Національний технічний університет
«Дніпровська політехніка»

ПУБЛІЧНЕ УПРАВЛІННЯ ТА МІСЦЕВЕ САМОВРЯДУВАННЯ

Випуск 2

Видавничий дім
«Гельветика»
2024

Реєстрація суб'єкта у сфері друкованих медіа: Рішення Національної ради України з питань телебачення і радіомовлення № 865 від 21.03.2024 року

Наказом МОН України № 886 від 2 липня 2020 року (додаток № 4) журнал включено до категорії «Б» Переліку наукових фахових видань України зі спеціальності 281 – Публічне управління та адміністрування.

Журнал до 20.07.2022 р. мав назву «Державне управління та місцеве самоврядування».

Відповідні зміни внесено до Переліку наукових фахових видань України:
Наказ МОН України від 10.10.2022 р. № 894 (додаток № 2).

Журнал ухвалено до друку Вченою радою Національного технічного університету «Дніпровська політехніка» 20.06.2024 р., протокол № 7

Офіційний сайт видання: *www.journals.politehnica.dp.ua/index.php/public*

Статті у виданні перевірені на наявність плагіату за допомогою програмного забезпечення StrikePlagiarism.com від польської компанії Plagiat.pl.

ISSN (print): 2414-4436

УДК 351
DOI https://doi.org/10.32782/2414-4436/2024-2-10

Надія ТРЕТЯК
Науковий співробітник науково-дослідної лабораторії проблем управління проектами інформації Науково-дослідного відділу проблем ведення та впровадження проектів інформатизації науково-дослідного управління проблем розвитку інформаційних технологій та впровадження проектів інформатизації Збройних Сил України центру воєнно-стратегічних досліджень Національного університету оборони України (Київ, Україна), e-mail: 0962064464@gmail.com.ua
***ORCID:** 0009-0004-1340-7878*

Бібліографічний опис статті: Третяк, Н. (2024). Публічно-управлінські аспекти впровадження та супроводу інформаційних систем у Міністерстві оборони України: нормативні основи НАТО. *Публічне управління та місцеве самоврядування,* (2), 70–76, doi: https://doi.org/10.32782/2414-4436/2024-2-10

ПУБЛІЧНО-УПРАВЛІНСЬКІ АСПЕКТИ ВПРОВАДЖЕННЯ ТА СУПРОВОДУ ІНФОРМАЦІЙНИХ СИСТЕМ У МІНІСТЕРСТВІ ОБОРОНИ УКРАЇНИ: НОРМАТИВНІ ОСНОВИ НАТО

Актуальність. Стаття присвячена аналізу публічно-управлінських аспектів впровадження та супроводу інформаційних систем у Міністерстві оборони України з урахуванням нормативних основ НАТО. У роботі детально розглянуто процеси інтеграції міжнародних стандартів безпеки в національну систему управління оборонними інформаційними системами. Автори досліджують ключові виклики, пов'язані з адаптацією нормативно-правової бази України до стандартів НАТО, зокрема в сфері інформаційної безпеки та кібербезпеки.

Результат. У статті визначено основні публічно-управлінські аспекти, які включають інституційну адаптацію та відповідність стандартам НАТО, вдосконалення системи управління ризиками, стандартизацію та уніфікацію інформаційних систем, забезпечення конфіденційності, цілісності та доступності інформації, а також координацію та співпрацю з міжнародними партнерами. Окрему увагу приділено питанням підвищення компетенцій персоналу, проведення регулярних аудитів та моніторингу ефективності впроваджених стандартів. У результаті дослідження було доведено, що ефективна інтеграція міжнародних стандартів безпеки в управлінські процеси Міністерства оборони України є критично важливою для зміцнення національної кібербезпеки та підвищення боєздатності військових підрозділів. Стаття також підкреслює важливість систематичної роботи з удосконалення управлінських процесів, регулярного перегляду та оновлення нормативної бази, а також залучення міжнародного досвіду для забезпечення ефективного захисту інформаційних активів. Автор зробив висновок, що інтеграція з міжнародними стандартами безпеки не тільки покращує захист інформаційних систем, але й сприяє підвищенню рівня взаємосумісності та співпраці між Україною та її міжнародними партнерами. Рекомендації, розроблені у статті, спрямовані на вдосконалення управлінських процесів, забезпечення прозорості та підвищення ефективності роботи Міністерства оборони України в контексті інтеграції з міжнародними стандартами безпеки.

