УДК 351
DOI https://doi.org/10.32689/2523-4625-2022-2(62)-23

Ярослав ЧМИР
доктор філософії в галузі публічного управління, докторант кафедри публічного адміністрування, Міжрегіональна Академія управління персоналом, вул. Фрометівська, 2, Київ, Україна, 03039
ORCID: 0000-0002-4476-6687

Yaroslav CHMYR
Doctoral Student at the Department of Public Administration, Interregional Academy of Personnel Management, Frometivska str., 2, Kyiv, Ukraine, 03039
ORCID: 0000-0002-4476-6687

СУЧАСНІ ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ ТА ПЕРСПЕКТИВНІ НАПРЯМИ ЇХ ВИРІШЕННЯ

CURRENT PROBLEMS OF INFORMATION SECURITY IN UKRAINE AND PROSPECTIVE DIRECTIONS FOR THEIR SOLUTION

У статті досліджено проблеми, які заважають повній інформаційній безпеці нашої держави. Автором визначено, що до них належать: відсутність чіткості під час проведення державної політики у сфері формування українського інформаційного простору; недостатній розвиток національної інформаційної інфраструктури; нехватка інституцій, які комплексно забезпечуватимуть систему інформаційної безпеки в державному управлінні; формування інноваційних інформаційних небезпек, які потребують негайного та ефективного вирішення; відсталість вітчизняних інформаційних технологій. Автором наголошено, що натепер однією з головних проблем забезпечення інформаційної безпеки України є інформаційна експансія, необ'єктивне та неупереджене висвітлення фактів та явищ з боку Російської Федерації. Автором зазначено, що пріоритетними напрямами державної інформаційної політики мають бути: інтеграція України до глобального та регіонального європейського інформаційного простору; створення власної національної моделі інформаційного простору та забезпечення розвитку інформаційного суспільства; модернізація всієї системи інформаційної безпеки держави та формування і реалізація ефективної інформаційної політики; удосконалення законодавства з питань інформаційної безпеки.

Мета роботи. *Метою написання статті є комплексне обґрунтування та проведення аналізу проблем інформаційної безпеки України та виділення перспективних напрямів щодо їх вирішення.*

Методологія. *У запропонованій статті визначено, що, на відміну від державних органів влади, органи місцевого самоврядування піддаються більшому ризику. Адже під загрозою є найважливіша інформація, яка належить місцевим органам, зокрема: іпотечні документи, записи про минулі злочини, народження, смерть, медичне страхування, а також доступ до інформації про військовослужбовців та іншої конфіденційної інформації.*

Наукова новизна. *Доведено, що в епоху інформаційного суспільства необхідно адаптуватися до всіх інновацій у сфері інформаційних технологій. І під час створення новітніх технологій розробляти засоби захисту від організацій, що становлять загрозу інформаційній безпеці України.*

Висновки. *Підкреслено, що у сучасних умовах інформаційних протистоянь, експансіоністської політики Російської Федерації національний інформаційний простір України не є належним чином захищеним від зовнішніх негативних пропагандистських інформаційно-психологічних впливів та загроз. Наголошено на тому, що нині захист інформаційного суверенітету, створення потужної та ефективної системи інформаційної безпеки в Україні, розробка ефективних стратегій і тактик протидії медійним загрозам мають бути пріоритетними завданнями органів влади державних і недержавних інституцій.*

Ключові слова: *державне управління, проблеми інформаційної безпеки, виклики та загрози, ефективний захист, інформаційний простір.*

The article examines the problems that hinder the complete information security of our state. The author determined that they include: lack of clarity during the implementation of state policy in the field of formation of the Ukrainian information space; insufficient development of the national information infrastructure; lack of institutions that will comprehensively provide a system of information security in the state administration; formation of innovative informational dangers that require immediate and effective solution; backwardness of domestic information technologies. The author emphasized that today one of the main problems of ensuring information security of Ukraine is information expansion, unbiased and unbiased coverage of facts and phenomena on the part of the Russian Federation. The author states that the priority directions of the state information policy should be: Ukraine's integration into the global and regional European information space; creation of its own national model of the information space and ensuring the development of the information society; modernization of the entire state information security system and formation and implementation of an effective information policy; improvement of information security legislation.

