



УДК 159.923:004.056

[https://doi.org/10.32689/2617-2224-2022-3\(31\)-7](https://doi.org/10.32689/2617-2224-2022-3(31)-7)

Сердюк Ірина Анатоліївна,

аспірантка кафедри публічного адміністрування Міжрегіональної Академії управління персоналом, молодший науковий співробітник, біофізик відділення нейрофізіології Державного закладу «Науково-практичний медичний реабілітаційно-діагностичний центр МОЗ України», 85110, Україна, Донецька область, м. Костянтинівка, вул. О.Невського, 14, тел. (06272) 2-55-17, e-mail: irina-serduk@ukr.net, <https://orcid.org/0000-0001-9840-7340>

Serdyuk Irina Anatolievna,

PhD student, Interregional Academy of Personnel Management, Junior Researcher, Biophysicist of the Department of Neurophysiology State institution "Scientific and Practical Medical Rehabilitation and Diagnostic Center of the Ministry of Health of Ukraine", 85110, Ukraine, Donetsk region, Kostiantynivka, Al.Nevskogo St. 14, (06272) 2-55-17, Email: irina-serduk@ukr.net, <https://orcid.org/0000-0001-9840-7340>

ПІДХОДИ ПУБЛІЧНОГО УПРАВЛІННЯ ДО ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОСОБИСТОСТІ

Анотація. Впровадження сучасних інформаційних технологій у всі сфери суспільного життя істотно підвищило залежність безпеки суспільства, кожної конкретної людини від надійності функціонування інформаційної інфраструктури, достовірності інформації, що використовується, її захищеності від несанкціонованої модифікації, а також протиправного доступу до неї. Потреби сучасної людини суттєво змінилися і розширилися, зріс попит на інформаційну безпеку. Виходячи з цього, виникає потреба у забезпеченні інформаційної безпеки, насамперед особистості, як носія індивідуальних здібностей, характеру, інтересів. В умовах турбулентних явищ, глобальне інформаційне суспільство надає істотний вплив на формування та активність особистості, створюючи для неї не тільки нові можливості, але й значні загрози. Таким чином, дослідження негативних інформаційних впливів, підходів публічного управління до збереження інформаційної безпеки людини, її ментального здоров'я є важливим і актуальним питанням державної інформаційної політики.

Мета роботи. Розкрити поняття інформаційна безпека особистості та дослідити підходи публічного управління щодо її забезпечення.

Методологія. Серед переліку методів дослідження обрано метод систематизації, узагальнення та ретроспективний аналіз.

Наукова новизна. Дістали подальший розвиток: історичний огляд основних підходів до поняття та ознак інформаційної безпеки особистості, підходи публічного управління до забезпечення інформаційної безпеки особистості як на державному рівні, що враховує вдосконалення законодавчої бази, так і на особистісному рівні, її здатність протистояти інформаційним загрозам і зберігати психічне здоров'я в умовах негативної інформаційної дії, що залежить від формування та розвитку культури особистої інформаційної безпеки.

Висновки. Ефективність правових механізмів протидії викликам і загрозам інформаційної безпеки особистості безпосередньо залежить від рівня правового забезпечення інформаційної безпеки особистості. Однак, розв'язання проблеми забезпечення інформаційної безпеки особистості

повинно мати комплексний системний характер та здійснюватися на різних рівнях (законодавчому, адміністративному, особистісному).

Ключові слова: інформація, безпека, публічне управління, турбулентність, інформаційна безпека особистості, загрози.

PUBLIC ADMINISTRATION APPROACHES TO PERSONAL INFORMATION SECURITY

Abstract. The introduction of modern information technologies into all spheres of social life has significantly increased the dependence of the society safety, of each individual person, on the reliability of the information infrastructure functioning, the reliability of the used information, its protection against unauthorized modification, as well as illegal access to it. The needs of modern people have changed and expanded significantly, and the demand for information security has increased. Based on this, there is a need to ensure information security, primarily of the individual, as the bearer of individual abilities, character, and interests. Under the conditions of turbulent phenomena, the global information society exerts a significant influence on the formation and activity of the individual, creating for him not only new opportunities, but also significant threats. Thus, the study of negative informational influences, approaches of public management to the preservation of information security of a person, his/her mental health is an important and urgent issue of the state information policy.