***Ключові слова:** публічне управління, інформаційні системи, кібербезпека, стандарти НАТО, Міністерство оборони України, інтеграція, управління ризиками, міжнародні стандарти, аудит інформаційної безпеки.*

Nadiia TRETIAK
Scientific Researcher at the Information Project Management Research Laboratory of the Information Management Research Department of the Information Technology Development and Implementation Projects of the Research Department of Information Technology Development and Implementation Projects of the Armed Forces of Ukraine of the Centre for Military Strategic Studies at the National Defence University of Ukraine (Kyiv, Ukraine), e-mail: 0962064464@gmail.com.ua
***ORCID:** 0009-0004-1340-7878*

To cite this article: Tretiak, N. (2024). Publichno-upravlinski aspekty vprovadzhennia ta suprovodu informatsiinykh system u Ministerstvi oborony Ukrainy: normatyvni osnovy NATO [Public administration aspects of implementation and support of information systems in the Ministry of Defence of Ukraine: NATO normative framework]*. Public Administration and Local Self-Government,* 2, 70–76, doi: https://doi.org/10.32782/2414-4436/2024-2-10

PUBLIC ADMINISTRATION ASPECTS OF IMPLEMENTATION AND SUPPORT OF INFORMATION SYSTEMS IN THE MINISTRY OF DEFENCE OF UKRAINE: NATO NORMATIVE FRAMEWORK

Relevance. The article is dedicated to the analysis of public administration aspects of the implementation and support of information systems within the Ministry of Defense of Ukraine, considering the normative foundations of NATO. The paper thoroughly examines the processes of integrating international security standards into the national management system of defense information systems. The authors explore the key challenges associated with adapting Ukraine's regulatory framework to NATO standards, particularly in the fields of information security and cybersecurity.

Results. The article identifies the main public administration aspects, including institutional adaptation and compliance with NATO standards, enhancement of risk management systems, standardization and unification of information systems, ensuring confidentiality, integrity, and availability of information, as well as coordination and cooperation with international partners. Special attention is given to the issues of personnel competency development, regular audits, and monitoring the effectiveness of the implemented standards. The research demonstrates that the effective integration of international security standards into the management processes of the Ministry of Defense of Ukraine is critically important for strengthening national cybersecurity and enhancing the combat readiness of military units. The article also emphasizes the importance of systematic work on improving management processes, regular review and updating of the regulatory framework, and leveraging international experience to ensure effective protection of information assets. The author concludes that integration with international security standards not only improves the protection of information systems but also contributes to increasing the level of interoperability and cooperation between Ukraine and its international partners. The recommendations developed in the article are aimed at improving management processes, ensuring transparency, and enhancing the efficiency of the Ministry of Defense of Ukraine in the context of integration with international security standards.

***Key words:** public administration, information systems, cybersecurity, NATO standards, Ministry of Defense of Ukraine, integration, risk management, international standards, information security audit.*

Постановка проблеми. У сучасному світі, де інформаційні технології відіграють ключову роль у забезпеченні національної безпеки, особливе значення набувають питання впровадження та супроводу інформаційних систем у структурах, що відповідають за оборону країни. Міністерство оборони України (далі – Міноборони), як один із основних органів, відповідальних за захист національних інтересів, активно залучає новітні технології для підвищення ефективності військового управління та оперативного реагування на загрози. Водночас, інтеграція України у міжнародні безпекові структури, зокрема НАТО, вимагає від держави не лише розвитку власних технологічних спроможностей, але й узгодження їх із загальновизнаними міжнародними стандартами.

Нормативні основи НАТО відіграють важливу роль у гармонізації публічно-управлінських процесів в Україні, зокрема в контексті впровадження інформаційних систем у Міноборони. Такі стандарти не лише встановлюють чіткі вимоги до функціонування систем, але й регулюють їхній життєвий цикл від початкового планування до технічного обслуговування та оновлення. На сьогодні існує потреба у визначенні та аналізі бар'єрів, що заважають ефективній інтеграції національних систем з міжнародними стандартами, а також у розробці рекомендацій щодо підвищення ефективності управління цими процесами в умовах зростаючих викликів у сфері національної безпеки.