The goal of the work. *The purpose of writing the article is a comprehensive justification and analysis of the information security problems of Ukraine and the selection of promising directions for their solution.*

Methodology. *In the proposed article, it is determined that, unlike state authorities, local self-government bodies are exposed to greater risk. After all, the most important information that belongs to local authorities is at risk, in particular: mortgage documents, records of past crimes, births, deaths, health insurance, as well as access to information about military personnel and other confidential information.*

Scientific novelty. *It is noted that the problem of information security in the system of state and local administration will exist for many years, or even forever. It has been proven that in the era of the information society it is necessary to adapt to all innovations in the field of information technologies. And during the creation of the latest technologies, develop means of protection against organizations that pose a threat to the information security of Ukraine.*

Conclusions. *It is emphasized that in the modern conditions of information confrontations, expansionist policy of the Russian Federation, the national information space of Ukraine is not adequately protected from external negative propaganda informational and psychological influences and threats. It was emphasized that currently the protection of information sovereignty, the creation of a powerful and effective system of information security in Ukraine, the development of effective strategies and tactics for countering media threats should be the priority tasks of the authorities of state and non-state institutions.*

Key words: *public administration, information security problems, challenges and threats, effective protection, information space.*

Вступ. Проблема захисту інформаційного простору в умовах формування сучасного інформаційного суспільства є основою поліпшення соціальної структуризації суспільства на постіндустріальному етапі. Інформація являє собою основу безпечного та оптимального розвитку сучасного інформаційного суспільства. Водночас інформація може служити зброєю, що впливає на світогляд людини, населення, виробляє негативне ставлення до певних явищ, до держави та суспільства загалом, спотворює факти та події, що впливають на якість та результативність сучасних реформ у суспільстві.

Водночас слід додати, що нині інформаційна безпека відіграє одну з ключових ролей у забезпеченні життєво важливих інтересів країни та суспільства. Вказане зумовлене швидким розвитком сучасних інформаційно-телекомунікаційних технологій, засобів зв'язку та інформатизації і, як наслідок, суттєвим зростанням впливу інформаційної сфери на життя нашого суспільства.

Аналіз останніх публікацій за проблематикою. Вагомий внесок у розвиток теоретичних засад проблем управління інформаційною безпекою держави зробили такі вчені, як: В. Антонов, В. Бурячок, П. Гаранюк, В. Демиденко, О. Зозуля, Ю. Лісовська, А. Нашинець-Наумова, О. Панченко, А. Платоненко, В. Толубко, Ю. Ткач, Я. Чмир та інші. Проте можна сказати, що це питання вивчено не досить.

Інформаційні технології у діяльності державних органів. Нині розвиток інформаційних технологій охоплює багато сфер життя кожної людини. Не стало винятком використання інноваційних технологій у державних органах України. Попит на використання інформаційних технологій у державному управлінні, бізнесі та багатьох інших сферах зростає з кожним днем і демонструє як позитивні, так і негативні фактори. Так, своєю чергою дослідник П. Гаранюк до позитивних факторів використання інформаційних технологій у діяльності державних органів відносить:

– підвищення якості державного обслуговування громадян України;

– збільшення оперативності за рахунок скорочення тимчасових витрат на отримання запитів, оповіщення громадян та інше;

– забезпечення гласності діяльності органів державної влади;

– створення електронного документообігу.

Дослідник також додає, що після впровадження інформаційних технологій в державне управління підвищилася якість державних послуг населенню країни, зросла ефективність апарату загалом тощо [3, с. 176].

Проте варто констатувати, що, крім позитивних факторів, у будь-якій сфері діяльності існують і негативні, які є незворотними, якщо їх негайно не усунути. Слід додати, що в ході аналізу стану інформаційної безпеки в Україні та визначення основних проблем у цій сфері необхідно враховувати політичні, соціально-економічні, організаційні та технічні фактори, які безпосередньо впливають на безпеку нашої країни.

Отже, якщо говорити про реалізацію інформаційних загроз на індивідуальному рівні, то можна сказати, що вона призводить до порушення або обмеження доступу громадян до публічної інформації. Це своєю чергою створює загрозу інформаційній безпеці особи як з боку влади, так і з боку сторонніх осіб чи груп, порушує баланс у взаєминах особи із суспільством та державою.

