УДК 35.078.1:001.102-049.5:316.32

[https://doi.org/10.32689/2708-7530-2020-3\(3\)-51-59](https://doi.org/10.32689/2708-7530-2020-3(3)-51-59)

Чмир Ярослав Ігорович аспірант кафедри публічного адміністрування Міжрегіональної академії управління персоналом, вул. Фрометівська, 2, м. Київ, 03039, тел.: (098) 995-88-88, e-mail: JaroslawCM@ukr.net, <https://orcid.org/0000-0002-4476-6687>

ГЛОБАЛЬНИЙ ІНФОРМАЦІЙНИЙ ПРОСТІР ЯК ЧИННИК АКТУАЛІЗАЦІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

Анотація. Стаття досліджує чинники актуалізації інформаційної безпеки держави в глобальному інформаційному просторі. Зазначається, що формування єдиного світового глобального інформаційного простору, який містить в собі значний потенціал не тільки використання, але й зловживання інформацією, перетворення її на інструмент маніпуляції або відверто злочинних дій, поставило на порядок денний більшості країн світу проблематику забезпечення власної інформаційної безпеки та національного суверенітету держави. Висвітлюється класифікація основних загроз інформаційній безпеці та інформаційному суверенітету сучасних держав. Інформаційна безпека суспільства та держави розглядається як система, що забезпечує необхідний рівень стабільності та захищеності політичної, соціально-економічної, військово-оборонної, духовно-культурної та інших сфер і галузей життєдіяльності суспільства від небезпечних, дестабілізуючих негативних деструктивних загроз, що здатні завдати шкоду національним інтересам держави, сталому розвитку суспільства, благополуччю й здоров'ю кожного громадянина. З огляду на неминучість подальшого зростання загроз в сфері інформаційної безпеки пропонується низка заходів із забезпечення інформаційної безпеки людини суспільства та держави. Обґрунтовується чіткий взаємозв'язок інформаційної безпеки держави з відповідним рівнем інформаційної культури, що обумовлює місце й роль країни в глобальному інформаційному просторі, дозволяє своєчасно виявляти й нейтралізувати загрози та ризики негативного впливу шкідливого контенту національного і світового інформаційного простору, забезпечувати задоволення інформаційних потреб людини й суспільства, реалізацію національних інтересів держави в глобальному інформаційному просторі та здійснювати ефективний захист національного інформаційного простору та інформаційного суверенітету держави.

Ключові слова: держава, інформаційна безпека, інформаційний суверенітет, глобальний інформаційний простір

Chmyr Yaroslav Igorovich graduate student of the Department of Public Administration of the Interregional Academy of Personnel Management, Frometivska Str., 2, Kyiv, 03039, tel.: (098) 995-88-88, e-mail: JaroslawCM@ukr.net, <https://orcid.org/0000-0002-4476-6687>

GLOBAL INFORMATION SPACE AS A FACTOR OF UPDATING THE STATE INFORMATION SECURITY

Abstract. The article investigates the factors of actualization of information security of the state in the global information space. It is noted that the formation of a single global information space, which contains significant potential not only for the use but also misuse of information, turning it into a tool of manipulation or outright criminal actions, has put on the agenda of most countries to ensure their own information security and national sovereignty of the states. The classification of the main threats to information security and information sovereignty of modern states is covered. Information security of society and the state is seen as a system that provides the necessary level of stability and protection of political, socio-economic, military-defense, spiritual, cultural and other spheres and spheres of society from dangerous, destabilizing negative destructive threats that could harm national interests. state, sustainable development of society, well-being and health of every citizen. Given the inevitability of further growth of threats in the field of information security, a number of measures are proposed to ensure the information security of human society and the state. A clear relationship of information security of the state with the appropriate level of information culture, which determines the place and role of the country in the global information space, allows to identify and neutralize threats and risks of negative impact of harmful content of national and world information space, to meet information needs of man and society, realization of national interests of the state in the global information space and to carry out effective protection of the national information space and information sovereignty of the state.

