SOCIAL AND BEHAVIORAL SCIENCES

DOI https://doi.org/10.51647/kelm.2022.4.30

INSTYTUCJONALNY WYMIAR BEZPIECZEŃSTWA INFORMACYJNEGO PAŃSTWA W WARUNKACH WSPÓŁCZESNYCH TRENDÓW GLOBALIZACYJNYCH

Svitlana Vnuchko
kandydat nauk politycznych, docent Katedry Nauk Politycznych
Kijowskiego Uniwersytetu Narodowego imienia Tarasa Szewczenki (Kijów, Ukraina)
ORCID ID: 0000-0001-9176-1304
vnuchko@ukr.net

Olena Polovko
kandydat nauk politycznych, docent Katedry Nauk Politycznych
Kijowskiego Uniwersytetu Narodowego imienia Tarasa Szewczenki (Kijów, Ukraina)
ORCID ID: 0000-0002-1207-7174
alena.polovko@gmail.com

Adnotacja. W artykule omówiono cechy instytucjonalnego pomiaru bezpieczeństwa informacji państwa w warunkach współczesnych trendów globalizacyjnych. Koncentruje się na kwestiach rozwoju sfery informacyjnej społeczeństwa i powstawania nowych zagrożeń dla bezpieczeństwa informacyjnego państwa w ramach realizacji zadań polityki wewnętrznej i zagranicznej państwa, zwłaszcza w warunkach wojny hybrydowej. Badane są cechy systemu ochrony bezpieczeństwa narodowego w sektorze przeciwdziałania ekspansji informacji. Badana jest rola bezpieczeństwa informacji Ukrainy jako jednej z kluczowych we współczesnej walce o własną niepodległość. W rezultacie należy zauważyć, że w celu zmniejszenia skutków ataków informacyjnych, państwowa polityka informacyjna powinna opierać się na zapewnieniu prawa do rzetelnej, kompletnej i terminowej informacji, wolności słowa i działalności informacyjnej, zapobieganiu ingerencji w treść i wewnętrzną organizację procesów informacyjnych; zachowaniu i poprawie krajowego produktu i technologii informacyjnych, zapewnieniu informacji i identyfikacji narodowo-kulturowej Ukrainy w światowej przestrzeni informacyjnej.

Słowa kluczowe: bezpieczeństwo informacji, przestrzeń informacyjna, wpływy informacyjne, zagrożenia zewnętrzne, globalizacja, sieci społecznościowe, polityka państwa.

INSTITUTIONAL DIMENSION OF STATE INFORMATION SECURITY IN THE CONDITIONS OF CURRENT GLOBALIZATION TRENDS

Svitlana Vnuchko
Candidate of Political Science,
Associate Professor at the Department of Political Sciences
Taras Shevchenko National University of Kyiv (Kyiv, Ukraine)
ORCID ID: 0000-0001-9176-1304
vnuchko@ukr.net

Olena Polovko
Candidate of Political Science,
Associate Professor at the Department of Political Sciences
Taras Shevchenko National University of Kyiv (Kyiv, Ukraine)
ORCID ID: 0000-0002-1207-7174
alena.polovko@gmail.com

Abstract. The article examines the peculiarities of the institutional dimension of state information security in the context of current globalization trends. Attention is focused on the issues of the development of the information sphere of society and the emergence of new threats to state information security within the framework of the implementation of the tasks of the state's internal and foreign policy, especially in the context of hybrid war. Peculiarities of the national security protection system in the sector of countering information expansion are being studied. The role of state information security is studied as one of the key factors in the current struggle for one's own independence. In conclusion, it is noted that in order to reduce the consequences of information attacks, the state information policy should be based on ensuring the right to reliable, complete and timely information, freedom of speech and information

activities, prevention of interference in the content and internal organization of information processes; preservation and improvement of the domestic national information product and technologies, provision of information and national-cultural identification of Ukraine in the world information space.

Key words: informative safety, informative space, informative influences, external threats, globalization, social networks, state policy.