Варто погодитись із думкою вченого А. Платоненка, який вважає, що наслідком впливу інформаційних загроз на соціальну спільність є ускладнення загальних процесів, що виявляється в наростанні протиріч між різними соціальними верствами, посиленні

політичної боротьби, розпалюванні релігійних та етнічних протиріч, зниженні загальної культури населення, зростанні злочинності та поширенні антигуманних ідей. Вчений також наголошує, що вплив інформаційних загроз на органи державної влади, які відповідальні за підготовку та прийняття рішень, реалізація яких безпосередньо впливає на безпеку, може сприяти виникненню надзвичайних ситуацій у державі та суспільстві, значним збиткам через порушення функціонування систем зв'язку, контролю та управління, витік інформації, що містить державну таємницю [15, с. 88].

Доцільно відзначити, що, як вважає Я. Чмир, інформаційна безпека у системі державного управління є складником національної безпеки України, вона забезпечує захист системи державного управління від інформаційно-комунікаційних викликів і загроз, водночас сама система державного управління забезпечує суспільство, державу та громадян інформаційно-відмінними послугами та високоякісною інформацією [18].

Проблеми забезпечення інформаційної безпеки у системі державного управління.

На нашу думку, реальними загрозами національним інтересам та національній безпеці України в інформаційній сфері є:

– проведення спеціальних інформаційних операцій, спрямованих на диверсію обороноздатності, деморалізацію особового складу Збройних сил України та інших військових формувань, провокування екстремістських проявів, панічні настрої, загострення та дестабілізацію суспільно-політичної та соціально-економічної ситуації, розпалювання міжетнічних та міжконфесійних конфліктів в Україні;

– недостатній розвиток національної інформаційної інфраструктури [17], що обмежує перспективи України ефективно протистояти інформаційній агресії та діяти активно в інформаційній сфері для реалізації національних інтересів нашої держави;

– неефективність державної інформаційної політики, недосконаліть законодавства щодо регулювання суспільних відносин в інформаційній сфері, недостатній рівень медіакультури нашого суспільства;

– поширення звернень до радикалів дії, пропаганда ізоляціоністських та автономістських концепцій регіонального співіснування в Україні [18].

Цікавою також є думка вченої Ю. Ткач, яка вважає, що головними проблемами надання інформаційної безпеки у системі державного управління є:

по-перше, забезпечення ефективного функціонування механізму електронної системи управління, що нині не функціонує;

по-друге, формування інноваційних інформаційних небезпек, які потребують негайного та ефективного вирішення;

по-третє, забезпечення підготовки якісних кадрів у системі державного управління у сфері інформаційної безпеки;

по-четверте, відсутність ефективних механізмів захисту інформації;

по-п'яте, нехватка інституцій, які комплексно забезпечуватимуть систему інформаційної безпеки в державному управлінні [11, с. 275].

Заслуговує на увагу також думка дослідниці А. Малєєвої, яка, аналізуючи сучасний стан інформаційної безпеки, наголошує, що її рівень неповною мірою відповідає вимогам часу. Є проблеми, які серйозно заважають повній інформаційній безпеці людини, суспільства та держави. Вчена до основних проблем у цій сфері видносить такі як:

– відсутність чіткості під час проведення державної політики у сфері формування українського інформаційного простору;

– недостатня державна підтримка діяльності інформаційних агентств України із просування своєї продукції на зовнішній інформаційний ринок;

– непокращенняя ситуації із забезпеченням збереження відомостей, що становлять державну таємницю;

– відсталість вітчизняних інформаційних технологій [14].

Своєю чергою вчена А. Нашинець-Наумова вважає, що нині основною проблемою у зазначеній сфері є непослідовність і нерозвиненість правового регулювання суспільних відносин у сфері інформації, що ускладнює дотримання необхідного балансу особистих, суспільних і державних інтересів у цій сфері. Недосконале правове регулювання не дає можливості завершити формування конкурентоспроможних українських інформаційних агентств і ЗМІ на території України [12, с. 154].

Окремо доцільно наголосити, що на сьогодні однією з головних проблем забезпечення інформаційної безпеки України є інформаційна експансія, необ'єктивне та неупереджене висвітлення фактів та явищ з боку Російської Федерації. Технології російських інформаційно-психологічних операцій налаштовані на забезпечення домінування в українському інформаційному просторі та на утримання медійної переваги. Через російські пропагандистські акції та медійні події

відбувається вплив не лише на суспільну свідомість громадян України, а й на світову спільноту.