Keywords: state, information security, information sovereignty, global information space

Постановка проблеми. Перехід до епохи інформаційного суспільства характеризується активним розгортанням процесів глобалізації та викликаних нею фундаментальних суспільно-політичних, економічних і промислово-виробничих трансформацій, що не останнім чином обумовлено інтенсивним розвитком інформаційно-комунікаційних технологій, стрімким розвитком технологій та значною інтенсифікацією обігу й споживання інформації. Інформаційно-комунікаційні технології та процеси почали набувати всеосяжного характеру й поступово перетворилися на системотворчий чинник життєдіяльності людської спільноти, основу нового високотехнологічного й комп'ютеризованого укладу.

Водночас, разом зі зростанням інтенсивності споживання інформації в усіх сферах життєдіяльності людства саме інформація та побудовані на її основі технології стають стратегічно визначальними характеристиками нового суспільно-цивілізаційного укладу привносячи в щоденну життєдіяльність людства як безперечні переваги, так і нові виклики, загрози та ризики. Невід'ємною складовою нової епохи є глобальне інформаційне інтегрування людства в переважній більшості сфер та галузей його життєдіяльності поза будь-які політичні, економічні, расові, культурні тощо розбіжності. Цей визначальний на сучасному етапі соціогуманітарний феномен обумовив створення єдиного світового

глобального інформаційного простору, який містить в собі значний потенціал не тільки використання, але й зловживання інформацією, перетворення її на інструмент маніпуляції або відверто злочинних дій, поставило на порядок денний більшості країн світу проблематику забезпечення власної інформаційної безпеки та національного суверенітету держави.

Аналіз останніх досліджень і публікацій. Дає підстави стверджувати, що у вітчизняному науковому дискурсі все активніше піднімається проблематика забезпечення інформаційного суверенітету держави, формування та розвитку системи інформаційної безпеки як важливої складової національної безпеки країни в цілому. Зокрема, плідно працюють в зазначеному напрямку такі науковці як І. Боднар [9], А. Головка [6], Л. Дорош [5], К. Молодецька [8], Ю. Нестеряк [10], І. Парфенюк [11], І. Сопілко [4], В. Торяник [2], А. Турчак [3] та інші. Водночас, все ще недостатнім є виявлення ознак, чинників та узагальнюючих ризиків і загроз інформаційній безпеці держави в глобальному інформаційному просторі в сучасних умовах, що й обумовлює формування **мети статі та постановки завдання** даного дослідження.

Виклад основного матеріалу. Інформаційне суспільство формує принципово нові умови існування націй, стверджує відомий британський професор Ентоні Сміт. На його думку створення глобального інформаційного простору, як "станового хребту сучасної цивілізації" призводить до зростання взаємовпливів національних культур, появи світоглядно-ціннісних конфліктів та так званого "інформаційного синдрому", що спричиняється низкою загрозливих факторів. Це, зокрема: диференціація суспільства, що тягне за собою необхідність розвитку діалогу між управлінським апаратом і підлеглими; небезпека виникнення інфократії (влади власників інформації); суперечність між універсальними завданнями демократії і потребами розвитку традиційного суспільства; суперечність між глобальними та національними цінностями; труднощі подолання демократичними засобами монополії на інформацію, забезпечення контролю суспільства за діяльністю засобів масової інформації і формування відповідного законодавства [1, с. 11].

Глобальний інформаційний простір складається з національних, корпоративних та приватних інформаційних просторів і має фактично ті ж ознаки, що й власне інформаційне суспільство. При цьому глобальний інформаційний простір "не має державних кордонів, не має таких інститутів захисту державних інтересів, якими є прикордонна й митна служби, поки що відсутні способи і засоби контролю цінності і важливості інформаційних ресурсів, що «перевозяться» через кордон. Поки що державний кордон є практично прозорим для інформаційних ресурсів" [2, с. 137].

