційної безпеки, праці Ю. Нестеряка [2014; 2018], В. Негодченко [2016], Ю. Мохової та А. Луцької [2018], С. Сірого та Ю. Турченко [2012], В. Фурашева [2009], Н. Голованової [2022] з питань інформаційної політики України, її змісту, головних напрямів і способів реалізації. Серед дослідників державної інформаційної політики та стратегії інформаційної безпеки в США цікавими є праці В. Морозової [2014], О. Олійника [2012a, 2012b], В. Разіцького [2008], К. Голода [2017]. Водночас, попри дослідницьку увагу зарубіжних та вітчизняних науковців до інформаційної політики держави, донині малодослідженими залишаються проблеми можливостей щодо її оптимізації в Україні, враховуючи світовий досвід.

Мета статті полягає у виокремленні можливих напрямів удосконалення та підвищення ефективності інформаційної політики України, наданні пропозицій стосовно впровадження в практику досвіду здійснення інформаційної політики США.

Виклад основного матеріалу. Традиційно інформаційна політика охоплює питання стосовно доступу та захисту урядової інформації**.** Проте слід зауважити, що протягом 1970-х і 1980-х років національні уряди наполягли на розробці комплексної національної інформаційної політики. На нашу думку, це свідчить, що саме інформаційна політика має створювати умови

для прийняття ефективних державних рішень, конструктивного публічного дискурсу та продуктивної політичної діяльності.

З'ясовуючи причини формування і розвитку інформаційної політики, слід відзначити, що до 1980-х років політика держав світу, американська зокрема, спричинила розвиток технологій до такої міри, що державні та федеральні урядові установи помітно посприяли розширенню досліджень інформаційної сфери [Rzhevska & Feshchenko, 2022, p. 250]. З іншого боку, збільшення інноваційних розробок та їх поширення продемонстрували, що розвиток інформаційної політики безпосередньо залежить від технологічного прогресу. Це й змусило тих, хто досліджує інформаційну політику, відійти від традиційних поглядів [Jaeger et al., 2015].

Тривалий час політику в сфері інформації вважали мало значимою. Концепція національної інформаційної політики, окремо, стала можливою завдяки віднесенню законів та нормативних актів, що регулюють інформацію, до стратегічно значимих. У кінцевому підсумку, не багато урядів запровадили єдиний комплекс інформаційної політики. Та, незважаючи на це, у світі формування й запровадження інформаційної політики і надалі зростає.

Зазвичай прерогативою інформаційної політики є конфіденційність, безпека, інтелектуальна власність і електронне врядування. Тут важливо розуміти, що виключного залучення до вирішення цих завдань фахівців-інформаційників не достатньо. Суттєво, щоб інформаційну політику розробляли й імплементували ті, хто розуміє, що інформаційний супровід є системним і виконує комунікаційну місію.

У широкому розумінні термін „інформаційна політика" позначає всі закони, нормативні акти та доктринальні положення стосовно інформації, комунікації та культури. Окремо він містить дії щодо ухвалення рішень та їхнього виконання, втілення яких має конструктивні наслідки для всього суспільства [Braman, 2011].

За впровадження інформаційної політики в Україні відповідальними є Президент України, Верховна Рада України, Кабінет Міністрів, Національна рада України з питань телебачення і радіомовлення та Міністерство цифрової трансформації України [Деякі питання оптимізації системи центральних органів виконавчої влади, 2019], що стало „головним органом у системі центральних органів виконавчої влади, що забезпечує формування та реалізацію державної політики: у сферах цифровізації, цифрового розвитку, цифрової економіки, цифрових інновацій та технологій, робототехніки та роботизації, електронного урядування та електронної демократії, розвитку інформаційного суспільства, інформатизації; у сфері впровадження електронного документообігу; у сфері розвитку цифрових навичок та цифрових прав громадян; у сферах відкритих даних, публічних електронних реєстрів, розвитку національних електронних інформаційних ресурсів та інтероперабельності, електронних комунікацій та радіочастотного спектра, розвитку інфраструктури широкосмугового доступу до Інтернету, електронної комерції та бізнесу; у сфері надання електронних та адміністративних

послуг; у сферах електронних довірчих послуг та електронної ідентифікації; у сфері розвитку ІТ-індустрії; у сфері розвитку та функціонування правового режиму Дія Сіті; у сфері хмарних послуг" [Положення про Міністерство цифрової трансформації, 2019]. Створення такого міністерства демонструє зацікавленість держави в контролі сфери інформаційного простору задля безпеки громадян та всієї країни.

Для формулювання цілей державної інформаційної політики об'єктивним буде те, що вона має скеровуватися на формування інформаційного простору держави; розширення і вдосконалення правової бази для регулювання суспільних відносин, націлених на здобуття, поширення та використання інформації; поглиблення політичної стабільності в державі та гарантування інформаційної безпеки суспільства.

Вирішення зазначених завдань потребує ефективного управління всіма видами інформаційних ресурсів, елементами інформаційно-телекомунікаційної інфраструктури, державної підтримки вітчизняного ринку інформаційних технологій, засобів, продуктів і послуг та регулювання діяльності державних електронних і друкованих медіа.

Серед значимих характеристик інформаційної політики є те, що вона забезпечує інформаційні ресурси послідовним, скоординованим та тривалим технологічним супроводом, створює вільний доступ до них, пропонує користувачам інструменти ефективного пошуку, використання та передачі інформації. Важливо розуміти, що дієву інформаційну політику можна розробити лише шляхом консенсусу, залучивши всі зацікавлені сторони, що значно підвищить її стійкість та імовірність упровадження.

І, нарешті, однією з особливостей, що ставлять інформаційну політику поряд із найбільш дієвими інструментами міжнародної взаємодії, є те, що вона може бути засобом розв'язання глобальних проблем.

Проте інформаційна політика, зазвичай, не є самоціллю. Саме тому іноді уряди не підтримують необмежений глобальний доступ до інформації та її поширення, використовують інформаційну політику у власних цілях, перешкоджаючи комунікації й обговоренню адміністративних дій, захисту приватних інтересів, чим підсилюють панічні настрої в суспільстві [Weiner, 2013].