The purpose of the article. It is necessary to reveal the concept of information security of an individual and to investigate the approaches of public management to its provision.

Methodology. Among the list of research methods, the method of systematization, generalization and retrospective analysis was chosen.

Scientific novelty. Further development received: a historical overview of the main approaches to the concept and signs of personal information security, public administration approaches to ensuring personal information security both at the state level, which takes into account the improvement of the legislative framework and at the personal level, its ability to resist information threats and preserve mental health under the conditions of negative information action, which depends on the formation and development of the culture of personal information security.

Conclusions. The effectiveness of legal mechanisms for countering challenges and threats to personal information security directly depends on the level of legal protection of personal information security. However, solving the problem of ensuring personal information security should have a complex systemic nature and be carried out at different levels (legislative, administrative, personal).

Key words: information, security, public administration, turbulence, personal information security, threats.

Вступ. Сьогодні інформаційна сфера стала такою ж важливою складовою суспільного життя, як економічна, екологічна, військова, зовнішньополітична чи правоохоронна сфера. Проте впровадження сучасних інформаційних технологій у всі сфери суспільного життя істотно підвищило залежність безпеки суспільства, кожної конкретної людини від надійності функціонування інформаційної інфраструктури, достовірності інформації, що використовується, її захищеності від несанкціонованої модифікації, а також протиправного доступу до неї. Потреби сучасної людини суттєво змінилися і розширилися, зріс попит на інформаційну безпеку задля особистісної реалізації в умовах турбулентного розвитку, інформаційного навалу та несистемного суспільного хаосу.

Недостатньо якісне інформаційне забезпечення, обмеженість в інформації або низька якість інформації призводить до руйнівних

змін психіки людей, які проявляються в підвищенні психічної напруженості та неадекватній соціальній поведінці, що є наслідком відсутності достатніх можливостей для соціального орієнтування людини в навколишній ситуації та розуміння напрямків її розвитку, тобто неможливість отримання соціально значущих даних у великому інформаційному потоці. Це завдає шкоди ментальному здоров'ю громадян, що руйнує моральні норми життя суспільства, призводить до дестабілізації соціально-політичної ситуації.

Вибрана тема дослідження покликана сприяти розв'язанню проблеми інформаційної безпеки особистості в умовах турбулентності.

Аналіз останніх публікацій за проблематикою. Питання публічного управління у сфері безпеки (національної, регіональної тощо) та її забезпечення розглядаються у працях Боднара І.Р., Петрика В.М., Степанова В.Ю., Ільницької

У., Олійника О.В. та ін. Проблеми забезпечення інформаційної безпеки як складової національної безпеки знайшли відображення у роботах Банчука М.В., Панченка О.А., Кукіна І.В., Шишкіної Х.Ю., Хворост М.Ю. та інших науковців. Авторами досліджувались, як окремі аспекти інформаційної безпеки особистості, суспільства, держави загалом, так і окремі питання психологічної безпеки особистості у сучасному інформаційному просторі. Однак в умовах турбулентних явищ, запобігання негативним інформаційним впливам вимагає додаткових досліджень щодо проблем інформаційної безпеки особистості.

Таким чином, дослідження негативних інформаційних впливів, підходів публічного управління до збереження інформаційної безпеки людини, її ментального здоров'я є важливим і актуальним питанням державної інформаційної політики.

Мета дослідження. Розкрити поняття інформаційна безпека особистості та дослідити підходи публічного управління щодо її забезпечення.