На думку В. Торяника інформаційний простір – це "середовище, де здійснюється формування, збір, зберігання та розповсюдження інформації. Інформаційний простір України – це інформаційний простір, на який розповсюджується юрисдикція України" [3, с. 152].

Основними суб'єктами глобального та національних інформаційних просторів є наддержавні міжнародні органи й установи та транснаціональні корпорації, держави та їх уряди, господарюючі суб'єкти та фінансово-промислові групи,

політичні партії та організації громадянського суспільства, релігійні організації, фундаменталістські та терористичні угруповання, окремі політики й громадські діячі, журналісти й публіцисти, блогери та пересічні громадяни – всі, хто спроможний та має бажання і можливості на власний розсуд збирати, обробляти, сприймати, зберігати, перетворювати й поширювати інформацію будь-яким з доступних каналів комунікації.

При цьому об'єктом в середовищі глобального інформаційного простору завжди є як сама інформація та інформаційні відносини між суб'єктами, так і інформаційно-комунікаційні канали та індивідуальна психіка людини й суспільна думка політичних та економічних еліт, певних соціальних груп, прошарків населення, націй і народів.

На зазначені об'єкти спрямовуються конкурентні інформаційні потоки, що вже обумовило появу такого явища як "інформаційний лобізм" як особливий вид політичної й економічної комунікації в глобальному інформаційному просторі, покликаний створити політичний, економічний, психологічний тощо інформаційний вплив на посадових осіб, що приймають ключові публічно-управлінські рішення в інституціях публічного врядування та господарюючих суб'єктах з метою схилення таких осіб до ухвалення (або відмови від ухвалення) певних управлінських рішень на користь інформаційних лобістів. Саме з інформаційним лобізмом пов'язують цьогорічне ухвалення Верховною радою України законів про продаж сільськогосподарської землі та ігорний бізнес.

Таким чином, йдеться про загрози й ризики, які разом з безсумнівними перевагами несе в собі глобальне інформаційне суспільство, адже глобальний інформаційний простір не має національних і державних кордонів, практично позбавлений державного контролю й впливу, спроби цензурування нівелюються миттєвістю розповсюдження інформації та наявністю сотен обхідних каналів та приховувань ір-адреси комп'ютера споживача тощо. Глобальний інформаційний простір виявився привабливим інфраструктурним середовищем для різного роду шахраїв, злочинців та недоброзичливців, що призводить до масових порушень прав людини, викрадення інформації, промисловим та іншими видами шпигунства, хакерських атак на офіційні веб-сайти державних та фінансових установ, викраденні й продажу конфіденційної інформації про політичних діячів та пересічних людей, розповсюдження протиправного аморального та зловмісного контенту, що загрожує психічному здоров'ю особистості, насамперед, молоді тощо.

Як зазначає з цього приводу І. Сопілко "інформаційний прогрес перетворився на інструмент поневолення людини інформаційними технологіями. Насправді в інформаційному суспільстві відбувається поглинання особистості інформаційними технологіями, в якому люди заради матеріальних благ, отриманих від участі у різних мережевих системах, втрачають духовну свободу та взагалі особистість. Більше того, за такого прискореного інформаційного прогресу, людина може перетворитися на придаток до інформаційних технологій та інформаційних ресурсів. Прогресивне збільшення споживання інформації призводить до втрати свободи людини, втрати мети існування і підпорядкування своїх цілей цілям збереження і примноження інформаційних ресурсів" [4, с. 78-79].

Ми встановили, що процеси глобалізації та становлення глобального інформаційного суспільства підіймають на принципово новий щабель проблематику забезпечення інформаційної безпеки людині, громаді, державі, суспільству як на національному так і на світовому рівнях. Так, на думку Л. Дорош "чинники інформаційного суспільства визначають специфіку зміни сучасної соціально-політичної ситуації як у світі загалом, так і у кожній державі зокрема. Агресія сучасних мас-медіа на свідомість індивіда у кожному суспільстві, велика кількість слабо контрольованих контактів, навала екологічних, демографічних та інших проблем, збереження залишків тоталітарних установок у масовій свідомості громадян пострадянських суспільств, готовність їх до покори, формування психологічної беззахисності населення, яка стала основною передумовою піддатливості фаховому тиску зацікавлених осіб/груп, брак ефективно діючих громадських соціальних інститутів – усі ці чинники загрожують інформаційно-психологічній безпеці особи і суспільства, впливаючи в такий спосіб і на міжнародну безпеку" [5, с. 111-112].