Інформаційна політика в умовах війни. Якщо мовиться про державну інформаційну політику в умовах війни, то вона має скеровуватися на вирішення основних завдань розвитку всього суспільства. Серед них важливим є створення єдиного інформаційного простору та долучення до світового інформаційного простору, гарантування інформаційної безпеки особистості, суспільства та держави [Горбань, 2015, с. 138]. Тож, у нинішньому вітчизняному контексті інформаційна політика має бути інструментом гарантування безпеки людини, суспільства, держави й світової спільноти

Інформаційна політика в умовах війни — це система заходів, здійснюваних державою разом із інститутами громадянського суспільства, скерованих на регулювання інформаційних процесів, формування та розвитку інформаційного суспільства, де пріоритетними є оборонні цілі. Така пріоритетність викликана потребою захистити права й інтереси

людини, моральні цінності, гарантувати інформаційну безпеку особистості, суспільства і держави.

Суттєвим є те, що алгоритм роботи представників медіа в умовах воєнного стану, в Україні зокрема, обмежує розголошення інформації, що може призвести до оприлюднення стратегічних даних про дії ЗСУ та військові об'єкти. Окремо встановлені правила роботи журналістів для цього періоду вимагають обмежень під час поширення інформації, бо це може суттєво зашкодити національній безпеці.

Організаційні та правові засади реалізації державної інформаційної політики в умовах воєнного стану. Державна інформаційна політика в умовах війни в сфері медіа в Україні регулюється Законом України „Про медіа" від 13 грудня 2022 року [Про медіа, 2022], що покликаний гарантувати права на свободу висловлення думок, на отримання різнобічної, достовірної та оперативної інформації, права на захист національних інтересів України і права користувачів медіа-сервісів. Згідно з цим законом діяльність у медіасфері регулюється відповідно до принципів прозорості, справедливості та неупередженості.

Проте, на жаль, нині нормативно-правова діяльність не охоплює такий важливий аспект діяльності медіа, як журналістське розслідування. Ідеться про відсутність всебічного аналізу та вивчення фактів і подій, що стосуються латентних аспектів суспільних проблем та справжніх причин їхнього нерозголошення перед громадським загалом. В умовах війни та інформаційного протистояння агресорові зростає вагомість неупереджених результатів такого аналізу.

Саме під час воєнного стану актуалізується питання правомірності оприлюднення результатів журналістського розслідування та їхнього публічного обговорення, що може призвести до гострого протистояння між суб'єктами державної влади та медіа. Така ситуація деструктивно впливає на психологічний стан громадян, загрожує цілісності соціальної системи, порушує єдність громадянського суспільства та держави [Терещенко, 2023].

Отже, забезпечення балансу інтересів у цій ситуації можливе завдяки встановленню відповідних нормативно-правових положень на рівні підзаконних актів, дія яких обмежується періодом воєнного стану. І хоча в демократичному суспільстві неможливо заборонити проведення журналістських розслідувань, у період воєнного конфлікту потрібно накладати обмеження, зокрема, на процедуру оприлюднення його результатів.

Інформація, здобута під час такого розслідування, може бути розглянута як орієнтовна, але далі її необхідно передавати до компетентних правоохоронних органів держави для подальшої перевірки і встановлення обсягу даних для публічного оприлюднення. Пріоритетом у цьому має бути захист інтересів суспільства, держави, прав та свобод громадян в умовах війни.

Указом Президента України від 25 лютого 2017 року була затверджена „Доктрина інформаційної безпеки України" [Доктрина про інформаційну безпеку України, 2017]. Проте в умовах повномасштабного воєнного вторгнення, 18 березня 2022 року, було ухвалено рішення Ради національної

безпеки і оборони України (РНБО) „Щодо реалізації єдиної інформаційної політики в умовах воєнного стану", в якому визначено, що в умовах воєнного стану реалізація єдиної інформаційної політики є пріоритетним завданням національної безпеки [Про медіа, 2022]. Також створено Центр протидії дезінформації при РНБО України, де можна здобути актуальну інформацію щодо інформаційно-безпекових викликів і подій.

Нині ми спостерігаємо зростання загроз від наслідків застосування методів інформаційного впливу з боку стратегічних противників та глобальних терористичних організацій. Це — не лише окремі військово-політичні операції, а й показники розвитку стратегічного потенціалу. Захист від таких загроз є надважливим для Збройних сил України та їхнього особового складу, який є головною мішенню для ураження.

Захист інформаційних ресурсів. Наразі пріоритетним завданням є захист інформаційних ресурсів, саме тому фахівці з безпекових питань, а особливо — інформаційно-безпекових, повинні вміло управляти інформаційними потоками та використовувати їх для захисту держави.

Планування та реалізація цілеспрямованого інформаційного впливу на військовослужбовців вимагає попередньої підготовки та навичок ідентифікації таких загроз. Найбільш серйозною проблемою, з погляду безпеки, є використання соціальних мереж, через які важлива інформація випадково може стати доступною широкому колу осіб. Саме тому серед головних завдань є виявлення таких загроз та їх негайне усунення.

Заходи з гарантування безпеки можна розділити на дві групи [Цимбалюк та Бабінська, 2014]. До першої групи належить захист інформаційних систем від пошкодження і запобігання витоку та перехоплення інформації. Це містить у собі захист об'єктів військової дислокації та комп'ютерної техніки від пошкодження, захист від віддаленого вторгнення, гарантування безпеки інформації, що становить державну або військову таємницю, радіоелектронний захист, використання захищених моделей комп'ютерів і програмного забезпечення, а також захист систем зв'язку.

Друга група заходів спрямована на запобігання цілеспрямованого інформаційно-психологічному впливу на психіку військовослужбовців та корекцію інформації, що транслюється потенційними супротивниками. Це вимагає досліджень методів впливу на психіку, ведення психологічної роботи з військовослужбовцями та ін.