Аналіз останніх досліджень і публікацій. Сучасні українські вчені активно досліджують проблематику інформаційної зброї в контексті міждержавної боротьби, приділяючи особливу увагу її впливу на національну безпеку

та стратегії протидії в умовах гібридної війни. Вчені, які досліджували впровадження стандартів НАТО в український оборонний комплекс, включають С. Шептуховського, який працював над публічно-управлінськими аспектами впровадження та супроводу інформаційних систем у Міністерстві оборони України, а також таких дослідників, як Т. Дзюба, О. Акульшин, Ф. Флурі, Ю. Карін, О. Коваленко, О. Копитько, Є. Магда, С. Шаповалов, О. Бондаренко, О. Покальчук, Н. Іванова, О. Паливода, Н. Крапівіна, І. Абакіна, І. Радкович, І. Недужа, Г. Яворська, О. Снитко, О. Іванов, Н. Слухай, О. Леонов, О. Войтко, В. Рахімов, Н. Кудрявцева, Ю. Міхєєв, М. Павленко, О. Грищук, І. Латко, О. Критенко, С. Томашевський, Е. Шнурко-Табакова, В. Романюк, К. Левченко, О. Дунебабіна, Б. Потасова, В. Азарова, М. Кармазіна, В. Кацап, А. Хоперія, І. Аблазов, К. Рубель, Р. Трофименко, Б. Бакалюк, Л. Федоренко, С. Череватий, С. Карнаух, О. Заруба, А. Демченко, В. Пивоварова, А. Богданова, Л. Компанева, В. Легкоконець та Л. Снігур, які працювали над стратегічними комунікаціями держави в умовах війни.

Метою статті є аналіз публічно-управлінських аспектів впровадження та супроводу інформаційних систем у Міноборони України з урахуванням нормативних основ НАТО, а також розробка рекомендацій щодо вдосконалення управлінських процесів у контексті інтеграції з міжнародними стандартами безпеки.

Виклад основного матеріалу. У сучасних умовах зростання загроз кібербезпеці, зумовлених як глобальними тенденціями, так і агресивними діями з боку рф, необхідність у вдосконаленні інформаційних систем та посиленні заходів кіберзахисту стає особливо актуальною. Міноборони України, розуміючи критичну важливість захисту своїх інформаційно-комунікаційних систем, вживає рішучих кроків у цьому напрямку. Одним із таких кроків стало ухвалення важливого нормативного акту, який визначає основні засади забезпечення інформаційної безпеки та кібербезпеки в структурі міністерства.

У квіті 2024 року Міноборони України ухвалило нормативний акт, який затверджує основні засади інформаційної безпеки та кібербезпеки в інформаційно-комунікаційних системах, що використовуються в структурі міністерства. Цей наказ встановлює уніфіковані базові вимоги, які виступають як політика верхнього рівня, щодо захисту інформації та кіберзахисту у всіх системах Міноборони (Єдині стандарти кібербезпеки: Міноборони зміцнює захист інформаційних систем у відповідності до стандартів НАТО, 2024), (Зусилля НАТО з протидії дезінформації та охоплення російськомовної аудиторії. Рекомендації та кращі кейси реалізації стратегічних комунікацій в умовах війни : практичний довідник, 2023).

Згідно з цим наказом, усі інформаційні системи, сервіси, застосунки та цифрові інструменти Міноборони мають дотримуватися єдиних, чітко визначених правил та стандартів кібербезпеки. Ці вимоги розроблені з урахуванням найкращих підходів НАТО, міжнародних стандартів та передових практик у сфері інформаційної та кібербезпеки.

Зокрема, затверджені основні засади безпеки базуються на директиві НАТО з кібербезпеки (NATO Primary Directive on CIS Security) і відповідають підходам до управління ризиками, викладеним у NIST Risk Management Framework – це документ, який визначає політику, стандарти і вимоги для забезпечення безпеки інформаційних і комунікаційних систем (далі – CIS) у НАТО. CIS Security Directive охоплює заходи, які необхідні для захисту конфіденційності, цілісності та доступності інформації, що обробляється, передається або зберігається в межах систем НАТО.

Доцільно зазначити, що директива НАТО з кібербезпеки, офіційно відома як “NATO Primary Directive on CIS Security”, є ключовим документом, що визначає політику, стандарти та рекомендації щодо забезпечення кібербезпеки в інформаційних та комунікаційних системах (CIS) НАТО. Ця директива спрямована на захист конфіденційності, цілісності та доступності інформації, яка обробляється, зберігається та передається через інформаційні системи альянсу.