Якщо спробувати класифікувати існуючі в глобальному інформаційному просторі загрози, то в найбільшому узагальненні маємо говорити про два основних класи таких загроз: інформаційно-психологічні та інформаційно-технологічні. Перші спрямовані на людину та її психологічний стан, систему цінностей, світоглядні орієнтації тощо. Сьогодні існує значна кількість різного роду технологій впливу на суспільну й особисту свідомість, від гіпнозу й нейролінгвістичного програмування (НЛП) до пропаганди та вірусної інформації ("фейки" і "меми"), зловмисне використання яких надає можливість морально-психологічний стан людини, дезорієнтувати її, похитнути усталені погляди й цінності. Ці загрози можуть бути персоніфікованими (спрямовані на конкретну людину) та деперсоніфікованими або масовими. Масове використання подібних технологій призводить до підриву суспільної свідомості суспільства та суспільно-політичного ладу й державно-владного режиму в цілому.

Загрози другого класу являють собою можливість пошкодження, спотворення або знищення інформації на носіях та в базах даних, встановлення шпійонських програм стеження, розміщення різного роду вірусів, "червів" та "троянів", виведення з ладу серверів, комп'ютерного обладнання та програмного забезпечення, пошкодження ліній урядового та військового зв'язку тощо.

А. Головка пропонує чотири групи інформаційних загроз, які відповідають чотирьом сферам, які піддаються їх впливу: 1) ціннісну (вплив на громадську думку); 2) технологічну (вплив на кіберпростір); 3) правову (відсутність / недосконалість правової бази, що регулює правовідносини в інформаційній сфері); 4) соціально-політичну (цензура, обмеження доступу до публічної інформації) [6, с. 44].

У свою чергу А. Турчак говорить про внутрішні та зовнішні джерела загроз. З його погляду, "внутрішні джерела – це відсутність історичних, політичних та соціальних практичних навичок проживання на території правової держави, що зачіпає процес практичного втілення конституційних прав і свобод населення, зокрема, в межах інформаційної сфери та примноження організованих правопорушень та ріст числа правопорушень комп'ютерного спрямування,

зменшення частки числа освіченого населення, що сильно утруднює підготовку трудового ресурсу для застосування новітнього технологічного забезпечення, зокрема, інформаційного. Недостатня координація роботи такого органу, як вище державне керівництво, владних структур та угруповань військового характеру у втіленні єдиної державної політики забезпечення нацбезпеки теж можна зарахувати до таких джерел. Тут же і відставання нашої держави від розвинених країн за інформатизацією посадовців, юридично- фінансових, промислових структур та побутовими умовами населення. Серед джерел зовнішнього характеру є іноземні політичні, військові, економічні та розвідувальні структури інформаційної сфери; політика домінування певних держав в інформаційній сфері; робота міжнародних терористичних угруповань; розробка різними структурами концепції війн інформаційного характеру; культурне захоплення конкретних країн" [7, с. 51].

Специфічним й одночасно доволі широко розповсюдженим джерелом загроз інформаційній безпеці держави К. Молодецька називає соціальні інтернет-сервіси (СІС), які є надзвичайно популярні серед людей всіх вікових і професійних категорій, рас і прошарків всієї Земної кулі. Проте, зазначає дослідниця, "їх позитивні комунікаційні характеристики можуть бути використані зловмисниками для поширення деструктивного контенту, який може носити недостовірний, неповний або упереджений характер і становити загрозу інформаційній безпеці держави [8, с. 13].