Для успішної реалізації цих заходів потрібно створити спеціалізовані підрозділи і використовувати найновіші наукові розробки та програмне забезпечення. Важливо знати, що робота в цьому керунку вимагає комплексного підходу та співпраці між різними підрозділами спеціалізованих служб та аналітичними центрами.

Інформаційна безпека військових формувань. Надзвичайно важливою стає інформаційна безпека військових формувань, оскільки деморалізація війська безпосередньо впливає на зниження бойового духу та підрив його бойової готовності. Також необхідно запобігати спрямованому впливу на

особовий склад через фальсифікацію інформації, посилення соціальної напруги та спроби втягнути його представників у політичні конфлікти. З цією метою проводиться психологічно-просвітницька робота з особовим складом та налагоджується співпраця з органами місцевої влади, щоб запобігти провокаційній діяльності засобів масової інформації та інших джерел інформаційних атак [Ніщименко, 2016, с. 18].

Є випадки, коли вплив на військовослужбовців виходить за межі психологічного тиску, що спричиняє не лише психічні розлади, а й — воєнні злочини чи дезертирство, призводить до створення серед військових груп, що мають на меті свідомий підрив обороноздатності держави.

Технічні проблеми помітно впливають як на функціонування інформаційних систем, що використовуються військами, включаючи системи управління, так і на збереження конфіденційної інформації, що передається військовими каналами. Це можуть бути збої в роботі системи, навмисне її пошкодження, крадіжка інформації та недбалість окремих співробітників.

Заходи захисту передбачають підвищення рівня безпеки автоматизованих систем управління і навчання персоналу відповідно до вимог захисту інформації. На державному рівні стандарти безпеки гарантуються шляхом їхнього дотримання та використання інших методик. Проте на практиці часто зволікають із упровадженням нових програмно-технічних засобів, що є умовою захисту від загроз противника. Таке зволікання може стати загрозою для загальної безпеки [Новицький, 2016, с. 34].

Досить складно реагувати на виклики технічного характеру, що містять у собі навмисне пошкодження техніки та комунікаційних ліній, іноді через недбалість особового складу або навмисні дії противника. Порушення інформаційної складової в системі життєзабезпечення військової техніки, спричинене необачністю або спеціальними атаками, може призвести до трагедій та загибелі екіпажу. Також існує ризик атак на інформаційні системи ядерних об'єктів, зокрема, серйозну загрозу становить потрапляння неправдивої інформації в систему виявлення можливих атак. Необхідно вживати заходів для запобігання цим загрозам та гарантування інформаційної безпеки військових частин.

Нині серйозною проблемою є недостатня розвиненість законодавчої бази, що регулює захист інформації і протидію новим загрозам в інформаційному просторі. Низка аспектів таких явищ і їх можливих наслідків досі не відображені в нормативних актах [Олійник, 2012а, с. 65]. Це ускладнює впровадження заходів щодо відповідальності за дії або організацію діяльності, що може завдавати шкоди інформаційній безпеці Збройних сил України та військовослужбовцям. Проте ситуація поступово змінюється, розробляються нормативно-правові акти, що регулюють використання військової техніки та інших технологій, особливо іноземного виробництва.

Вище зазначалося, що з уведенням в Україні воєнного стану було внесено зміни до законодавчо-правої бази у сфері інформаційної політики та інформаційної безпеки, що враховують реалії війни. Ці зміни стосуються регулювання окремих аспектів інформаційної політики, вклю-

чаючи обмеження поширення конкретної інформації, зважаючи на її суспільно небезпечний характер, регламентацію щодо обсягу інформації для оприлюднення в умовах воєнного стану, посилення відповідальності за поширення певних видів інформації та процедур здобуття інформації. Наприклад, на законодавчому рівні було введено кримінальну відповідальність за незаконну фото- та відеозйомку переміщень військовослужбовців, зброї і техніки.

Управління суспільними процесами з боку держави неможливе без різних джерел і потоків інформації, що відображають соціальні потреби та інтереси різних суб'єктів соціально-політичного процесу і сприяють підвищенню ефективності діяльності державних органів. Взаємодія між державними органами та медіа залежить від політичної ситуації і специфіки взаємодії громадянського суспільства і влади на певному етапі їх розвитку [Захаренко, 2021].

Поява нових загроз в інформаційному просторі в період воєнного стану вимагає постійного пошуку шляхів і засобів їхньому протистоянню та подоланню наслідків впливу, що сприятиме гарантуванню інформаційної безпеки Збройних сил України.

Варто зазначити, що Україна представила дієву інформаційну політику від початку повномасштабної війни. Так, з метою інформування громадян оперативно було створено і поширено необхідні офіційні сторінки та канали державних підприємств у соціальних мережах. Створення єдиного порталу державних послуг у додатку „Дія" сприяє інформаційному розвитку держави, завдяки чому населення має доступ до основних документів та певних функцій у смартфоні, якими багато хто користується. Для Української держави необхідними є регуляція інформаційної діяльності населення, створення безпечних умов використання інформації, забезпечення його електронним документообігом, доступним у смартфоні. Створення електронного уряду надало Україні статусу інноваційної держави.

На нашу думку, вивчення зарубіжних моделей інформаційної політики, особливо в контексті гарантування інформаційної безпеки, є надзвичайно важливим для вітчизняної практики. Щодо цього, вагомим є досвід США, оскільки вони були першою державою, що впровадила електронне урядування з використанням передових інформаційних технологій, сформували систему захисту національного інформаційного суверенітету та безпеки інформаційних ресурсів [*International Strategy for Cyberspace*, 2011].

Інформаційна політика США втілюється згідно з такими принципами: захист особистого життя, безпека і надійність мереж; сприяння технологічним інноваціям; координація державних зусиль; залучення приватних інвестицій; забезпечення доступу до державної інформації; забезпечення інтерактивного доступу; концепція універсального доступу та поліпшення управління радіочастотним спектром.

Щодо гарантування інформаційної безпеки, Сполучені Штати мають відповідальні державні інституції, зокрема йдеться про Агентство національної безпеки (АНБ), Національне управління кібербезпекою при

Міністерстві внутрішньої безпеки США, Федеральне бюро розслідувань (ФБР) та Центральне розвідувальне управління (ЦРУ).