Отже, директива є фундаментом для країнчленів НАТО у забезпеченні надійного кіберзахисту їхніх інформаційних та комунікаційних систем, сприяючи зміцненню колективної безпеки альянсу.

Інформаційно-комунікаційні системи Міноборони України також відповідають міжнародним стандартам з інформаційної безпеки, таким як ДСТУ ISO\IEC 27001:2023 «Інформаційна безпека, кібербезпека та захист конфіденційності. Система управління інформаційною безпекою. Вимоги».

Доцільно підкреслити, що ДСТУ ISO/IEC 27001:2023 – це національний стандарт України, який є еквівалентом міжнародного стандарту ISO/IEC 27001:2022. Цей стандарт встановлює вимоги до створення, впровадження, експлуатації, моніторингу, підтримки та вдосконалення системи управління інформаційною безпекою в організації.

Основні аспекти стандарту ДСТУ ISO/IEC 27001:2023 включають:

1. Система управління інформаційною безпекою (далі – СУІБ):

− визначення політик, процесів та процедур, які допомагають організаціям захищати інформаційні активи, зокрема, забезпечувати конфіденційність, цілісність та доступність інформації;

− вимоги до документування та підтримки системи управління інформаційною безпекою.

2. Управління ризиками:

− процес ідентифікації, оцінки та управління ризиками, пов'язаними з інформаційною безпекою;

− впровадження заходів для мінімізації ризиків відповідно до результатів оцінки ризиків.

3. Контекст організації:

− визначення зовнішніх та внутрішніх факторів, які можуть впливати на інформаційну безпеку;

− визначення зацікавлених сторін та їхніх вимог щодо інформаційної безпеки.

4. Лідерство та відповідальність:

− вимоги до залучення керівництва організації до процесу управління інформаційною безпекою;

− визначення ролей і відповідальності у рамках СУІБ.

5. Планування та підтримка:

− визначення цілей з інформаційної безпеки, а також процесів для досягнення цих цілей;

− забезпечення ресурсів, необхідних для функціонування СУІБ, включаючи навчання персоналу та підвищення їхньої обізнаності.

6. Операційні процеси:

− впровадження заходів захисту інформації відповідно до встановлених вимог;

− моніторинг і контроль виконання заходів з інформаційної безпеки.

7. Оцінка результативності:

− моніторинг і вимірювання ефективності системи управління інформаційною безпекою;

− проведення внутрішніх аудитів і аналізу результативності СУІБ.

8. Покращення: процес постійного вдосконалення системи управління інформаційною безпекою, включаючи усунення виявлених невідповідностей і поліпшення заходів безпеки.

Отже, зазначений стандарт є критично важливим для організацій, які прагнуть забезпечити високий рівень захисту інформаційних активів, особливо в умовах зростаючих кіберзагроз. Він

Основні положення директиви "NATO Primary Directive on CIS Security"

№ з/п	Основні положення директиви	Короткий опис
1	Загальні вимоги	− забезпечення захисту інформаційних систем від кібератак та інших загроз; − встановлення чітких правил доступу до конфіденційної інформації; − впровадження заходів щодо виявлення, попередження та реагування на інциденти кібербезпеки.
2	Управління ризиками	− використання підходів ризик-менеджменту для оцінки та мінімізації ризиків, пов'язаних із кібербезпекою; − регулярне проведення оцінок вразливостей інформаційних систем та їхніх компонентів; − впровадження заходів для зменшення ризиків на основі результатів оцінок.
3	Технічні заходи	впровадження сучасних технологій шифрування для захисту даних; використання засобів автентифікації та авторизації для контролю доступу до систем; постійне оновлення та вдосконалення програмного забезпечення для запобігання кіберзагрозам.
4	Координація та співпраця	− координація дій між країнами-членами НАТО для забезпечення єдиного підходу до кібербезпеки; − обмін інформацією та найкращими практиками між країнами-членами щодо захисту від кіберзагроз; − спільні тренування та навчання для підвищення готовності до кіберінцидентів.
5	Аудит та відповідність	− проведення регулярних аудитів для забезпечення відповідності інформаційних систем вимогам директиви; − розробка планів дій для усунення виявлених недоліків та підвищення рівня кібербезпеки.

Розроблено автором на основі аналізу джерела (Про прийняття національних стандартів, зміни до національного стандарту та скасування національних стандартів, 2023; Стандарти НАТО: механізм і темпи впровадження, адаптація до українських реалій, 2021).