Визначення категорії «інформаційна безпека особистості». Інформація завжди відіграла надзвичайно важливу роль і ставала все більш суттєвою. Володіння інформацією у достатній кількості допомагає людині правильно оцінити події, що відбуваються навколо неї, розробити варіанти своїх дій та прийняти обдумане рішення. Водночас інформація є найсильнішим засобом впливу на особистість, суспільство та світ загалом (Шишкіна, Хворост, 2013). Саме тому людству в умовах турбулентності потрібен механізм фільтрації інформації, а згодом інструмент захисту від небажаної та негативної інформації.

Основною особливістю функціонування інформації в інформаційне суспільство є її спрямованість на людину. У такій інформаційній спрямованості є свої плюси, і свої мінуси. До плюсів можна віднести те, що інформаційне середовище спрямоване на людину, задоволення її інформаційних та інших потреб. До негативних наслідків інформаційної спрямованості належать соціальні страхи та соціальні фобії, інформаційні загрози та ризики, стресогенні інформаційні чинники та форми інформаційного соціального тиску.

Стан захищеності особистості від внутрішніх та зовнішніх загроз в інформаційній сфері досліджувався в різних науках: юридичних, соціологічних, історичних, педагогічних, політичних, технічних, економічних, філософських, військових наук, культурології та інших (Боднар,

Вовчанська, 2014; Ільницька, 2016; Степанов, 2016). При цьому сам концепт «особистість» як збірний термін щодо таких суб'єктів як людина, персону, індивід, кожен, громадянин, підданий, особа, фізична особа дозволяє акумулювати різні форми реалізації прав і свобод людини в системі правового забезпечення інформаційної безпеки та обґрунтовує особистісно-орієнтований підхід до забезпечення його активності та безпеки в сучасному інформаційному просторі.

В умовах турбулентності, що руйнує звичні стереотипи поведінки та сформований образ життя, потреба в безпеці стає домінують (Панченко, Кабанцева, 2020). Феномен безпеки за своїм змістом є багатограним, а отже, і поняття безпеки є неоднозначним. Безпека характеризує конкретний стан захищеності та здатність протистояти змінам, умовам функціонування передбачуваного або спонтанного характеру та може застосовуватися як щодо особистості зокрема, так і суспільства та держави в цілому. Як поняття, безпека відрізняється в залежності від сфери застосування: економіки, науки, соціології, сфери управління та ін. Безпека – гарантована конституційними, законодавчими та практичними заходами.

Безпека в основі державної політики визначається як стан захищеності життєво важливих інтересів особистості, суспільства та держави від зовнішніх та внутрішніх загроз. Однак, безпека, що є державним завданням, полягає не тільки у відсутності загроз, які суб'єктивно сприймаються окремими особами й групами, а й в оцінці та підготовці особистості та державних структур до інформаційних загроз.

Інформаційна безпека являє собою складну, динамічну, цілісну соціальну систему, компонентами якої є підсистеми безпеки особистості, держави й суспільства. В аналізі проблеми забезпечення інформаційної безпеки важливим аспектом є розкриття її сутності. Під інформаційною безпекою мається на увазі: 1) стан захищеності життєво-важливих інтересів особи, суспільства й держави, за якого зводиться до мінімуму заподіяння шкоди через неповність, несвоєчасність та недостовірність інформації; деструктивний її вплив; неправомірне використання та поширення персональних даних; 2) стан захищеності національного інформаційного простору, який забезпечує формування, використання і розвиток останнього в інтересах громадян, організацій, держави. Виділяють наступні види інформаційної безпеки (рис. 1.) (Панченко, 2020). Забезпечення інформаційної безпеки можна визначити як комплекс адміні-

стративних заходів необхідний для досягнення такого стану інформаційного розвитку (духовного, соціально-політичного, технічного) та захищеності особи, суспільства, держави, за якого сторонні інформаційні впливи не завдають суттєвої шкоди національним інтересам (Петрик, 2015).



Рис. 1. Види інформаційної безпеки.