Зокрема, АНБ співпрацює з приватним сектором і науковими установами у справах боротьби з загрозами неурядовим комп'ютерним мережам. Така співпраця містить заходи щодо захисту приватних телекомунікаційних, електронних та банківських мереж, а також — заходи, спільні разом із приватними установами і громадськими організаціями, з протидії тероризму [Голод, 2017].

Слід зауважити, що вже на початку нинішнього століття понад 150 державних організацій [Проценко та Тупчієнко, 2012] і багато приватних структур США залучено до гарантування інформаційної безпеки. Всі ці заходи координує АНБ, проте головною інституцією, що відповідає за державне регулювання інформаційною безпекою, є президент.

Сучасна організаційно-правова база збереження інформаційної безпеки Сполучених Штатів, що гарантує безпеку інформаційної та оборонної системи, з'явилася після Другої світової війни, саме тоді, коли американська інформаційна система стала прицільним об'єктом деструктивного впливу радянської пропаганди. Ця правова база охоплює федеральні закони та закони штатів. Усупереч відмінностям між цими законами, у США існує загальне розуміння того, що інформаційна безпека держави є важливою для безпеки кожного громадянина [United nations development programme, 2022].

Правовим підґрунтям адміністрування інформаційною безпекою США є низка федеральних законів, зокрема, „Про охорону особистих таємниць" (1974), „Про таємницю" (1974), „Про висвітлення діяльності уряду", „Про право на фінансову таємницю" (1978), „Про доступ до інформації та про діяльність ЦРУ" (1984), „Про безпеку комп'ютерних систем" (1987), „Про комп'ютерне шахрайство та зловживання" (1986) та інші. Особливе значення мають Директиви президента США, де визначено політику і стратегію інформаційної безпеки держави. Такою, до прикладу, є Директива PD/NSC-24 (1977), що визначила політику в галузі захисту систем зв'язку, Директива SDD-145 (1984), що окреслила національну політику безпеки систем зв'язку в автоматизованих інформаційних системах.

У 1990-х роках, коли інформаційні відносини почали активно розвиватися і набувати глобального характеру, у Сполучених Штатах були прийняті федеральні закони, спрямовані на гарантування інформаційної безпеки. Серед них — закони „Про інформаційну безпеку" та „Про удосконалення інформаційної безпеки", ухвалені в 1997 році [Morze & Veselovska, 2014]. Поряд із цим, зростання ролі інформаційних технологій у військовій сфері привело до збільшення військового впливу на інформаційну безпеку.

У 1992 році була введена в дію Директива Міністерства оборони США „Інформаційна війна", що окреслила політику щодо захисту інформаційних ресурсів і надала відповідної значимості самому поняттю „інформаційна війна". Директива охоплювала різні аспекти інформаційної безпеки, зокрема, психологічний вплив на супротивника, оперативну безпеку, електронне втручання, інформаційну розвідку, інформаційний захист та інші.

Задля гарантування інформаційної безпеки у США велике значення приділяється управлінню інформаційними ресурсами. Основна мета цього — убезпечення власної системи інформаційної безпеки та вплив на інформаційно-безпекову систему потенційного супротивника [United nations development programme, 2022].

Починаючи з 2001 року гарантування інформаційної безпеки було визнано головним пріоритетом національної безпеки у Сполучених Штатах і запроваджено загальні федеральні програми захисту національного інформаційного середовища в комп'ютерних мережах. Метою цих програм було створення умов для розвідувальних органів зі збору та обробки інформації стосовно загроз інформаційному потенціалу держави від інших країн та осіб. Це привело до розвитку нормативно-правової бази щодо протидії кіберзлочинності.

У 2003 році введено Національну стратегію безпечного кіберпростору, а в подальшому — прийняті різні законодавчі акти і директиви, що регулюють кібербезпеку. Особливу увагу приділяють взаємодії між державними інституціями у сфері кібербезпеки та розробці стандартів електронної аутентифікації [United nations development programme, 2022].

Значимо, що у 2009 році в Конгресі був представлений проєкт закону „Акт про кібербезпеку", що надавав президентові США повноваження обмежувати доступ до Інтернету в будь-якій частині країни в разі загрози національній безпеці. Цей закон наголошує на ключовій ролі президента в управлінні системою кібербезпеки та визначає його вагу для захисту інформаційних проєктів загально федерального, регіонального та місцевого рівнів у сфері кібербезпеки.

За президента Б. Обами цифрову інфраструктуру США було визнано стратегічною національною цінністю, а захист цієї інфраструктури став національним пріоритетом. Таке бачення ґрунтується на ідеї М. Макклюена [McLuhan & Parkerm, 1968] про те, що в сучасному світі обмін знаннями та інформацією стає ключовим, переважаючи над обміном товарами. Таким чином, боротьба за доступ до інформаційних ресурсів та знань стає головною проблемою національної безпеки.

У 2010 році запроваджена „Ініціатива зі всебічної національної кібербезпеки", що передбачала створення загальної федеральної мережі захищених зв'язків і спеціальних підрозділів кіберконтррозвідки для виявлення та запобігання загрозам інформаційним мережам у державі. Також була розроблена система управління ризиками у прогнозуванні можливих наслідків несанкціонованого втручання в інформаційні мережі державних установ. Для визначення втручання в державні інформаційні мережі була запроваджена програма „Ейнштейн" [Privacy Impact Assessment EINSTEIN Program, 2004].

З 2012 року хакерські атаки в США стали кваліфікуватися як збройна агресія, що вимагає відповідного реагування, а значна частина фінансування науково-дослідних розробок у США — спрямовуватися на розробку систем захисту інформації. Черговим свідченням значущості управління

інформаційною безпекою у Сполучених Штатах на державному рівні є заява Адміністрації Дж. Байдена про виділення з федерального бюджету 2024 року 27,5 млрд доларів на кібербезпеку [*The US Federal Budget Allocates …*, 2024], а також — стратегічне зосередження на захисті кіберпростору дослідницьких центрів та корпорацій, що впливають на розвиток технологій, фінансову стабільність і зростання економічних показників світового співтовариства [Голод, 2017].