дозволяє структурувати підхід до інформаційної безпеки, забезпечуючи відповідність кращим міжнародним практикам і вимогам.

Варто зазначити, що заступниця Міністра оборони з цифровізації, цифрових трансформацій та цифрового розвитку, К. Черногоренко, наголосила на важливості постійної уваги до питань кібербезпеки, особливо в умовах безперервних кібератак з боку ворога. Вона підкреслила, що: "заходи з кібербезпеки мають бути системними і повинні постійно вдосконалюватися. Нова політика передбачає систематичний перегляд та оновлення вимог Міноборони у сфері кібербезпеки, що забезпечує адаптацію до нових загроз та викликів у цифровому середовищі" (Ablazov I., and other; The Institute of International & European Affairs).

Доцільно наголосити, що станом на початок 2024 року в Міністерстві оборони, Збройних Силах та інших складових сектору безпеки і оборони України було впроваджено 309 стандартів НАТО. Це число перевищує кількість стандартів, запроваджених у деяких країнах-членах НАТО, що приєдналися до Альянсу під час останньої хвилі його розширення (Про прийняття національних стандартів, зміни до національного стандарту та скасування національних стандартів.).

Так, впровадження стандартів і керівних документів НАТО відіграє ключову роль у системному підвищенні боєздатності наших військ та досягненні взаємосумісності з силами провідних країн світу. Це сприяє не лише ефективному використанню державних ресурсів у сфері оборони, але й посилює готовність держави до спільних дій з міжнародними партнерами. Водночас важливо зазначити, що механічне впровадження стандартів НАТО у сфері оборони України не є доцільним підходом. Досягнення повної відповідності стандартам НАТО не є самоціллю, оскільки навіть держави-члени НАТО не досягають цього показника. Основним завданням є забезпечення взаєморозуміння, взаємозамінності та взаємосумісності між Україною та її партнерами, як на рівні державних установ, штабів усіх рівнів, так і безпосередньо на полі бою.

Варто також враховувати, що стандарти та керівні документи НАТО постійно оновлюються, адаптуючись до нових викликів, переглядаються або замінюються новими стандартами, що відповідають сучасним вимогам. Тому говорити про остаточні часові рамки для їх впровадження було б невірно. Це безперервний процес, який відбувається не тільки в країнах-членах НАТО, але й у державах-партнерах.

Загалом, запровадження стандартів НАТО – це спільна цілеспрямована діяльність усіх складових сектору безпеки та оборони України, систематична робота, що охоплює весь оборонний комплекс і спрямована на забезпечення ефективної та злагодженої взаємодії з нашими міжнародними партнерами.

Так, на основі аналізу ключових стандартів та вимог можна визначити основні публічно-управлінські аспекти впровадження та супроводу інформаційних систем у Міноборони України з урахуванням нормативних документів НАТО:

1. Інституційна адаптація та відповідність стандартам НАТО:

− гармонізація законодавчої та нормативної бази: потребує адаптації національних нормативних документів до стандартів НАТО, щоб забезпечити узгодженість у підходах до інформаційної безпеки;

− створення відповідних організаційних структур: включає формування спеціалізованих підрозділів та органів, відповідальних за управління інформаційними системами та забезпечення кібербезпеки згідно зі стандартами НАТО.

2. Управління ризиками та забезпечення кібербезпеки:

− впровадження системи управління ризиками: застосування підходів NIST Risk Management Framework для ідентифікації, оцінки та мінімізації ризиків у інформаційних системах Міністерства оборони;

− постійний моніторинг та оновлення систем кібербезпеки: забезпечення регулярного перегляду та вдосконалення заходів кіберзахисту відповідно до нових загроз і викликів.

3. Стандартизація та уніфікація інформаційних систем

− встановлення уніфікованих вимог до інформаційних систем: включає розробку та впровадження єдиних стандартів, які б відповідали директивам НАТО щодо безпеки інформаційно-комунікаційних систем;

− взаємозамінність та взаємосумісність: забезпечення можливості інтеграції та взаємодії інформаційних систем Міноборони з аналогічними системами НАТО.

4. Забезпечення конфіденційності, цілісності та доступності інформації

− реалізація технічних заходів захисту: впровадження сучасних технологій шифрування, автентифікації та авторизації для захисту інформації в інформаційних системах Міноборони;

− регулювання доступу до конфіденційної інформації: встановлення чітких правил та про-

цедур щодо доступу до конфіденційних даних, які відповідають міжнародним стандартам.