ІНСТИТУЦІЙНИЙ ВИМІР ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ В УМОВАХ ГЛОБАЛІЗАЦІЙНИХ ТЕНДЕНЦІЙ СУЧАСНОСТІ

Світлана Внучко
кандидат політичних наук, доцент кафедри політології
Київського національного університету імені Тараса Шевченка (Київ, Україна)
ORCID ID: 0000-0001-9176-1304
vnuchko@ukr.net

Олена Половко
кандидат політичних наук, доцент кафедри політології
Київського національного університету імені Тараса Шевченка (Київ, Україна)
ORCID ID: 0000-0002-1207-7174
alena.polovko@gmail.com

Анотація. У статті розглядаються особливості інституційного виміру інформаційної безпеки держави в умовах глобалізаційних тенденцій сучасності. Акцентується увага на питаннях розвитку інформаційної сфери суспільства та виникнення нових загроз для інформаційної безпеки держави в рамках реалізації завдань внутрішньої і зовнішньої політики держави, особливо в умова гібридної війни. Досліджуються особливості системи захисту національної безпеки в секторі протидії інформаційній експансії. Вивчається роль інформаційної безпеки України як однієї з ключових у сучасній боротьбі за власну незалежність. У підсумку відмічається, що для зменшення наслідків інформаційних атак, державна інформаційна політика повинна базуватись на забезпеченні права на достовірну, повну та своєчасну інформацію, свободу слова та інформаційну діяльність, недопущення втручання в зміст та внутрішню організацію інформаційних процесів; збереженні та вдосконаленні вітчизняного національного інформаційного продукту та технологій, забезпеченні інформаційної та національно-культурної ідентифікації України у світовому інформаційному просторі.

Ключові слова: інформаційна безпека, інформаційний простір, інформаційні впливи, зовнішні загрози, глобалізація, соціальні мережі, політика держави.

Вступ. XXI століття знаменувалося шаленим розвитком інформаційних систем. Інформація в сучасному світі активно впливає на всі сфери життєдіяльності не лише окремих індивідів та держав, але і всього світового співтовариства. Жодна сфера життя не може функціонувати без розвинутої інформаційної структури. Проникаючи в усі сфери діяльності держави, інформація здобуває конкретне політичне, матеріальне і вартісне вираження.

Інформаційна безпека й відповідна політика держави в цій сфері набувають усе більш глобального характеру. Процеси інформаційної глобалізації дуже гостро дали про себе знати й, крім позитивних елементів, поставили перед державами та суспільством серйозні виклики щодо готовності протидії негативним складовим інформаційного розвитку, до яких світова спільнота виявилася неготовою. Сьогодні необхідність забезпечення інформаційної безпеки держави відіграє важливу роль в функціонування політичної системи кожної країни. Адже в епоху інформаційних війн цінність інформації зростає в багато разів. Інформація стала вже не тільки товаром, а й інструментом тиску, маніпуляції суспільством, громадською думкою.

Глобальні соціальні мережі стали чи не головним інструментом розвитку сучасних засобів інтелектуального спілкування та пізнання, що робить Інтернет новим складним об'єктом інформаційного впливу на суспільство та видозмінили комунікативні технології спеціального впливу на особистість. Звіт Digital 2022 Global Statshot від DataReportal демонструє, що понад 5 млрд людей у всьому світі користуються Інтернетом, а 63 % всього населення світу майже постійно перебуває онлайн. При цьому лише за останній рік їх загальна кількість зросла майже на 200 млн осіб. Крім того, 5,32 млрд людей у всьому світі користуються мобільними телефонами, це 67 % населення планети; 4 з 5 мобільних телефонів – смартфони. У всьому світі сьогодні 4,65 млрд користувачів соціальних мереж, це 58,7 % всього населення планети (Digital Global Statshot Report, 2022).

Сучасними Інтернет-технологіями відпрацьовані й апробовані ефективні методи інформаційних впливів на особистість. Інформаційна сфера перетворюється в арену міжнародного суперництва та створює небезпеку для національних інтересів. Випадки міжнародного інформаційного тероризму й інформаційних воєн стали геополітичною реальністю.

Ефективно протистояти інформаційним загрозам у сучасних умовах може лише добре організована державна система забезпечення інформаційної безпеки, що повинна здійснюватися при повній взаємодії всіх державних органів, недержавних структур і громадян. Таким чином, питання інформаційної

безпеки держави в умовах глобалізаційних тенденцій сучасності надзвичайно актуальні й потребують поглибленого вивчення.