Зважаючи, що інформаційна індустрія є головним стратегічним чинником конкуренції та провідним сектором економіки, інформаційна політика США охоплює широке коло урядових заходів, спрямованих на створення інформаційних технологій та управління ними. Одним із ключових напрямів розвитку американської інформаційної безпеки, як і в інших державах, є гарантування національної безпеки та безпеки інформаційних систем „силових" відомств: збройних сил та зовнішньої розвідки [Терещенко, 2023].

Проєкція державних пріоритетів Сполучених Штатів у гарантуванні інформаційної безпеки на вітчизняну практику дає змогу дійти **висновку,** що українська інформаційна політика потребує розвиненої системи реагування на події у сфері інформаційної безпеки; реалізації комплексних заходів щодо зменшення загроз інформаційній безпеці; забезпечення підготовки спеціалістів у сфері комп'ютерної безпеки та відповідального ставлення всього населення до питань захисту інформації, а також забезпечення надійного захисту інформаційних систем державних органів, а особливо — розвитку різних форм (надто — міжнародних) кооперації у сфері гарантування інформаційної безпеки.

Вирішуючи завдання з визначення умов створення моделі національної інформаційної політики, адаптивної до різних ситуацій, зокрема до умов воєнного стану, державі та громадянському суспільству варто зосередитися на:

— створенні й упровадженні дійових механізмів реалізації конституційних і законних інформаційних прав і свобод громадянина, суспільства і держави в Україні;

— формуванні єдиної державної системи зв'язків із громадськістю, забезпеченої інформаційною культурою;

— постійному вдосконаленні інформаційного законодавства України, враховуючи світовий досвід і реалії вітчизняного сьогодення;

— безперестанному розвитку й удосконаленні, враховуючи досягнення сучасних інформаційних технологій, національної інформаційної інфраструктури, системи інформаційно-аналітичного забезпечення Президента України та органів державної влади, підвищенні конкурентоспроможності вітчизняних виробників інформаційного продукту;

— встановленні порядку функціонування та розробці дієвих механізмів забезпечення державного контролю за супутниковими, кабельними й комп'ютерними системами передачі інформації;

— забезпеченні лібералізації українського ринку телекомунікацій за умови гарантування реалізації національних інтересів та недопущення монополізації інформаційних ринків;

— розвитку науково-технічного та кадрового забезпечення інформаційної галузі;

— і, нарешті, забезпеченні інформаційного суверенітету України та вдосконаленні системи захисту національних інформаційних ресурсів.

Окрім усього, розробляючи сучасну національну інформаційну політику, доцільно створити проєкт фінансування технологічної бази держави та формування навичок у населення щодо правильного використання інформації, паралельно формуючи закони, що регулюватимуть таку діяльність.

Інформаційна політика України постійно наражається на нові виклики, адаптуючись до умов сьогодення. Попри все, вона беззаперечно має потенціал для подальшого вдосконалення. Забезпечення відкритості, прозорості, адаптивності та ефективної взаємодії з громадськістю є ключовим пріоритетом у подальшому поступі національної інформаційної політики.

Актуальним для України залишається питання створення оптимальної моделі забезпечення національної політики в інформаційній сфері, що є можливим завдяки вивченню досвіду держав розвиненого інформаційного суспільства.

Бібліографічні посилання

Арістова, І. В. (2000). *Державна інформаційна політика: організаційно-правові аспекти* (О. М. Бандурко, Ред.). Харків: Вид-во Ун-ту внутр. справ.

Бондар, Г., & Ракутіна, Л. (2020). Інформаційна політика та інформаційна безпека. *Публічне управління та митне адміністрування, 4*(23), 42–49.

Брижко, В. М. (2009). Про сучасну інформаційну політику. *Правова інформатика, 2*(22), 1–43.

Голованова, Н. (2022). Інформаційна політика України в умовах війни (архетипний підхід). *Наукові перспективи, 6*(24), 57–70. http://perspectives.pp.ua/index.php/np/article/view/1864

Голод, К. (2017). Інформаційна безпека США: сучасний стан та уроки для України. *Геополітика України: історія і сучасність, 2*(19), 91–107.

Горбань, Ю. О. (2015). Інформаційна війна проти України та засоби її ведення. *Вісник Національної академії державного управління при Президентові України, 1*, 136–141.

Дацків, І. (2019). Вплив світового досвіду на формування основних засад інформаційної політики країни. *Наук. зап. Тернопіл. нац. пед. ун-ту ім. Володимира Гнатюка. Серія: Історія, 2*, 97–109. http://nbuv.gov.ua/UJRN/NZTNPU_ist_2019_2_13

Деякі питання оптимізації системи центральних органів виконавчої влади. Постанова Кабінету Міністрів України № 829 (2019) (Україна). https://zakon.rada.gov.ua/laws/show/829-2019-%D0%BF#Text

Доктрина про інформаційну безпеку України. Указ Президента України № 47/2017 (2017) (Україна). https://www.president.gov.ua/documents/472017-21374

Захаренко, К. В. (2021). *Інституційний вимір інформаційної безпеки України: трансформаційні виклики, глобальні контексти, стратегічні орієнтири*. (Автореф. дис. ... д-ра політ. наук, Львівський національний університет імені Івана Франка). https://lnu.edu.ua/wp-content/uploads/2021/04/aref_zakharenko.pdf

Ляшенко, О., & Дацків, І. (2015). Концептуальні засади формування інформаційної політики країни: світовий досвід. *Україна–Європа–Світ. Серія: Історія, міжнародні відносини, 15*, 211–224. http://nbuv.gov.ua/UJRN/Ues_2015_15_22

Морозова, В. О. (2014). Державна політика та стратегії США у сфері інформаційної безпеки в умовах глобальних викликів. *Науковий часопис НПУ імені М. П. Драгоманова. Серія 22: Політичні науки та методика викладання соціально-політичних дисциплін, спец. вип.*, 154–159. https://enpuir.npu.edu.ua/bitstream/handle/123456789/13746/Morozova.pdf? sequence=1&isAllowed=y

Мохова, Ю. Л., & Луцька, А. І. (2018). Сутність та головні напрямки державної інформаційної політики України. *Державне управління: удосконалення та розвиток*. http://www.dy.nayka.com.ua/pdf/12_2018/27.pdf

Негодченко, В. (2016). Основні напрями державної інформаційної політики в Україні. *Інформаційне право, 4*, 77–81.