В умовах турбулентності інтереси особистості полягають у реальному забезпеченні своїх конституційних прав і свобод, особистої безпеки, підвищення якості та рівня життя, можливості фізичного, інтелектуального та духовного розвитку. Виходячи з цього, виникає потреба у забезпеченні інформаційної безпеки, насамперед особистості, як носія індивідуальних здібностей, характеру, інтересів. Інформаційна безпека особистості – це по-перше, стан захищеності, у якому відсутня загроза заподіяння шкоди інформації, якою володіє особистість; по-друге, стан та умова життєдіяльності особистості, за яких відсутня загроза заподіяння шкоди особистості інформацією (Панченко, 2011).

Інформаційна безпека особистості характеризується захищеністю психіки, свідомості від небезпечних інформаційних впливів. Вона залежить як від особистісних якостей індивіда, так і від моральних, соціальних та правових умов у суспільстві. Неодмінними умовами маніпулювання людиною, групою людей є неінформованість або дезінформованість, відсталість особистості й суспільства в галузі користування сучасними засобами масової інформації або ізольованість від них (Панченко, Кабанцева, 2020).

Зростаюча небезпека інформаційного плану особистості, суспільства, держави представляє новий тип соціально небезпечних злочинів, заснованих на використанні сучасної інформаційної техніки та технології. Проблема інформаційної безпеки особистості безпосередньо пов'я-

зана з інформаційними технологіями взагалі й з рекламними інформаційними технологіями зокрема, що психологічно впливають на особистість, маніпулюють її свідомістю, конструюють псевдореальність, спонукаючи людину до тих чи інших вчинків.

1. **Підходи публічного управління до інформаційної безпеки особистості.** Задля забезпечення інформаційною безпекою особистість необхідний потужний захист з боку держави. Вона на правому рівні повинна забезпечувати цю безпеку (Закон України «Про інформацію», Закон України «Про захист інформації в інформаційно-телекомунікаційних системах», Закон України «Про захист персональних даних», Указ Президента України «Про стратегію інформаційної безпеки» та ін.). Причому треба постійно вдосконалювати законодавчу базу, яка повинна змінюватися «в ногу з часом» з урахуванням динаміки загроз в інформаційній сфері.

Під державно-правовим механізмом забезпечення інформаційної безпеки особистості мається на увазі «система нормативних, організаційних елементів та процедур, які гарантують стан захищеності людини в інформаційній сфері та надають особистості фактичну можливість реалізувати свої інформаційні права та свободи». До структури цього механізму, входять: соціальні норми, гарантії забезпечення інформаційної безпеки особистості, а також функціонування різних соціальних інститутів суспільства, у тому числі міжнародних та внутрішньодержавних урядових та неурядових організацій (Кукін, 2020). Так, нормативну основу досліджуваного механізму складають досить великий комплекс міжнародних та внутрішньодержавних нормативних правових актів, що регламентують сферу забезпечення права особи на інформаційну безпеку. До структурних елементів конституційних гарантій права і свободи особи відносять: правові принципи, суб'єктивні права та свободи, юридичні обов'язки, заборони, обмеження, вимоги; заходи, спрямовані на охорону, захист та компенсацію; повноваження Президента України, державних органів, органів місцевого самоврядування, посадових осіб, громадських об'єднань (Олійник, 2012).

Основні підходи публічного управління щодо забезпечення інформаційної безпеки особистості повинні базуватися на забезпеченні права на достовірну, повну та своєчасну інформацію, свободи слова та інформаційної діяльності в національному інформаційному просторі, недопущення втручання в зміст та внутрішню організацію інформаційних процесів, крім

випадків, визначених законодавством відповідно до Конституції України; збереженні та вдосконаленні вітчизняного національного інформаційного продукту та технологій, гарантування державної підтримки та розвитку ресурсів науково-технічної продукції та інформаційних технологій (Боднар, Вовчанська, 2014).