Так, в інтерв'ю для сайту Реформи державного управління Голова Держспецзв'язку Юрій Щиголя зазначив, що нині російські військові хакери в кіберпросторі роблять те саме, що й їхні «колеги» на землі. Вони намагаються зруйнувати все, чого можуть досягти, створити хаос, дестабілізувати уряд, залякати населення, спричинити гуманітарну катастрофу та позбавити людей доступу до життєво важливих послуг [7].

Тому атакують вони все: від органів влади та сектору безпеки й оборони – до локальних провайдерів і просто цивільних громадян. Юрій Щиголя також зауважує, що критична інфраструктура піддається найбільшій атаці. Голова підкреслює, що останнім часом спостерігається надзвичайно велика кількість кібератак, спрямованих на гуманітарну катастрофу в Україні: атакується логістичний сектор, кілька днів не працює сайт і пошта Державної служби з надзвичайних ситуацій. Таким чином, росіяни намагаються використати будь-яку можливість, щоб нашкодити Україні. До найпоширеніших типів кібератак Юрій відносить: фішингові листи та електронні листи зі шкідливим програмним забезпеченням. Голова зауважує, що під час поширення фішингових листів росіяни намагаються викрасти облікові дані, а потім використовувати їх для атак, спрямованих на знищення інформаційних систем [7].

Принципи державної політики забезпечення інформаційної безпеки.

Незважаючи на сучасні загрози, варто відзначити, що державні органи влади останніми роками сформували ефективну систему управління інформаційною безпекою в нашій країні. Доцільно погодитись із думкою вченого В. Петрика, який під системою управління інформаційною безпекою розуміє цілий комплекс дій, що здійснюються в державній установі, які спрямовані на досягнення відповідних рівнів конфіденційності, цілісності та доступності інформації [8, с. 251]. Вчений відзначає, що як організаційна основа системи забезпечення інформаційної безпеки фундаментальну роль відіграють принципи державної політики забезпечення інформаційної безпеки, до принципів учений відносить:

– принцип відкритості під час виконання функцій органів державної влади та громадських об'єднань, що передбачає інформування громадськості про їхню діяльність з урахуванням встановлених обмежень законодавства України в цій сфері;

– принцип правової рівності всіх учасників процесу інформаційної взаємодії, гарантії їх політичного, соціального та економічного статусу, заснованого на конституційному праві громадян вільно шукати, отримувати, передавати, виробляти інформацію та поширювати будь-яким законним способом;

– принцип пріоритетного розвитку сучасних інформаційних і телекомунікаційних технологій нашої країни, що сприяють збереженню державної телекомунікаційної мережі, їх підключенню до глобальної інформаційної мережі відповідно до всіх інтересів України [8, с. 258].

Необхідно загострити свою увагу на тому, що зараз у сфері інформаційної безпеки працює ціла система державних органів. Ця система складається з департаментів, міністерств, комісій тощо, найважливішими з них слід вважати:

– Міністерство інформаційної політики України;

– Департамент контррозвідувального захисту інтересів держави у сфері інформаційної безпеки СБУ;

– Міжвідомчу комісію з питань інформаційної політики та інформаційної безпеки при Раді національної безпеки і оборони України [9, с. 356].

Варто підкреслити, що дослідник О. Панченко наголошує, що, на відміну від державних органів влади, органи місцевого самоврядування піддаються більшому ризику. Адже під загрозою є найважливіша інформація, яка належить місцевим органам. Дослідник вважає, що до такої інформації слід віднести: іпотечні документи, записи про минулі злочини, народження, смерть, медичне страхування, а також доступ до інформації про військовослужбовців та іншої конфіденційної інформації [13].

Так, своєю чергою вчений В. Демиденко до основних причин, які негативно впливають на створення ефективної системи захисту інформації в органах місцевого самоврядування, відносить:

– ігнорування місцевими органами нормативних вимог;

– відсутність тісної взаємодії з іншими департаментами для забезпечення єдиної інфраструктури інформаційної безпеки в муніципалітеті;

– несумлінне ставлення службовців, що призводить до зниження якості та безпеки;

– відсутність бюджету для створення ефективної, працездатної програмної платформи;

– призначення некваліфікованого службовця у сфері інформаційної безпеки [2, с. 151].

У результаті вищевикладеного слід зазначити, що проблема інформаційної безпеки у системі державного та місцевого управління буде існувати багато років, а то й вічно. В епоху інформаційного суспільства необхідно адаптуватися до всіх інновацій у сфері інформаційних технологій. І під час створення новітніх технологій розробляти засоби захисту від організацій, що становлять загрозу інформаційній безпеці.