5. Координація та співпраця з міжнародними партнерами:

− спільні навчання та тренування: організація та проведення спільних навчань з країнами-членами НАТО для підвищення готовності до реагування на кіберзагрози;

− обмін найкращими практиками: створення механізмів для регулярного обміну інформацією та досвідом між Україною та партнерами з НАТО щодо забезпечення кібербезпеки.

6. Аудит та відповідність стандартам:

− регулярний аудит інформаційних систем: проведення внутрішніх та зовнішніх аудитів для перевірки відповідності інформаційних систем встановленим стандартам і директивам НАТО;

− коригуючі дії та покращення: впровадження планів дій для усунення виявлених недоліків та підвищення рівня інформаційної безпеки.

7. Освіта та підготовка кадрів:

− навчання та сертифікація персоналу: забезпечення постійного підвищення кваліфікації та сертифікації персоналу, який займається кібербезпекою та управлінням інформаційними системами;

− підвищення обізнаності щодо кіберзагроз: включення програм з підвищення обізнаності щодо сучасних кіберзагроз та методів захисту у професійну підготовку військовослужбовців і цивільних працівників Міноборони.

Зазначені аспекти є ключовими для успішного впровадження та супроводу інформаційних систем у Міноборони України з урахуванням нормативних основ НАТО, що дозволяє забезпечити надійний захист інформаційних активів та підвищити ефективність оборонних можливостей країни.

Висновки та пропозиції. Таким чином, у сучасних умовах стрімкого зростання кіберзагроз, пов'язаних як з глобальними тенденціями, так і з агресивними діями з боку рф, Міноборони України демонструє рішучі кроки щодо забезпечення надійного захисту своїх інформаційно-комунікаційних систем. Ухвалення нормативного акту, який регламентує основні засади інформаційної безпеки та кібербезпеки, є важливим етапом у зміцненні національної безпеки. Цей акт, що спирається на найкращі підходи НАТО та міжнародні стандарти, забезпечує єдиний, чітко визначений підхід до кіберзахисту в усіх системах Міноборони.

Впровадження цих засад дозволяє Міноборони України не лише відповідати найсучаснішим вимогам інформаційної безпеки, але й активно адаптуватися до нових викликів, що виникають у цифровому середовищі. Керівництво міністерства усвідомлює важливість систематичного перегляду та вдосконалення політики кібербезпеки, що підтверджується постійним моніторингом та оцінкою результативності вжитих заходів. Такий підхід забезпечує надійний захист інформаційних активів та зміцнює позиції України у сфері міжнародної кібербезпеки.

Для вдосконалення управлінських процесів у контексті інтеграції з міжнародними стандартами безпеки в Міноборони України слід розробити та впровадити стратегічний план інтеграції, який включатиме аналіз існуючих стандартів та створення поетапної дорожньої карти; підвищити компетенції персоналу через систематичне навчання, сертифікацію та залучення міжнародних експертів; гармонізувати нормативно-правову базу, оновивши національні нормативні акти з урахуванням міжнародних стандартів та спрощенням регуляторних процедур; вдосконалити систему управління ризиками, впроваджуючи міжнародні методології та регулярний аудит; забезпечити взаємодію та співпрацю з міжнародними партнерами через інтеграцію з міжнародними платформами, спільні навчання та обмін найкращими практиками; а також впровадити систему моніторингу та оцінки ефективності управлінських процесів із використанням KPI, що дозволить вчасно впроваджувати коригуючі дії та підвищити загальну ефективність.

ЛІТЕРАТУРА:

1. Єдині стандарти кібербезпеки: Міноборони зміцнює захист інформаційних систем у відповідності до стандартів НАТО. URL: https://www.mil.gov.ua/news/2024/04/22/i-minoboroni-uhvalilo-nakaz/

2. Зусилля НАТО з протидії дезінформації та охоплення російськомовної аудиторії. Рекомендації та кращі кейси реалізації стратегічних комунікацій в умовах війни : практичний довідник / [В. Азарова та ін. ; за заг. ред. Л. Компанцевої]. Київ : 7БЦ, 2023. 232 с.

3. Про прийняття національних стандартів, зміни до національного стандарту та скасування національних стандартів. Наказ. Державне підприємство "Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості". 17.08.2023 № 210. URL: https://zakon.rada.gov.ua/rada/show/v0210774-23#Text.