Іншим засобом захисту, виступає сама особистість, її завбачливе ставлення до інформації, яку вона має, надає або розміщує. Для того, щоб задати певні моральні орієнтири, систему цінностей, необхідно як додатковий елемент у структурі механізму забезпечення права особи на інформаційну безпеку виділити культуру особистої інформаційної безпеки.

Саме поняття «культури особистої інформаційної безпеки» не нове, воно впливає з поняття «інформаційна культура» і набуває у сучасних реаліях іншого значення. Безсумнівно, інформаційна культура є частиною загальної культури особистості. Вона доповнюється характеристиками, необхідними сучасної дійсності: вміння орієнтуватися у величезному масиві інформаційних джерел, аналізувати інформацію, користуватися сучасними інформаційно-комунікаційними технологіями, критично оцінювати будь-яку отриману інформацію. Розвивати цей вид культури потрібно у всіх категорій громадян з урахуванням їхнього віку.

Під культурою особистої інформаційної безпеки мається на увазі сукупність принципів, вкладених у формування правил поведінки в інформаційному просторі, вивчення основ функціонування інформаційного суспільства, певного рівня інформаційного світогляду та інформаційної етики. Варто зазначити, що громадяни самі досить часто легковажно ставляться до розголошення та розповсюдження своїх особистих даних, дають згоду на обробку своїх персональних даних, не ознайомившись належним чином з її умовами. При цьому рідко хто замислюється про виникнення можливих негативних наслідків для себе від даних дій. У зв'язку з цим виникає потреба у необхідності формування культури особистої інформаційної безпеки, бо лише правового закріплення основ інформаційної безпеки без належного ставлення громадян до цих питань недостатньо.

Як зазначено в Стратегії інформаційної безпеки «відсутність належного рівня інформаційної культури та медіаграмотності в суспільстві в умовах стрімкого розвитку цифрових технологій створює підґрунтя для маніпулювання громадською думкою, проведення стрімких деструктивних інформаційних операцій, що

зумовлює існування потенційних та реальних загроз інформаційній безпеці України» (Указ Президента України № 685/2021). Тому формування та розвиток культури особистої інформаційної безпеки в умовах турбулентного часу повинно мати комплексний системний характер. Розвиток культури інформаційної безпеки особистості має здійснюватися як ззовні (навчання в дитячому віці прийомів безпечного користування Інтернетом з моменту початку його використання на рівні сім'ї, школи, суспільства, держави), так і власними зусиллями людини (саморозвиток, самоорганізація, мотивація).

Окремо можна виділити поняття «культура інформаційного самозахисту», оскільки воно комплексно поєднує в собі риси матеріального й ідеального світогляду особистості, що формують його інформаційну культуру як в частині культури інформаційно-професійної компетенції, так і в частині культури інформаційної безпеки.

Культура інформаційного самозахисту характеризується тими рисами інформаційної культури особистості, які визначають уміння поведінки з інформацією без завдання шкоди собі та іншим учасникам інформаційних відносин; здатність протистояти інформаційним загрозам і зберігати психічне здоров'я в умовах негативної інформаційної дії. Вона формується протягом всього життя людини в процесі безперервного навчання, виховання і самовиховання, чому сприяє високий рівень інформаційної культури та грамотності суспільства.

Інформаційна безпека особистості в умовах турбулентності постає як нагальна проблема, що потребує системного вирішення. Розв'язання проблеми забезпечення інформаційної безпеки суспільства та особистості повинно мати комплексний системний характер і здійснюватися на різних рівнях:

1) законодавчий рівень (закони, нормативні акти, стандарти тощо), що є вкрай важливим для забезпечення інформаційної безпеки. До заходів цього рівня належить регламентація законом та нормативними актами дій з інформацією та обладнанням, та настання відповідальності за порушення таких дій.