Висновки. Отже, можна сказати, що у сучасних умовах інформаційних протистоянь, експансіоністської політики Російської Федерації національний інформаційний простір України не є належним чином захищеним від зовнішніх негативних пропагандистських інформаційно-психологічних впливів та загроз. Тому слід наголосити, що нині захист інформаційного суверенітету, створення потужної та ефективної системи інформаційної безпеки в Україні, розробка ефективних стратегій і тактик протидії медійним загрозам мають бути пріоритетними завданнями органів влади державних і недержавних інституцій.

Література:

1. Бурячок В.Л., Гулак Г.М., Толубко В.Б. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби : підручник. Київ : ТОВ «СІК ГРУП Україна», 2015. 449 с.

2. Демиденко В.О. Принципи застосування органами місцевого самоврядування законодавства України у сфері кібербезпеки. *Юридичний часопис НАВС.* 2018. № 1. С. 141–153.

3. Дудикевич В.Б., Опірський І.Р., Гаранюк П.І., Зачепило В.С., Партика А.І. Забезпечення інформаційної безпеки держави : навчальний посібник. Львів : Видавництво Львівської політехніки, 2017. 204 с.

4. Закон України «Про національну безпеку України» від 15 червня 2022 р., № 1882-IX. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text.

5. Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» від 09 січня 2007 р. № 537-V. URL: https://zakon.rada.gov.ua/laws/show/537-16#Text.

6. Зозуля О.С. Періодизація розбудови системи державного управління забезпеченням інформаційної безпеки України. *Інвестиції: практика та досвід.* Київ, 2016. № 8. С. 106–114.

7. Інтерв'ю Голови Держспецзв'язку Юрія Щиголя для сайту Реформи державного управління, 9.05.2022. URL: https://www.kmu.gov.ua/news/intervyu-golovi-derzhspeczvyazku-yuriya-shchigolya-dlya-sajtu-reformi-derzhavnogo-upravlinnya-9052022.

8. Інформаційна безпека держави : підручник: в 2 т. Т. 1. / В.М. Петрик та ін. ; за заг. ред. В.В. Остроухова. Київ : ДНУ «Книжкова палата України», 2016. 264 с.

9. Інформаційна безпека : підручник / В.В. Остроухов, М.М. Присяжнюк, О.І. Фармагей, М.М. Чеховська та ін. ; під ред. В.В. Остроухова. Київ : Видавництво Ліра-К, 2021. 412 с.

10. Лісовська Ю.П. Інформаційна безпека України : навчальний посібник. Київ : Кондор, 2018. 172 с.

11. Мехед Д.Б., Базилевич В.М., Ткач Ю.М., Петренко Т.А. Аналіз загроз інформаційної безпеки в мережах стандарту IEEE 802.11. *Захист інформації.* Київ, 2015. Т. 17, № 4. С. 274–278.

12. Нашинець-Наумова А.Ю. Інформаційна безпека: питання правового регулювання : монографія. Київ : Гельветика, 2017. 168 с.

13. Панченко О.А. Інформаційна безпека в контексті викликів і загроз національній безпеці. *Державне управління та місцеве самоврядування*. 2020. Вип. 2(45).

14. Панченко О.А., Антонов В.Г., Малєєва А.М. Державне управління інформаційною безпекою як запорука особистісного благополуччя. *Вчені записки ТНУ імені В.І. Вернадського. Серія «Державне управління»*. Том 31 (70). № 4. 2020.

15. Платоненко А.В. Сучасні загрози інформаційної безпеки для державних та приватних установ України. *Сучасний захист інформації*. 2015. № 4. С. 86–90.

16. Указ Президента України «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.

17. Семенець-Орлова І.А. Державне управління освітніми змінами в Україні: теоретичні засади : монографія. Київ : ЮСТОН, 2018. 420 с.

18. Чмир Я.І. Проблеми забезпечення інформаційної безпеки у системі публічного управління. *Аспекти публічного правління.* Том 6. № 9. 2018.

References:

1. Buriachok V.L., Hulak H.M., Tolubko V.B. Informatsiinyi ta kiberprostory: problemy bezpeky, metody ta zasoby borotby: pidruchnyk. Kyiv: TOV "SIK HRUP Ukraina", 2015. 449 s.

2. Demydenko V.O. Pryntsypy zastosuvannia orhanamy mistsevoho samovriaduvannia zakonodavstva Ukrainy v sferi kiberbezpeky. *Yurydychnyi chasopys NAVS.* 2018. No. 1. S. 141–153.