Як вважає І. Боднар, "головна інформаційна загроза національній безпеці – це загроза впливу іншої сторони на інформаційну інфраструктуру країни, інформаційні ресурси, на суспільство, свідомість, підсвідомість особистості, з метою нав'язати державі бажану (для іншої сторони) систему цінностей, поглядів, інтересів і рішень у життєво важливих сферах суспільної й державної діяльності, керувати їхньою поведінкою і розвитком у бажаному для іншої сторони напрямку. Власне, це є загрозою суверенітету України в життєво важливих сферах суспільної й державної діяльності, що реалізовується на інформаційному рівні" [9, с. 69].

Отже, ми встановили, що в інформаційному суспільстві та глобальному інформаційному просторі оперування інформаційними потоками, вся сукупність інформаційно-комунікаційних відносин і системи їх регулювання відіграють системотворчу роль життєдіяльності людських спільнот та здійснюють вирішальний вплив на стан і динаміку політичної, соціально-економічної, військово-оборонної, духовно-культурної та інших складових суспільно-політичного буття людини, всю систему органів публічного врядування кожної країни. Це означає, що в кожній з названих складових важливу роль відіграє інформаційна безпека відповідної сфери, а сама інформаційна безпека все більше виходить на передній план загальної національної безпеки і ця тенденція надалі тільки зростатиме. Адже якщо інформація є основним ресурсом постіндустріального інформаційного суспільства, то й інформаційна безпека також є основою національної безпеки держави.

Неминучість подальшого зростання загроз в сфері інформаційної безпеки підкреслив доктор наук з державного управління Ю. Нестеряк. Очевидно – зазначив він – "що технологічно розвинені держави намагаються і

продовжуватимуть збільшувати політичну, економічну та військову перевагу за рахунок досягнення переваг у рівні інформатизації; і, як наслідок, – установа та проведення глобального інформаційного контролю над менш розвиненими державами, проведення в загальному інформаційному просторі ідеологічної та культурної експансії" [10, с. 64-65].

У відповідь на посталі загрози заходи із забезпечення інформаційної безпеки людини суспільства та держави також можна поділити на кілька основних груп: 1) відкритості та доступності інформації; 2) відносної повноти та цілісності інформації; 3) захисту конфіденційної інформації; 4) мережевої безпеки; 5) технічної інфраструктури; 6) програмного забезпечення.

Під таким кутом зору інформаційна безпека суспільства та держави характеризує рівень стабільності та захищеності політичної, соціально-економічної, військово-оборонної, духовно-культурної та інших сфер і галузей життєдіяльності суспільства від кожної з шести вищеперелічених груп небезпечних, дестабілізуючих негативних деструктивних загроз, що здатні завдати шкоду національним інтересам держави, сталому розвитку суспільства, благополуччю й здоров'ю кожного громадянина. В цілому інформаційну безпеку країни в загальнонаціональних масштабах А. Турчак визначає "як систему заходів, що мають на меті не допустити несанкціонований доступ до інформаційних ресурсів, їхню модифікацію та руйнацію. Вона передбачає втілення таких цілей: захистити політичні, державні і громадські інтереси; захистити моральні цінності; заборонити інформацію, яка пропагує агресивну війну, насилля, дискримінацію та порушення прав громадянина" [7, с. 48].

Перебуваючи щоденно в інформаційному просторі кожна людина постійно відчуває на собі вплив інформаційних потоків, які завжди залишають свій слід хоча б на рівні підсвідомості. Інформація поступово й латентно змінює нашу свідомість та впливає на зміни в нашому світогляді в цілому без різниці – приймаємо ми активну або пасивну участь в інформаційно-комунікаційних відносинах – інформація накопичується в свідомості людини й рано чи пізно але її кількість може обумовити якісний стрибок, який може бути як позитивним, так і негативним в залежності від інформаційного контенту, який надходить з тієї частки глобального інформаційного простору, в яку інтегрований даний індивід.