Інформаційну безпеку, проблеми захисту національного інформаційного простору досліджували багато науковців. Так, поняття «інформаційної безпеки держави» розглядають Зернецька О., Кормич Б., Ліпкан В., Марущак А., Петрик В., Резнікова О., Сащук Г. та ін. Вивченням ролі держави у формуванні інформаційного суспільства займаються такі вчені як Арістова І., Почепцов Г. та ін. Супрун В., Ярочкін В. досліджують питання основних принципів забезпечення інформаційної безпеки. Однак, поза увагою науковців залишились проблеми чіткого окреслення джерел інформаційних загроз, визначення та обґрунтування методів протидії інформаційно-психологічним негативним впливам. Окремого дослідження також потребують інституційні виміри процесу гарантування інформаційної безпеки держави.

Мета статті полягає в проведенні аналізу глобалізаційних тенденцій інформаційної безпеки в сучасному суспільстві, окресленні джерел загроз інтересам держави та виокремленні інструментів протидії інформаційним загрозам.

Основна частина. Протягом тривалого часу інформаційну безпеку здебільшого визначали через комп'ютерну безпеку, вказуючи на необхідність захисту величезних обсягів інформації, яка стосується державних таємниць, особистих даних громадян тощо та містяться на електронних носіях. Бажання отримати доступ до такої інформації призвело до поширення таких явищ як хакерські атаки, інформаційні диверсії тощо. Інформаційна інфраструктура країн і національних інформаційних ресурсів виявилися досить уразливими об'єктами впливу з боку іноземних держав та терористичних організацій.

Сьогодні поняття інформаційної безпеки, залежно від його використання, можна розглядати у двох ракурсах. У найзагальнішому випадку, інформаційна безпека визначається як стан захищеності інформаційного середовища суспільства, який забезпечує його формування, використання і розвиток в інтересах громадян, організацій, держави.

Більш розгорнуте формулювання інформаційної безпеки – це стан захищеності потреб в інформації особистості, суспільства і держави, при якому забезпечується їхнє існування і прогресивний розвиток незалежно від наявності внутрішніх і зовнішніх інформаційних загроз. Саме розгорнуте визначення інформаційної безпеки найбільш повно відображає ключові аспекти поняття в умовах сучасних глобалізаційних тенденцій.

Організація діяльності держави у питаннях гарантування інформаційної безпеки – це послідовний безперервний процес, спрямований на розробку і здійснення правових, організаційних, технічних та інших заходів у цій сфері. Наразі Україна переживає нелегкий період у забезпеченні інформаційної безпеки, проходячи через купу загроз, пов'язаних із гібридною війною, де вміло використовуються прийоми дезінформації та поширюються фейкові новини з метою дестабілізації ситуації в країні. Інформаційне вторгнення, маніпуляції, застосування соціально-психологічного впливу є серйозною загрозою як головним засадам демократичного суспільства, так і особистій інформаційно-психологічній безпеці громадян, у тому числі – загрозою є застосування "fake news" з метою політичного впливу та здійснення політичних завдань (Невельська-Гордєєва, 2022: 124).

В умовах російсько-української війни спроба росії зруйнувати інформаційну безпеку України напряму пов'язана з загрозою національній безпеці – це намагання росії вплинути на інформаційну інфраструктуру України, інформаційні ресурси, на суспільство, свідомість, підсвідомість особистості, з метою нав'язати українцям бажану (для росії) систему цінностей, поглядів, інтересів і рішень у життєво важливих сферах суспільної й державної діяльності, керувати їхньою поведінкою і розвитком у бажаному для росії напрямку.

Інформаційна складова гібридної війни росії проти України поставила на порядок денний питання забезпечення та посилення захисту національного інформаційного продукту, в тому числі боротьбу з фейками, використання маніпулятивних технологій в соціальних мережах, запровадження адміністративних обмежень транслювання на українській території програм іноземних (російських) теле- і радіоканалів та поширення іншої мас-медійної продукції, яка дестабілізує суспільну ситуацію в Україні і формує загрози національній безпеці.

Маніпулятивні технології на службі у гібридної інформаційної війни росії проти України: нагнітання психологічного шоку, ефект первинності (удар на випередження), ефект присутності (трюки, покликані імітувати реальність у «репортажах з місць боїв») розпочали активно застосовуватись ще з 2014 року на Донбасі, а з лютого 2022 р. поширились не лише на всю територію України, а й вийшли на міжнародний рівень.