Нестеряк, Ю. В. (2014). *Державна інформаційна політика України: теоретико-методологічні засади*. Київ: НАДУ.

Нестеряк, Ю. В. (2018). Становлення національного інформаційного простору України. *Вісник Національної академії державного управління при Президентові України. Серія: Державне управління, 1*, 11–17.

Ніщименко, О. А. (2016). Інформаційна безпека України на сучасному етапі розвитку держави і суспільства. *Наше право, 1*, 17–23.

Новицький, А. (2016). Щодо питання структуризації інформаційного права як наукової категорії. *Актуальні проблеми правознавства, 4*, 34–38.

Олійник, О. (2012a). Адміністративно-правові засади інформаційної безпеки. *Європейські перспективи, 4*(1), 65–68.

Олійник, О. В. (2012b). Інформаційна безпека США. *Боротьба з організованою злочинністю і корупцією (теорія і практика), 1*, 280–288.

Панова, І. В. (2014). Парадигма сучасного інформаційного права України. *Інформація і право, 3*(12), 31–40.

Пахнін, М. Л. (2014). Особливості державної інформаційної політики в розвинених країнах світу. *Теорія та практика державного управління, 4*, 414–422.

Положення про Міністерство цифрової трансформації. Постанова Кабінету Міністрів України. № 856 (2019) (Україна). https://zakon.rada.gov.ua/laws/show/856-2019-%D0%BF#n12

Про медіа. Закон України № 2849-IX (2022) (Україна). https://zakon.rada.gov.ua/laws/show/2849-20#Text

Проценко, Д., & Тупчієнко, Д. (2012). Огляд підходів до регулювання нових конвергентних аудіовізуальних засобів масової інформації: міжнародний досвід. *Національна рада України з питань телебачення і радіомовлення*. http://nrada.gov.ua/userfiles/file/2012/PDF/Brochure_ReviewOfRegulatoryApproaches.pdf

Разіцький, В. (2008). Інформаційна політика США в XX ст.: Становлення та розвиток. *Вісник Київського національного університету імені Тараса Шевченка. Історія, 94–95*, 48–51.

Сірий, С., & Турченко, Ю. (2012). Інформаційна політика України доби глобалізації: теоретичний аналіз. *Політичний менеджмент, 4–5*, 237–245.

Солодка, О. М. (2013). Сучасні тенденції міжнародної політики забезпечення інформаційної безпеки. *Інформаційна безпека людини, суспільства, держави, 3*, 25–29.

Терещенко, В. В. (2023). Особливості державної інформаційної політики в умовах війни. *Юридичний науковий електронний журнал, 2*, 391–395. http://www.lsej.org.ua/2_2023/92

Токар, О. (2009). Державна інформаційна політика: проблеми визначення концепту. *Політичний менеджмент, 5*, 131–141.

Фурашев, В. (2009). Інформаційні операції крізь призму системи моніторингу та інтеграції Інтернет-ресурсів. *Правова інформатика, 2*, 49–57.

Цимбалюк, В. С. & Бабінська, А. В. (2014). Правове регулювання інформаційної безпеки в Україні: проблеми теорії та практики. *Адміністративне право і процес, 2*(8), 22–30.

Braman, S. (2011). Defining information policy. *Journal of Information Policy, 1*, 1–5. https://www.academia.edu/2310219/Defining_Information_Policy

International Strategy for Cyberspace. (2011). White House. http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

Jaeger, P. T., Gorham, U., & Greene N. (2015, July). Teaching Information Policy in the Digital Age: Issues, Strategies, and Innovation. *J. of Education for Library and Information Science, 56*(3). (Summer). https://files.eric.ed.gov/fulltext/EJ1074656.pdf

McLuhan, M., & Parkerm, H. (1968). *Through the Vanishing Point: Space in Poetry and Painting*. N.Y.: Harper & Row.

Morze, N., & Veselovska, O. (2014). An analysis of information society development in Ukraine. *CeON Repository*. https://elibrary.kubg.edu.ua/id/eprint/6189/1/N_Morze_O_Veselovska_EICDDC_IS.pdf

Privacy Impact Assessment EINSTEIN Program. (2004). In *Collecting, Analyzing, and Sharing Computer Security Information Across the Federal Civilian Government. United States Computer Emergency Readiness Team (US-CERT)*. https://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_eisntein.pdf

Rzhevska, N., & Feshchenko, A. (2022). The peculiarities of Space State Information Policy. Language-Cultura-Politics. *International Jornal, 1*, 247–264. https://cejsh.icm.edu.pl/cejsh/element/bwmeta1.element.ojs-doi-10_54515_lcp_2022_1_247-264

The US Federal Budget Allocates 275 billion dollars for Cyber Security. (2024). https://hackyourmom.com/en/novyny/federalnyj-byudzhet-ssha-vydilyaye-275-mlrd-dolariv-na-kiberbezopasnist/

United nations development programme. Human Development Reports. (2022). *Human Development Report 2021–2022*. https://hdr.undp.org/en/indicators/52306

Weiner, S. A. (2013). Overview: The Role of Information Policy in Resolving Global Challenges. *Purdue Policy Research Institute Policy Briefs, 1*(1), Article 6. https://docs.lib.purdue.edu/gpripb/vol1/iss1/6/

References

Aristova, I. V. (2000). *Derzhavna informatsiina polityka: orhanizatsiino-pravovi aspekty* [State information policy: organizational and legal aspects]. (O. M. Bandurko, Red.). Kharkiv: Vyd-vo Un-tu vnutr. sprav [in Ukrainian].