Це дає підстави стверджувати про існування феномену інформаційної культури людини, який безпосередньо пов'язаний з інформаційною безпекою. Такої думки дотримується, І. Парфенюк, який зазначає, що "інформаційна безпека особистості й держави багато в чому залежить від стану культурного простору, який є своєрідним "фільтром" для шкідливого контенту в процесі соціальних комунікацій. Завдання підтримання безпеки передбачає не лише моніторинг відкритих і закритих джерел інформації всередині та зовні країни, вивчення здійснених інформаційних атак, дослідження громадської думки, прогнозування суспільно-політичних процесів, удосконалення інформаційного та культурного законодавства, а й розроблення теоретичних засад відновлення культурного простору, розповсюдження якісної національної інформаційної продукції тощо" [11, с. 10].

Отже з точки зору забезпечення інформаційної безпеки особистості, суспільства та держави є важливим формування відповідної інформаційної, інформаційно-комунікаційної та інформаційно-світоглядної системи освіти громадян, формування сучасної інформаційної культури суспільства в цілому. Це має бути принципово новий тип інформаційної культури, оскільки вперше в людській історії головним в інформаційно-комунікаційних відносинах стає не стільки отримання й усвоєння знань, а вміння користуватися інформацією, тобто не знати щось необхідне сьогодні й зараз (що є неможливим в умовах безмежного валу інформації в інформаційному просторі), а вміння знайти сьогодні й зараз саме цю потрібну інформацію й відділити її від "спаму" та іншого інформаційного сміття.

Висновки. Таким чином, в результаті проведеного в даному дослідженні аналізу, ми встановили чіткий взаємозв'язок державної інформаційної політики, інформаційної безпеки людини та суспільства з відповідним рівнем інформаційної культури, що обумовлює місце й роль країни в глобальному інформаційному просторі, дозволяє своєчасно виявляти й нейтралізувати загрози та ризики негативного впливу шкідливого контенту національного і світового інформаційного простору, забезпечувати задоволення інформаційних потреб людини й суспільства, реалізацію національних інтересів держави в глобальному інформаційному просторі та здійснювати ефективний захист національного інформаційного простору та інформаційного суверенітету держави.

Формування нової інформаційної культури суспільства – одна з функцій та нагальних завдань держави, що хоче бути повноправним суб'єктом глобального інформаційного простору. Це передбачає як концептуальне бачення, так і стратегічне планування, закріплені на законодавчому рівні (наприклад, в Доктрині інформаційної безпеки України), а також формування на цих засадах і реалізацію державної інформаційної політики в цілому й державної політики інформаційної безпеки зокрема.

Література:

1. Smith Anthony. Nations and Nationalism in a Global Era. John Wiley & Sons, 2013. 222 p.
2. Соціально-гуманітарна сфера України в сучасних дискурсах : монографія ; за заг. ред. проф. О. Ю. Панфілова. Харків : ХІФ КНТЕУ, 2019. 284 с.
3. Торяник В. Інформаційна безпека як складова національної безпеки держави: роль ЗМІ в забезпеченні інформаційного суверенітету України. *Право і суспільство*. 2016. № 2. С. 151-156.
4. Сопілко І. Інформаційні загрози та безпека сучасного українського суспільства. *Юридичний вісник*. 2015. № 1 (34). С. 75–80.
5. Дорош Л. Інформаційно-психологічна безпека особи, суспільства та держави: новітні виклики міжнародній безпеці. *Українська національна ідея: реалії та перспективи розвитку*. 2013. Вип. 25. С. 107-112.
6. Holovka, A. Information threats in a globalized world: economics, politics, society (experience of Ukraine). *Baltic Journal of Economic Studies*, Vol. 2 (2016), No. 3 : p. 42-47.
7. Турчак А. Основні складові інформаційної безпеки держави. *Аспекти публічного управління*. 2019. Т. 7, № 5. С. 44-56.
8. Молодецька К. Соціальні інтернет-сервіси як суб'єкт інформаційної безпеки держави. *Information Technology and Security*. 2016. Vol. 4, № 1. С. 13-20.
9. Боднар І. Інформаційна безпека як основа національної безпеки. *Mechanism of*

Economic Regulation. 2014. № 1. С. 68-75.