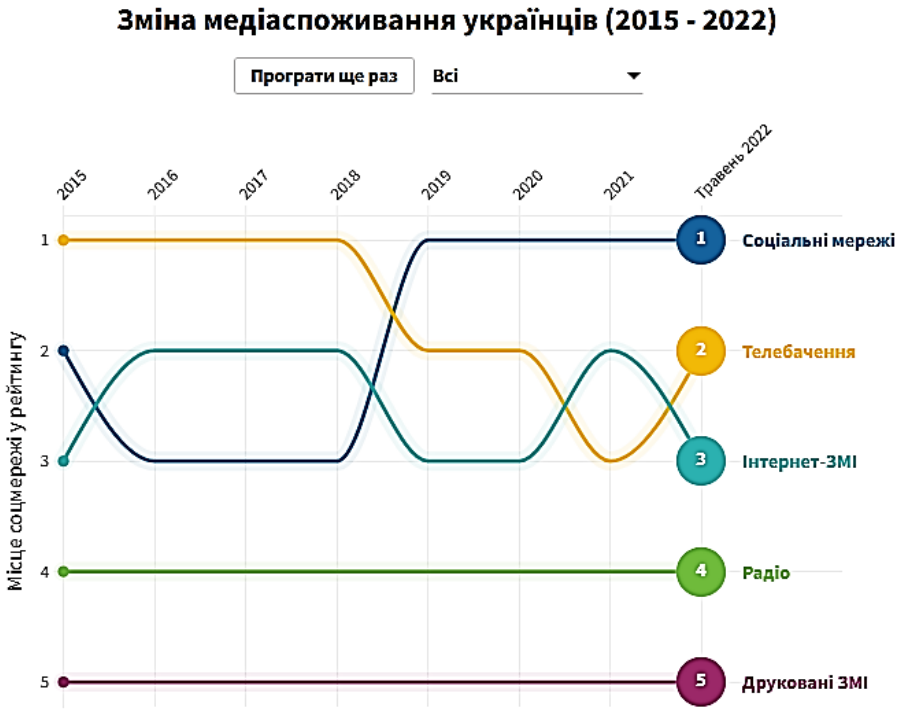
Однією з найбільш поширених технологій «інформаційної обробки» населення став прийом, який застосовує російські телеканали – організація виступів свідків подій на підготовленому підґрунті та тиражування центральним телебаченням потрібної версії. Підтвердженням цього є чисельні приклади відео репортажів російських телеканалів з тимчасово окупованих територій України, на яких лунають гасла в підтримку так званого «руського міра».

Серед інших прийомів, які часто застосовуються, варто відмітити такий прийом як «підтасовування фактів». За допомогою підтасовки фактів, поширення чуток створюється штучна атмосфера: нагнітання паніки та страху серед українців (в інформаційних повідомлення щодо можливих ракетних обстрілів, ядерних загроз тощо) та «спокою і впевненості росіян» (щодо приховування реальних наслідків затоплення крейсера «Москва», вибухів в Новофедоровці тощо). В арсеналі «агентів інформаційно-комунікативного впливу» є окремі представники журналістської спільноти та навіть цілі організації, від імені яких поширюються

неправдиві та неперевірені свідчення про «злочини» українських військових (як приклад можна навести нещодавні скандальні відео сюжет телеканалу CBS та звіт правозахисної організації Amnesty International).

За умов широкомасштабного використання ворогом маніпулятивного інструментарію інформаційного суспільства, необхідність гарантування інформаційної безпеки визначається, по-перше, потребою забезпечення національної безпеки України в цілому, по-друге, існуванням таких загроз інформаційній сфері країни, які можуть завдавати значної шкоди загальним національним інтересам, по-третє, врахуванням того, що за допомогою інформації можна впливати на зміну свідомості і поведінку людей (Бондаренко В., 1999: 129). Завдання інформаційної безпеки держави – створення системи протидії інформаційним загрозам та захист власного інформаційного простору, інформаційної інфраструктури, інформаційних ресурсів держави. Підтвердженням цього виступають дані корпорації Microsoft, відповідно до яких більшість хакерських атак (46 %) протягом 2020–2021 років спрямовувалися проти США. Україна перебуває на 2 місці в списку – 19 %, на третьому Велика Британія – 9 %. Найбільше хакерських атак – 58 % – зафіксовано з рф, 23 % – із Північної Кореї, 11 % – з Ірану. При цьому російські хакери почали частіше зламувати урядові організації: кількість таких злочинів збільшилася з 3 % до 53 % (Microsoft Digital Defense Report, 2021). Від 24 лютого працівниками кіберполіції України було знешкоджено понад 300 ворожих атак на етапі їхньої підготовки, ще 83 атаки фахівці кіберполіції відбили у співпраці з іншими правоохоронними органами (Офіційний сайт Національної поліції України, 2022).