Bondar, H., & Rakutina, L. (2020). Informatsiina polityka ta informatsiina bezpeka [Information policy and information security]. *Publichne upravlinnia ta mytne administruvannia,*

4(23), 42–49 [in Ukrainian].

Braman, S. (2011). Defining information policy. *Journal of Information Policy, 1*, 1–5. https://www.academia.edu/2310219/Defining_Information_Policy

Bryzhko, V. M. (2009). Pro suchasnu informatsiinu polityku [About modern information policy]. *Pravova informatyka, 2*(22), 31–43 [in Ukrainian].

Datskiv, I. (2019). Vplyv svitovoho dosvidu na formuvannia osnovnykh zasad informatsiinoi polityky krainy [The influence of world experience on the formation of the main principles of the country's information policy]. *Nauk. zap. Ternopil. nats. ped. un-tu im. Volodymyra Hnatiuka. Seriia: Istoriia, 2*, 97–109. http://nbuv.gov.ua/UJRN/NZTNPU_ist_2019_2_13 [in Ukrainian].

Deiaki pytannia optymizatsii systemy tsentralnykh orhaniv vykonavchoi vlady [Some issues of optimization of the system of central executive bodies]. Postanova Kabinetu Ministriv Ukrainy № 829 (2019) (Ukraina). https://zakon.rada.gov.ua/laws/show/829-2019-%D0%BF#Text [in Ukrainian].

Doktryna pro informatsiinu bezpeku Ukrainy [The doctrine of information security of Ukraine]. Ukaz Prezydenta Ukrainy № 47/2017 (2017) (Ukraina). https://www.president.gov.ua/documents/472017-21374 [in Ukrainian].

Furashev, V. (2009). Informatsiini operatsii kriz pryzmu systemy monitorynhu ta intehratsii Internet-resursiv [Information operations through the prism of the system of monitoring and integration of Internet resources]. *Pravova informatyka, 2*, 49–57 [in Ukrainian].

Holod, K. (2017). Informatsiina bezpeka SShA: suchasnyi stan ta uroky dlia Ukrainy [US information security: state of the art and lessons for Ukraine]. *Heopolityka Ukrainy: istoriia i suchasnist, 2*(19), 91–107 [in Ukrainian].

Holovanova, N. (2022). Informatsiina polityka Ukrainy v umovakh viiny (arkhetypnyi pidkhid) [Information policy of Ukraine in the conditions of war (archetypal approach)]. *Naukovi perspektyvy, 6*(24), 57–70. http://perspectives.pp.ua/index.php/np/article/view/1864 [in Ukrainian].

Horban, Yu. O. (2015). Informatsiina viina proty Ukrainy ta zasoby yii vedennia [Information war against Ukraine and means of its conduct]. *Visnyk Natsionalnoi akademii derzhavnoho upravlinnia pry Prezydentovi Ukrainy, 1*, 136–141 [in Ukrainian].

International Strategy for Cyberspace. (2011). White House. http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

Jaeger, P. T., Gorham, U., & Greene N. (2015, July). Teaching Information Policy in the Digital Age: Issues, Strategies, and Innovation. *J. of Education for Library and Information Science, 56*(3). (Summer). https://files.eric.ed.gov/fulltext/EJ1074656.pdf

Liashenko, O., & Datskiv, I. (2015). Kontseptualni zasady formuvannia informatsiinoi polityky krainy: svitovyi dosvid [Conceptual foundations of the formation of the country's information policy: world experience]. *Ukraina–Ievropa–Svit. Seriia: Istoriia, mizhnarodni vidnosyny, 15*, 211–224. http://nbuv.gov.ua/UJRN/Ues_2015_15_22 [in Ukrainian].

McLuhan, M., & Parkerm, H. (1968). *Through the Vanishing Point: Space in Poetry and Painting*. N.Y.: Harper & Row.

Mokhova, Yu. L., & Lutska, A. I. (2018). Sutnist ta holovni napriamky derzhavnoi informatsiinoi polityky Ukrainy [The essence and main directions of the state information policy of Ukraine]. *Derzhavne upravlinnia: udoskonalennia ta rozvytok*. http://www.dy.nayka.com.ua/pdf/12_2018/27.pdf [in Ukrainian].

Morozova, V. O. (2014). Derzhavna polityka ta stratehii SShA u sferi informatsiinoi bezpeky v umovakh hlobalnykh vyklykiv [US public policy and strategies in the field of information security in the face of global challenges]. *Naukovyi chasopys NPU imeni M. P. Drahomanova. Seriia 22: Politychni nauky ta metodyka vykladannia sotsialno-politychnykh dystsyplin, spets. vyp*., 154–159. https://enpuir.npu.edu.ua/bitstream/handle/123456789/13746/Morozova.pdf?sequence=1&isAllowed=y [in Ukrainian].

Morze, N., & Veselovska, O. (2014). An analysis of information society development in Ukraine. *CeON Repository*. https://elibrary.kubg.edu.ua/id/eprint/6189/1/N_Morze_O_Veselovska_EICDDC_IS.pdf

Nehodchenko, V. (2016). Osnovni napriamy derzhavnoi informatsiinoi polityky v Ukraini [The main directions of the state information policy in Ukraine]. *Informatsiine pravo, 4*, 77–81 [in Ukrainian].

Nesteriak, Yu. V. (2014). *Derzhavna informatsiina polityka Ukrainy: teoretyko-metodolohichni zasady* [The main directions of the state information policy in Ukraine]. Kyiv: NADU [in Ukrainian].

Nesteriak, Yu. V. (2018). Stanovlennia natsionalnoho informatsiinoho prostoru Ukrainy [Formation of the national information space of Ukraine]. *Visnyk Natsionalnoi akademii derzhavnoho upravlinnia pry Prezydentovi Ukrainy. Seriia: Derzhavne upravlinnia, 1*, 11–17 [in Ukrainian].

Nishchymenko, O. A. (2016). Informatsiina bezpeka Ukrainy na suchasnomu etapi rozvytku derzhavy i suspilstva [Information security of Ukraine at the current stage of development of the state and society]. *Nashe pravo, 1*, 17–23 [in Ukrainian].