2) адміністративний рівень (дії загального характеру, що здійснюються керівництвом організації). Головною метою заходів цього рівня є формування програм у галузі інформаційної безпеки та забезпечення їх виконання, виділяючи необхідні ресурси та контролюючи стан справ. Основою програми є безпекова політика, що відображає підхід організації до захисту

своїх інформаційних активів. Задля підтримки режиму безпеки необхідно виділяти значні ресурси.

3) особистісний рівень, що пов'язаний, перш за все, із самовихованням, самоосвітою. Заходи цього рівня направлені на формування потрібних особистісних якостей щодо забезпечення інформаційного самозахисту особистості.

Висновки та перспективи подальших досліджень

В умовах турбулентних явищ, глобальне інформаційне суспільство надає істотний вплив на формування та активність особистості, створюючи для неї не тільки нові можливості, але й значні загрози. Ефективність правових механізмів протидії викликам і загрозам інформаційної безпеки особистості безпосередньо залежить від рівня правового забезпечення інформаційної безпеки особистості. Однак, розв'язання проблеми забезпечення інформаційної безпеки особистості повинно мати комплексний системний характер та здійснюватися на різних рівнях (законодавчому, адміністративному, особистісному).

Задля забезпечення інформаційною безпекою особистість необхідний потужний захист з боку держави. Механізм публічного управління інформаційною безпекою особистості являє собою спільну діяльність органів державної влади та місцевого самоврядування, які із залученням громадських організацій, окремих осіб, притаманними їм нормативно-правовими актами що повинна забезпечувати адекватне реальності сприйняття людиною соціально значущої інформації з метою створення умов для всебічного і гармонійного розвитку людини. Іншим засобом захисту, виступає сама особистість. Її здатність протистояти інформаційним загрозам і зберігати психічне здоров'я в умовах негативної інформаційної дії залежить від формування та розвитку культури особистої інформаційної безпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Боднар І.Р., Вовчанська О.М. Державна політика та інформаційна безпека України: післякризові виклики. *Вісник Львівської комерційної академії. Серія економічна*. 2014. Вип. 46. С. 28-32.
2. Ільницька У. Інформаційна безпека України: сучасні виклики, загрози та механізми протидії негативним інформаційно-психологічним впливам. *Політичні науки*. Вип. 2. № 1. 2016. С. 27-32.
3. Кукін І.В. Комплексний механізм публічного управління інформаційною безпекою особистості у сфері національної безпеки та її прикордонному

секторі. *Публічне управління та митне адміністрування*. № 4 (27), 2020. С. 134-139.

4. Олійник О.В. Адміністративно-правові засади інформаційної безпеки. *Європейські перспективи*. 2012. № 4(1). С. 65-68.
5. Панченко О.А. Державне управління інформаційною безпекою в турбулентному суспільстві. *World Science*. 2020. № 5(57). Vol. 3. С. 4-9.
6. Панченко О.А. Информационная безопасность личности: монография / О.А. Панченко, Н.В. Банчук. К.: КИТ, 2011. 672 с.
7. Панченко О.А., Кабанцева А.В., Сердюк І.А. Потреби особистості на інформаційну безпеку. *Публічне урядування*. 2020. № 3 (23). С. 203-214.
8. Петрик В.М. Забезпечення інформаційної безпеки держави: підручник; за заг. ред. О.А. Семченка та В.М. Петрика. Київ: ДНУ «Книжкова палата України», 2015. 672 с.
9. Степанов В.Ю., Інформаційна безпека в інформаційній сфері державного управління. *Теорія та практика державного управління*. 2016. 4(55). С. 24-28.
10. Указ Президента України Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки» від 28.12.2021 № 685/2021.
11. Шишкіна Х.Ю., Хворост М.Ю. Інформаційна безпека особистості як передумова збереження психічного здоров'я. *Проблеми екстремальної та кризової психології*. 2013. Вип. 14. Частина IV. С. 246-253.