Повномасштабне вторгнення рф в Україну призвело до різкого зростання використання соціальних мереж як джерела новин. Найпопулярнішим джерелом інформації за травень-червень 2022 р. виявилися соціальні мережі: ними для отримання новин користуються 76,6 % українців (серед них 66 % обирають Telegram, 61 % – YouTube, 58 % – Facebook). На другому місці – телебачення з 66,7 % голосів. Третє місце взяв інтернет (за винятком соцмереж) – 61,2 % користувачів. Радіо наразі слухають близько 28,4 % громадян України, а друковані ЗМІ читають лише 15,7 % опитаних (Снопок О., 2022). Це свідчить про зростання потреби в більш оперативних джерелах інформації, однак призводить до того, що споживання дезінформації також зростає. За даними щорічного опитування USAID-Internews щодо споживання медіа лише 3 % людей в Україні можуть розпізнати брехню в новинах (Результати опитування USAID-Internews, 2021). Якщо говорити про українську молодь віком 15–19 років, то, за даними молодіжного опитування U-Report, лише 14 % завжди перевіряють інформацію (U-Report, 2020).



Джерело: Громадянська мережа ОПОРА, USAID-Internews (Снопок О., 2022)

Важливим елементом, який потрібно враховувати при дослідженні особливостей використання соціальних мереж є явище інформаційної бульбашки – це інтелектуальна ізоляція, спричинена персональним підбором інформації для користувачів за допомогою алгоритмів цифрових платформ. Зі стрічки новин залишається все, на що конкретна людина активно реагує (особливо негативно), і, навпаки, зникає все, що суперечить її інтересам та поглядам. У результаті користувач не бачить ширшої реальності. Таким чином соціальні мережі головним чином надають користувачу інформацію, яка найбільшою мірою відповідає його вподобанням, випускаючи з поля зору інформацію, яка суперечить його вподобанням, проте могла би потенційно розширити його світогляд, зробити більш толерантними до інших точок зору чи навіть спонукати змінити думку про щось, вказати на іншу логіку подій чи процесів.

Таким чином, нова соціальна реальність забезпечила сприятливі умови для швидкого та широкомасштабного поширення як необхідної і важливої так і завідома неправдивої й маніпулятивної інформації, спотвореної зумисно заради певних економічних, політичних або інших вигод. За таких умов інформаційна гігієна – фільтрація потоку отримуваної інформації, що допомагає не засмічувати голову фейками, протистояти шахрайству та не робити непотрібних помилок у момент паніки – набуває особливої актуальності.

Превентивні заходи та швидка адаптація до умов реальної ситуації на рівні державних інститутів значною мірою сприяють забезпечення інформаційної безпеки. Так, ще 28 грудня 2021 року Президент України Володимир Зеленський увів у дію рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки», яка спрямована на посилення можливості держави щодо забезпечення власної інформбезпеки, захисту інформаційного простору. Основною загрозою безпеці України в цьому документі називається росія і проведена нею інформаційна політика. «Застосовані Російською Федерацією технології гібридної війни проти України, у тому числі моделі і механізми інформаційного втручання, поширюються на інші держави, швидко адаптуючись до локальних контекстів та регуляторних політик. Обмежувальні заходи (санкції) та ефективний механізм моніторингу і відповідальності за їх порушення є одним із дієвих механізмів відповіді на дезінформаційну активність Російської Федерації як держави-агресора», – сказано в документі. В документі також досить повно визначені глобальні та національні виклики і загрози інформаційній безпеці України: збільшення кількості глобальних дезінформаційних кампаній; соціальні мережі як суб'єкти впливу в інформаційному просторі; недостатній рівень медіаграмотності (медіакультури) в умовах стрімкого розвитку цифрових технологій; інформаційне домінування Російської Федерації як держави-агресора на тимчасово окупованих територіях України, несформованість системи стратегічних комунікацій тощо та представлені основні стратегії протидії їм (Указ Президента України, 2021).