Novytskyi, A. (2016). Shchodo pytannia strukturyzatsii informatsiinoho prava yak naukovoi katehorii [Regarding the issue of structuring information law as a scientific category]. *Aktualni problemy pravoznavstva, 4*, 34–38 [in Ukrainian].

Oliinyk, O. (2012a). Administratyvno-pravovi zasady informatsiinoi bezpeky [Administrative and legal principles of information security]. *Yevropeiski perspektyvy, 4*(1), 65–68 [in Ukrainian].

Oliinyk, O. V. (2012b). Informatsiina bezpeka SShA [US Information Security]. *Borotba z orhanizovanoiu zlochynnistiu i koruptsiieiu (teoriia i praktyka), 1*, 280–288 [in Ukrainian].

Pakhnin, M. L. (2014). Osoblyvosti derzhavnoi informatsiinoi polityky v rozvynenykh krainakh svitu [Peculiarities of state information policy in developed countries of the world]. *Teoriia ta praktyka derzhavnoho upravlinnia, 4*, 414–422 [in Ukrainian].

Panova, I. V. (2014). Paradyhma suchasnoho informatsiinoho prava Ukrainy [Paradigm of modern information law of Ukraine]. *Informatsiia i pravo, 3*(12), 31–40 [in Ukrainian].

Polozhennia pro Ministerstvo tsyfrovoi transformatsii [Regulations on the Ministry of Digital Transformation]. Postanova Kabinetu Ministriv Ukrainy № 856 (2019) (Ukraina). https://zakon.rada.gov.ua/laws/show/856-2019-%D0%BF#n12 [in Ukrainian].

Privacy Impact Assessment EINSTEIN Program. (2004). In *Collecting, Analyzing, and Sharing Computer Security Information Across the Federal Civilian Government. United States Computer Emergency Readiness Team (US-CERT)*. https://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_eisntein.pdf

Pro media [About media]. Zakon Ukrainy № 2849-IX (2022) (Ukraina). https://zakon.rada.gov.ua/laws/show/2849-20#Text [in Ukrainian].

Protsenko, D., & Tupchiienko D. (2012). Ohliad pidkhodiv do rehuliuvannia novykh konverhentnykh audiovizualnykh zasobiv masovoi informatsii: mizhnarodnyi

dosvid [Review of approaches to the regulation of new convergent audiovisual media: international experience]. *Natsionalna rada Ukrainy z pytan telebachennia i radiomovlennia.* http://nrada.gov.ua/userfiles/file/2012/PDF/Brochure_ReviewOfRegulatoryApproaches.pdf [in Ukrainian].

Razitskyi, V. (2008). Informatsiina polityka SShA v XX st.: Stanovlennia ta rozvytok [The information policy of the USA in the 20th century: Formation and development]. *Visnyk Kyivskoho natsionalnoho universytetu imeni Tarasa Shevchenka. Istoriia, 94–95*, 48–51 [in Ukrainian].

Rzhevska, N., & Feshchenko, A. (2022). The peculiarities of Space State Information Policy. Language-Cultura-Politics. *International Jornal, 1*, 247–264. https://cejsh.icm.edu.pl/cejsh/element/bwmeta1.element.ojs-doi-10_54515_lcp_2022_1_247-264

Siryŭ, S., & Turchenko, Yu. (2012). Informatsiina polityka Ukrainy doby hlobalizatsii: teoretychnyi analiz [Information policy of Ukraine in the age of globalization: theoretical analysis]. *Politychnyi menedzhment, 4–5*, 237–245 [in Ukrainian].

Solodka, O. M. (2013). Suchasni tendentsii mizhnarodnoi polityky zabezpechennia informatsiinoi bezpeky [Modern trends in the international policy of ensuring information security]. *Informatsiina bezpeka liudyny, suspilstva, derzhavy, 3*, 25–29 [in Ukrainian].

Tereshchenko, V. V. (2023). Osoblyvosti derzhavnoi informatsiinoi polityky v umovakh viiny [Peculiarities of state information policy in conditions of war]. *Yurydychnyi naukovyi elektronnyi zhurnal, 2*, 391–395. http://www.lsej.org.ua/2_2023/92 [in Ukrainian].

The US Federal Budget Allocates 275 billion dollars for Cyber Security. (2024). https://hackyourmom.com/en/novyny/federalnyj-byudzhet-ssha-vydilyaye-275-mlrd-dolariv-na-kiberbezopasnist/

Tokar, O. (2009). Derzhavna informatsiina polityka: problemy vyznachennia kontseptu [State information policy: problems of defining the concept]. *Politychnyi menedzhment, 5*, 131–141 [in Ukrainian].

Tsymbaliuk, V. S., & Babinska, A. V. (2014). Pravove rehuliuvannia informatsiinoi bezpeky v Ukraini: problemy teorii ta praktyky [Legal regulation of information security in Ukraine: problems of theory and practice]. *Administratyvne pravo i protses, 2*(8), 22–30 [in Ukrainian].

United nations development programme. Human Development Reports. (2022). *Human Development Report 2021–2022*. https://hdr.undp.org/en/indicators/52306

Weiner, S. A. (2013). Overview: The Role of Information Policy in Resolving Global Challenges. *Purdue Policy Research Institute Policy Briefs, 1*(1), Article 6. https://docs.lib.purdue.edu/gpripb/vol1/iss1/6/

Zakharenko, K. V. (2021). Instytutsiinyi vymir informatsiinoi bezpeky Ukrainy: transformatsiini vyklyky, hlobalni konteksty, stratehichni oriientyry [Institutional dimension of information security of Ukraine: transformational challenges, global contexts, strategic orientations]. (Avtoref. dys. d-ra polit. nauk, Lvivskyi natsionalnyi universytet imeni Ivana Franka). https://lnu.edu.ua/wp-content/uploads/2021/04/aref_zakharenko.pdf [in Ukrainian].

Стаття надійшла до редакції 10.03.2024