3. Dudykevych V.B., Opirskyi I.R., Haraniuk P.I., Zachepylo V.S., Partyka A.I. Zabezpechennia informatsiinoi bezpeky derzhavy: navchalnyi posibnyk. Lviv: Vydavnytstvo Lvivskoi politekhniky, 2017. 204 s.

4. Zakon Ukrainy "Pro natsionalnu bezpeku Ukrainy" vid 15 chervnia 2022 r., No. 1882-IX. Retrieved from: https://zakon.rada.gov.ua/laws/show/2469-19#Text.

5. Zakon Ukrainy "Pro Osnovni zasady rozvytku informatsiinoho suspilstva v Ukraini na 2007–2015 roky" vid 09 sichnia 2007 r. No. 537-V. Retrieved from: https://zakon.rada.gov.ua/laws/show/537-16#Text.

6. Zozulia O.S. Periodyzatsiia rozbudovy systemy derzhavnoho upravlinnia zabezpechenniam informatsiinoi bezpeky Ukrainy. *Investytsii: praktyka ta dosvid*. Kyiv, 2016. No. 8. S. 106–114.

7. Interviu Holovy Derzhspetszviazku Yuriia Shchyholia dlia saitu Reformy derzhavnoho upravlinnia, 9.05.2022. Retrieved from: https://www.kmu.gov.ua/news/intervyu-golovi-derzhspeczvyazku-yuriya-shchigolya-dlya-sajtu-reformi-derzhavnogo-upravlinnya-9052022.

8. Informatsiina bezpeka derzhavy: pidruchnyk: v 2 t. T. 1. / V.M. Petryk ta in.; za zah. red. V.V. Ostroukhova. Kyiv: DNU "Knyzhkova palata Ukrainy", 2016. 264 s.

9. Informatsiina bezpeka: pidruchnyk / V.V. Ostroukhov, M.M. Prysiazhniuk, O.I. Farmahei, M.M. Chekhovska ta in.; pid red. V.V. Ostroukhova. Kyiv: Vydavnytstvo Lira-K, 2021. 412 s.

10. Lisovska Yu.P. Informatsiina bezpeka Ukrainy: navchalnyi posibnyk. Kyiv: Kondor, 2018. 172 s.

11. Mekhed D.B., Bazylevych V.M., Tkach Yu.M., Petrenko T.A. Analiz zahroz informatsiinoi bezpeky v merezhakh standartu IEEE 802.11. *Zakhyst informatsii.* Kyiv, 2015. T. 17, No. 4. S. 274–278.

12. Nashynets-Naumova A.Yu. Informatsiina bezpeka: pytannia pravovoho rehuliuvannia: monohrafiia. Kyiv: Helvetyka, 2017. 168 s.

13. Panchenko O.A. Informatsiina bezpeka v konteksti vyklykiv i zahroz natsionalnii bezpetsi. *Derzhavne upravlinnia ta mistseve samovriaduvannia*, 2020, Vyp. 2(45).

14. Panchenko O.A., Antonov V.H, Malieieva A.M. Derzhavne upravlinnia informatsiinoiu bezpekoiu yak zaporuka osobystisnoho blahopoluchchia. *Vcheni zapysky TNU imeni V.I. Vernadskoho. Seriia: Derzhavne upravlinnia.* Tom 31 (70). No. 4. 2020.

15. Platonenko A.V. Suchasni zahrozy informatsiinoi bezpeky dlia derzhavnykh ta pryvatnykh ustanov Ukrainy. *Suchasnyi zakhyst informatsii*. 2015. No. 4. S. 86–90.

16. Ukaz Prezydenta Ukrainy "Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 15 zhovtnia 2021 roku "Pro Stratehiiu informatsiinoi bezpeky". Retrieved from: https://zakon.rada.gov.ua/laws/show/685/2021#Text.

17. Semenets-Orlova I.A. Derzhavne upravlinnia osvitnimy zminamy v Ukraini: teoretychni zasady [State management of educational changes in Ukraine: theoretical principles]. 2018. Kyiv: YuSTON [in Ukrainian].

18. Chmyr Ya.I. Problemy zabezpechennia informatsiinoi bezpeky v systemi publichnoho upravlinnia. *Aspekty publichnoho pravlinnia.* Tom 6. No. 9. 2018.