За ініціативи Міністерства культури та інформаційної політики України 16 лютого 2022 року було проведено телемарафон на всіх телеканалах України на тему єднання, створено єдину інформаційну платформу стратегічної комунікації «UA разом» (в подальшому телемарафон «Єдині новини»). З моменту уведення воєнного стану в Україні 24 лютого 2022 року, телеканали «UA: Перший», «Рада», «1+1», «ICTV», «Інтер» й «Україна 24» відразу об'єдналися і позмінно проводять трансляцію, не зважаючи на воєнні дії, перебуваючи в студії, чи в бомбосховищах. Таким чином українська влада намагалася пристосувати інформаційне поле до умов воєнного часу, а також розширити кількість офіційних каналів комунікації, створюючи офіційні профілі органів влади у Telegram, YouTube та інших соціальних мережах.

В липні 2022 року Міністр культури та інформаційної політики України додатково ініціював створення єдиної позиції України до світових техплатформ із протидії дезінформації та фейкам. Міністерство культури та інформаційної політики України разом з Центром стратегічних комунікацій та інформаційної безпеки пропонує державним органам та громадським організаціям просувати «єдину позицію» в частині інформаційної безпеки під час взаємодії з соціальними мережами та платформами США. Зокрема, мова йде про так званий Big Tech – Google, Amazon, Microsoft, Apple, Meta (Facebook та Instagram), Twitter, Linkedin, YouTube, Telegram (Офіційний сайт Міністерства культури та інформаційної політики України, 2022).

Висновки. Сьогодні український інформаційний простір зазнає безпрецедентного впливу. Україна зіткнулася зі спробами системного нагнітання паніки, поширенням фейкової інформації та викривленням реального стану речей. Усе це в комплексі – ніщо інше як чергова потужна хвиля гібридної війни росії проти України. Водночас ми чудово розуміємо мотиви нинішнього інформаційного нагнітання – посіяти тривогу в українському суспільстві, підірвати віру в здатність держави захистити своїх громадян, розхитати нашу єдність.

Зважаючи на постійну інформаційну боротьбу, для забезпечення своєї незалежності Україні необхідно і далі удосконалювати та розвивати як правові засади (в тому числі й міжнародні), так і структурну й технічну складову інформаційної безпеки.

Україні потрібно продовжувати процес побудови системи стратегічних комунікацій. Державна політика з забезпечення інформаційної безпеки повинна і надалі бути направлена на здійснення низки організаційних та практичних заходів зі зміцнення власної інституційної спроможності у сфері стратегічних комунікацій, створення дієвого механізму координації і взаємодії між усіма органами державної влади, залученими до здійснення заходів із протидії загрозам в інформаційній сфері, об'єднання всіх ключових суб'єктів у сфері інформаційних відносин, суб'єктів формування і реалізації державної політики щодо ефективного захисту національного інформаційного простору, реалізації цілей захисту національної безпеки України в інформаційній сфері. Також варто враховувати, що реалізація державою стратегії інформаційної безпеки повинна бути направлення не лише на державні інституції, а й враховувати комплекс заходів спрямованих на підвищення рівня медіа грамотності українців, рівня інформаційної гігієни та безпеки людини в соціальних мережах.

Список використаних джерел:

1. Бондаренко В. О., Литвиненко О. В. Інформаційна безпека сучасної держави: концептуальні роздуми. *Стратегічна панорама*. – 1999. – № 1–2. – С. 127–133.
2. Microsoft Digital Defense Report. Russian cyberattacks pose greater risk to governments and other insights from our annual report, 2021. URL: https://blogs.microsoft.com/on-the-issues/2021/10/07/digital-defense-report-2021/
3. Невельська-Гордєєва О. П., Нечитайло В. О. Феномен "fake news" у контексті забезпечення інформаційної безпеки держави. *Вісник Національного юридичного університету імені Ярослава Мудрого*. 2022. № 1 (52). С. 123–135. DOI: 10.21564/2663-5704.52.250655