REFERENCES:

1. Bodnar I.R., Vovchanska O.M. (2014). Derzhavna polityka ta informatsijna bezpeka Ukrainy: pisljakrizovi vyklyky [Sovereign policy and information security of Ukraine: post-crisis wiki]. *Visnyk Lvivs'koj komertsijnoj akademii. Serija ekonomichna – Bulletin of the Lviv Commercial Academy. The series is economical*, Vol. 46, pp. 28–32 [in Ukrainian].
2. Il'nyts'ka U. (2016). Informatsijna bezpeka Ukrainy: suchasni vyklyky, zahrozy ta mekhanizmy protydii nehatyvnyim informatsijno-psykholohichnym vplyvam [Information security of Ukraine: modern challenges, threats and countermeasures against negative informational and psychological influences]. *Politychni nauky – Political sciences*, 2(1), pp. 27–32 [in Ukrainian].
3. Kukin I.V. (2020). Kompleksnyj mekhanizm public'noho upravlinnia informatsijnoju bezpekoju osobystosti u sferi natsional'noi bezpeky ta ii prykor-donnomu sektori [A comprehensive mechanism of public management of information security of an individual in the sphere of national security and its border sector]. *Publichne upravlinnia ta mytne administruvannia – Public administration and customs administration*, 4 (27), pp. 134–139 [in Ukrainian].
4. Olijnyk O.V. (2012). Administratyvno-pravovi zasady informatsijnoj bezpeky [Administrative and

- legal principles of information security]. *Yevropejs'ki perspektyvy – European perspectives*, 4(1), pp. 65–68 [in Ukrainian].
5. Panchenko O.A. (2020). *Derzhavne upravlinnia informatsijnoi bezpekoiu v turbulentnomu suspil'stvi*. [State management of information security in a turbulent society]. *World Science*, 5(57), Vol. 3, pp. 4-9 [in Ukrainian].
 6. Panchenko O.A. (2011). *Ynformatsyonnaia bezopasnost' lychnosti: monohrafiia*. [Information security of a person: monograph] / O.A. Panchenko, N.V. Banchuk. K.: KYT, 2011, 672 p. [in Ukrainian].
 7. Panchenko O.A., Kabantseva A.V., Serdiuk I.A. (2020). *Potreby osobystosti na informatsijnu bezpeku*. [Personal needs for information security]. *Publichne uriaduvannia – Public administration*, 3(23), pp. 203–214 [in Ukrainian].
 8. Petryk V.M. (2015). *Zabezpechennia informatsijnoi bezpeky derzhavy: pidruchnyk*. [Ensuring information security of the state: a textbook]; za zah. red. O.A. Semchenka ta V.M. Petryka. Kyiv: DNU «Knyzhkova palata Ukrainy», 672 p. [in Ukrainian].
 9. Stepanov V.Yu. (2016). *Informatsijna bezpeka v informatsijnij sferi derzhavnoho upravlinnia*. [Information security in the information sphere of public administration]. *Teoriia ta praktyka derzhavnoho upravlinnia – Theory and practice of public administration*, 4(55), pp. 24-28 [in Ukrainian].
 10. Ukaz Prezydenta Ukrainy Pro rishennia Rady natsional'noi bezpeky i oborony Ukrainy vid 15 zhovtnia 2021 roku «Pro Stratehiiu informatsijnoi bezpeky» vid 28.12.2021 № 685/2021. [Decree of the President of Ukraine On the decision of the National Security and Defense Council of Ukraine dated October 15, 2021 "On Information Security Strategy" dated December 28, 2021 No. 685/2021]. Retrieved from <https://zakon.rada.gov.ua/laws/show/23/2023#Text> [in Ukrainian].
 11. Shyshkina Kh.Yu., Khvorost M.Yu. (2013). *Informatsijna bezpeka osobystosti iak peredumova zberzhennia psykhičnoho zdorov'ia*. [Information security of the individual as a prerequisite for maintaining mental health]. *Problemy ekstremal'noi ta kryzovoi psykholohii – Problems of extreme and crisis psychology*, Vol. 14, Part IV, pp. 246-253 [in Ukrainian].