4. Стандарти НАТО: механізм і темпи впровадження, адаптація до українських реалій. URL: https://armyinform.com.ua/2021/02/12/standarty-nato-mehanizm-i-tempy-vprovadzhennya-adaptacziya-do-ukrayinskyh-realij/

5. Ablazov I., Demenko O., Leonov O., Mokliak S., Khamula S. Information Weapons within the Interstate Struggle in the XXI Century. *Amazonia Investiga,* 2022. № 11(52). P. 269–277. https://doi.org/10.34069/AI/2022.52.04.29.

6. The Institute of International & European Affairs. URL: https://www.iiea.com/securitydefence?gad_source=1&gclid=CjwKCAjw_Na1BhAIEiwAM-dm7LoKFy4Dp_axDAdPSoZWpJHUvW9RW79S-FLlpf6y6QNcOLSLrGWLxoCti0QAvD_BwE.

REFERENCES:

1. Yedyni standarty kiberbezpeky: Minoborony zmitsniuie zakhyst informatsiinykh system u vidpovidnosti do standartiv NATO [Unified Cybersecurity Standards: The Ministry of Defense Strengthens Information Systems Protection in Accordance with NATO Standards]. Retrieved from: https://www.mil.gov.ua/news/2024/04/22/i-minoboroni-uhvalilo-nakaz/ [in Ukrainian].

2. Zusyllia NATO z protydii dezinformatsii ta okhoplennia rosiiskomovnoi audytorii (2023). [NATO's Efforts to Counter Disinformation and Engage Russian-speaking Audiences. Recommendations and Best Practices for Implementing Strategic Communications in Wartime]. Rekomendatsii ta krashchi keisy realizatsii stratehichnykh komunikatsii v umovakh viiny : praktychnyi dovidnyk / [V. Azarova ta in. ; za zah. red. L. Kompantsevoi]. Kyiv : 7BTs. 232 s. [in Ukrainian].

3. Pro pryiniattia natsionalnykh standartiv, zminy do natsionalnoho standartu ta skasuvannia natsionalnykh standartiv [On the Adoption of National Standards, Amendments to the National Standard, and Cancellation of National Standards]. Nakaz. Derzhavne pidpryiemstvo "Ukrainskyi naukovo-doslidnyi i navchalnyi tsentr problem standartyzatsii, sertyfikatsii ta yakosti". 17.08.2023 № 210. Retrieved from: https://zakon.rada.gov.ua/rada/show/v0210774-23#Text [in Ukrainian].

4. Standarty NATO: mekhanizm i tempy vprovadzhennia, adaptatsiia do ukrainskykh realii [NATO Standards: Implementation Mechanism and Pace, Adaptation to Ukrainian Realities]. Retrieved from: https://armyinform.com.ua/2021/02/12/standarty-nato-mehanizm-i-tempy-vprovadzhennya-adaptacziya-do-ukrayinskyh-realij/ [in Ukrainian].

5. Ablazov, I., Demenko, O., Leonov, O., Mokliak, S., & Khamula, S. (2022). Information Weapons within the Interstate Struggle in the XXI Century. *Amazonia Investiga*, № 11(52). P. 269–277. https://doi.org/10.34069/AI/2022.52.04.29 [in English].

6. The Institute of International & European Affairs. Retrieved from: https://www.iiea.com/securitydefence?gad_source=1&gclid=CjwKCAjw_Na1BhAIEiwAM-dm7LoKFy4Dp_axDAdPSoZWpJHUvW9RW79S-FLlpf6y6QNcOLSLrGWLxoCti0QAvD_BwE [in English].

ЗМІСТ

CONTENTS

ПУБЛІЧНЕ УПРАВЛІННЯ ТА МІСЦЕВЕ САМОВРЯДУВАННЯ

Випуск 2

Коректура • Ірина Миколаївна Чудеснова

Комп'ютерна верстка • Марина Сергіївна Михальченко

Підписано до друку: 21.06.2024. Формат 60x84/8. Гарнітура Arial.
Папір офсет. Цифровий друк. Ум. друк. арк. 9,99. Замов. № 0924/648. Наклад 300 прим.

Видавництво і друкарня – Видавничий дім «Гельветика»
65101, Україна, м. Одеса, вул. Інглезі, 6/1
Телефон +38 (095) 934 48 28, +38 (097) 723 06 08
E-mail: mailbox@helvetica.ua
Свідоцтво суб'єкта видавничої справи
ДК № 7623 від 22.06.2022 р.