10. Нестеряк Ю. Міжнародні критерії інформаційної безпеки держави: теоретико-методологічний аналіз. *Публічне управління: теорія та практика*. 2014. Вип. 1. С. 62-67.

11. Парфенюк І. Інструментарій інформаційних війн: традиційні та новітні засоби. *Вісник Книжкової палати*. 2019. № 1. С. 7-10.

References:

1. Smith, Anthony. (2013). *Nations and Nationalism in a Global Era*. John Wiley & Sons.
2. Panfilov O. (ed.), (2019), *Sotsial'no-humanitarna sfera Ukrayiny v suchasnykh dyskursakh [Socio-humanitarian sphere of Ukraine in modern discourses]*, Monograph, Press HIF KNTU, Kharkiv, 284 p. In Ukraine.
3. Toryanyk, V. (2016), Informatsiyna bezpeka yak skladova natsional'noyi bezpeky derzhavy: rol' ZMI v zabezpechenni informatsiynoho suverenitetu Ukrayiny [Information security as a component of national security: the role of the media in ensuring the information sovereignty of Ukraine], *Pravo i suspil'stvo – Law and Society*, vol. 2, pp. 151-156. In Ukraine.
4. Sopilko, I. (2015), Informatsiyni zahrozy ta bezpeka suchasnoho ukrayins'koho suspil'stva [Information threats and security of modern Ukrainian society], *Yurydychnyy visnyk – Legal Bulletin*, vol. 1 (34), pp. 75–80. In Ukraine.
5. Dorosh, L. (2013), Informatsiyno-psykholohichna bezpeka osoby, suspil'stva ta derzhavy: novitni vyklyky mizhnarodniy bezpetsi [Information and psychological security of the individual, society and state: the latest challenges to international security], *Ukrayins'ka natsional'na ideya: realiyi ta perspektyvy rozvytku – Ukrainian national idea: realities and prospects for development*, vol. 25, pp. 107-112. In Ukraine.
6. Holovka, A. (2016). Information threats in a globalized world: economics, politics, society (experience of Ukraine). *Baltic Journal of Economic Studies*, Vol. 2, No. 3, pp. 42-47.
7. Turchak, A. (2019), Osnovni skladovi informatsiynoyi bezpeky derzhavy [The main components of information security of the state], *Aspekty publichnoho upravlinnya – Aspects of public administration*, T. 7, vol. 5. pp. 44-56. In Ukraine.
8. Molodetskaya, K. (2016), Sotsial'ni internet-servisy yak sub'yekt informatsiynoyi bezpeky derzhavy [Internet social services as a subject of information security of the state, Information Technology and Security], *Information Technology and Security*, Vol. 4, № 1, pp. 13-20. In Ukraine.
9. Bodnar, I. (2014), Informatsiyna bezpeka yak osnova natsional'noyi bezpeky [Information security as a basis for national security], *Mechanism of Economic Regulation*, vol. 1, pp. 68-75. In Ukraine.
10. Nesteryak, Y. (2014), Mizhnarodni kryteriyi informatsiynoyi bezpeky derzhavy: teoretyko-metodolohichnyy analiz [International criteria of information security of the state: theoretical and methodological analysis], *Publichne upravlinnya: teoriya ta praktyka – Public administration: theory and practice*, vol. 1, pp. 62-67. In Ukraine.
11. Parfenyuk, I. (2019), Instrumentariy informatsiynykh viyn: tradytsiyni ta novitni zasoby [Tools of information wars: traditional and modern means], *Visnyk Knyzhkovoyi palaty – Bulletin of the Book Chamber*, vol. 1, pp. 7-10. In Ukraine.