4. Офіційний сайт Міністерства культури та інформаційної політики України. Олександр Ткаченко ініціює створення єдиної позиції України до світових техплатформ із протидії дезінформації та фейкам. 19.07.2022 р. URL: https://www.kmu.gov.ua/news/oleksandr-tkachenko-initsiiuie-stvorennia-iedynoi-pozytsii-ukrainy-do-svitovykh-tekhplatform-iz-protydii-dezinformatsii-ta-feikam
5. Офіційний сайт Національної поліції України. Брифінг в Медіацентрі Україна – Укрінформ 10.08.2022. URL: https://www.npu.gov.ua/news/kiberzlochini/Iz-pochatku-povnomasshtabnogo-vijskovogo-vtorgnennya-rf-kiberpolicziya-poperedila-ponad-300-kiberatak-na-ukrajinski-resursi/
6. Ставлення населення до медіа та споживання різних типів медіа 2021. *Результати опитування USAID-Internews.* URL: https://www.ukrinform.ua/rubric-presshall/3349746-opituvanna-usaidinternews-sodo-spozivanna-media.html/
7. Снопок О. Дивимося, читаємо, слухаємо: як змінилося медіаспоживання українців в умовах повномасштабної війни (22.06.2022). URL: https://www.pravda.com.ua/columns/2022/06/22/7353987/
8. Указ Президента України № 685/2021 від 28.11.2021 р. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки». URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text
9. Digital 2022 July Global Statshot Report. Datareportal. URL: https://ain.ua/2022/04/30/zvit-digital-2022/
10. U-Report. Your voice matters. URL: https://ukraine.ureport.in/opinion/4025

References:

1. Bondarenko, V. O., Lytvynenko, O. V. Informatsiina bezpeka suchasnoi derzhavy: kontseptualni rozdumy [Information security of the modern state: conceptual reflections]. *Stratehichna panorama*. – 1999. – № 1–2. – S. 127–133. [in Ukrainian]
2. Microsoft Digital Defense Report. Russian cyberattacks pose greater risk to governments and other insights from our annual report, 2021. URL: https://blogs.microsoft.com/on-the-issues/2021/10/07/digital-defense-report-2021/
3. Nevelska-Hordieieva, O. P., Nechytailo, V. O. Fenomen "fake news" u konteksti zabezpechennia informatsiinoi bezpeky derzhavy ["Fake news" phenomenon in context ensuring information security of the state]. *Visnyk Natsionalnoho yurydychnoho universytetu imeni Yaroslava Mudroho*. 2022. № 1 (52). S. 123–135. DOI: 10.21564/2663-5704.52.250655 [in Ukrainian]
4. Ofitsiinyi sait Ministerstva kultury ta informatsiinoi polityky Ukrainy [Official website of the Ministry of Culture and Information Policy of Ukraine]. Oleksandr Tkachenko initsiiuie stvorennia yedynoi pozytsii Ukrainy do svitovykh tekhplatform iz protydii dezinformatsii ta feikam. 19.07.2022 r. URL: https://www.kmu.gov.ua/news/oleksandr-tkachenko-initsiiuie-stvorennia-iedynoi-pozytsii-ukrainy-do-svitovykh-tekhplatform-iz-protydii-dezinformatsii-ta-feikam [in Ukrainian]
5. Ofitsiinyi sait Natsionalnoi politsii Ukrainy [Official website of the National Police of Ukraine]. Bryfinh v Mediatsentri Ukraina – Ukrinform 10.08.2022. URL: https://www.npu.gov.ua/news/kiberzlochini/Iz-pochatku-povnomasshtabnogo-vijskovogo-vtorgnennya-rf-kiberpolicziya-poperedila-ponad-300-kiberatak-na-ukrajinski-resursi/ [in Ukrainian]
6. Stavlennia naselennia do media ta spozhyvannia riznykh typiv media 2021. [Public attitudes towards media and consumption of different types of media 2021]. *Rezultaty opytuvannia USAID-Internews.* URL: https://www.ukrinform.ua/rubric-presshall/3349746-opituvanna-usaidinternews-sodo-spozivanna-media.html/ [in Ukrainian]
7. Snopok, O. Dyvymosia, chytaiemo, slukhaiemo: yak zminylosia mediaspozhyvannia ukraintsiv v umovakh povnomasshtabnoi viiny (22.06.2022) [We watch, read, listen: how the media consumption of Ukrainians has changed in the conditions of a full-scale war]. URL: https://www.pravda.com.ua/columns/2022/06/22/7353987/ [in Ukrainian]
8. Ukaz Prezydenta Ukrainy № 685/2021 vid 28.11.2021 r. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 15 zhovtnia 2021 roku "Pro Stratehiiu informatsiinoi bezpeky". Decree of the President of Ukraine "On Information Security Strategy". URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text [in Ukrainian]
9. Digital 2022 July Global Statshot Report. Datareportal. URL: https://ain.ua/2022/04/30/zvit-digital-2022/
10. U-Report. Your voice matters. URL: https://ukraine.ureport.in/opinion/4025/