УДК 351.123 (045)

Л. Г. Комаха,
д. філос. н., професор, директор, Навчально-науковий інститут публічного управління та державної служби Київського національного університету імені Тараса Шевченка
ORCID ID: https://orcid.org/0000-0002-8474-372X

DOI: 10.32702/2306-6814.2024.9.136

ЗМІЦНЕННЯ ЗОВНІШНЬОПОЛІТИЧНОЇ СТІЙКОСТІ УКРАЇНИ: БЕЗПЕКОВІ АСПЕКТИ ІНФОРМАЦІЙНОЇ СФЕРИ

L. Komaha,
Doctor of Science of Philosophy, Professor, Director, Educational and Scientific Institute of Public Administration and Civil Service Taras Shevchenko National University of Kyiv

STRENGTHENING FOREIGN POLICY STABILITY OF UKRAINE: SECURITY ASPECTS OF THE INFORMATION SPHERE

У статті проаналізовано проблему зміцнення зовнішньополітичної стійкості України в контексті сучасних викликів у інформаційній сфері. Звертаючи увагу на активність російської агресії та її вплив на українське суспільство через кібератаки, дезінформаційні кампанії та інші методи, визначено ключові аспекти та загрози для національної безпеки. Проаналізовано новий тип загроз для національної безпеки — транскордонні загрози, які характеризуються одночасною внутрішньою та зовнішньою спрямованістю та глобальним впливом. Ці загрози зазвичай виникають всередині країни, однак мають зовнішні джерела походження. Надано огляд стратегій та заходів, спрямованих на протидію цим загрозам, включаючи підвищення кібербезпеки, розвиток кібердипломатії та співпрацю з міжнародними партнерами. Розглянуто значення підвищення обізнаності громадян щодо кіберзагроз, а також необхідність розвитку механізмів взаємодії між різними суб'єктами інформаційної безпеки. Зокрема, закцентовано увагу на аналізі нових методів деструктивного впливу та використанні передового досвіду країн-учасниць НАТО для ефективного протистояння загрозам у сучасному інформаційному просторі.

The article analyzes the problem of strengthening Ukraine's foreign policy stability in the context of modern challenges in the information sphere. It is emphasized that at the current stage of the development of society there is a rapid increase in information flows, therefore the dynamics of the development of the information sphere creates new challenges, when "control over information", "power" and "influence" become inextricably linked, and the management of information resources turns into a vital an important element that is necessary for strategic planning of Ukraine's foreign policy development. Taking into account the strengthening of efforts aimed at strengthening foreign policy stability, security aspects are added to the specified challenges, since the state of security of the information sphere has always played a key role in the formation of the state foreign policy strategy. The use of information and communication technologies to carry out cyber attacks, disinformation campaigns, manipulation of information and attacks on communication systems have become not only a threat to individual users, but also a serious challenge to the national security of countries.

Paying attention to the activity of Russian aggression and its impact on Ukrainian society through cyber attacks, disinformation campaigns and other methods, key aspects and threats to national security are identified. A new type of threats to national security is analyzed — cross-border threats, their difference is that they simultaneously have signs of both internal and external threats to national security and are global in nature. Such threats, as a rule, arise internally, but their sources of origin are mostly external. An overview of strategies and measures aimed at countering these threats is provided, including improving cyber security, developing cyber diplomacy and working with international partners. The importance of raising citizens' awareness of cyber threats, as well as the need to develop mechanisms of interaction between various subjects of information security, are considered. In particular, attention is focused on the analysis of new methods of destructive influence and the use of best practices of NATO member countries for effective resistance to threats in the modern information space.

Ключові слова: зовнішньополітична стійкість, інформаційна сфера, безпекові аспекти інформаційної сфери, кіберзагрози, протидія дезінформації, кібергігієна.

Key words: foreign policy stability, information sphere, security aspects of the information sphere, cyber threats, countering disinformation, cyber hygiene.

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

На сучасному етапі розвитку суспільства спостерігається швидкий приріст інформаційних потоків, відтак динаміка розвитку інформаційної сфери породжує нові виклики, коли "контроль за інформацією", "могутність" і "вплив" стають нерозривно пов'язаними, а управління інформаційними ресурсами перетворюється на життєво важливий елемент, який є необхідним для стратегічного планування зовнішньополітичного розвитку України. З урахуванням посилення зусиль, спрямованих на зміцнення зовнішньополітичної стійкості, до вказаних викликів додаються безпекові аспекти, оскільки стан захищеності інформаційної сфери завжди відігравав ключову роль у формуванні державної зовнішньополітичної стратегії. Використання інформаційно-комунікативних технологій для проведення кібератак, дезінформаційних кампаній, маніпуляцій інформацією та атак на комунікаційні системи стали не лише загрозою окремим користувачам, а й серйозним викликом для національної безпеки країн.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

У наукових працях досліджуються різні аспекти зміцнення зовнішньополітичної стійкості України у інформаційній сфері, які спрямовані на покращення зовнішньополітичної позиції України, забезпечення її стійкості до інформаційних викликів та загроз з боку зовнішніх акторів. Серед сучасних українських вчених, які активно досліджують зазначену тему, варто виокремити О. Адамчука, О. Барановського, А. Берко, В. Гурковського, Б. Кормича, В. Ліпкана, О. Олексюка, В. Пилипчука, М. Швеця та інших.

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ (ПОСТАНОВКА ЗАВДАННЯ)

Метою дослідження є аналіз проблеми зміцнення зовнішньополітичної стійкості України в контексті сучасних викликів у інформаційній сфері.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ ДОСЛІДЖЕННЯ

Аналіз безпекових аспектів інформаційної сфери у контексті зміцнення зовнішньополітичної стійкості України є актуальним і важливим завданням, спрямованим на захист національних інтересів, забезпечення стабільності країни в умовах сучасних глобальних викликів, що обумовлюється наступними факторами.

По-перше, інформаційна сфера стає все більш важливим аспектом міжнародних відносин, впливаючи на формування уявлень про країну та її позицію в світі. У контексті змін геополітичного середовища інформаційна війна, дезінформація та кібератаки стають засобами впливу на зовнішньополітичні рішення та імідж країни.

По-друге, на сьогодні Україна перебуває в складній ситуації, де зовнішній тиск і російська військова агресія становлять серйозну загрозу для національної безпеки. Інформаційні технології можуть використовуватися і як засіб у військовому протистоянні, і як інструмент для зміцнення міжнародного статусу та підтримки союзників.

По-третє, забезпечення стійкості інформаційної сфери має важливе значення для економічного розвитку країни та залучення інвестицій. Негативний імідж, створений за допомогою дезінформації та кібератак, підриває довіру потенційних інвесторів до економічних перспектив України.

Вказане стосується й інших аспектів геополітики (екологічного, соціального, військового тощо), що проявляється у пріоритеті більшості напрямів зовнішньої політики щодо інтересів національної та міжнародної інформаційної безпеки. Це підтверджується прийнятою 23 липня 2000 р. Окінавською хартією глобального інформаційного суспільства і систематично підтверджується на Всесвітніх самітах з інформаційного суспільства під егідою ООН, перший з яких відбувся у грудні 2003 р. в Женеві [1; 2].

Такі глобального значення документи є переконливим доказом того, що здатність країни адаптуватися до глобального інформаційного простору, постійне розширення та удосконалення власних інформаційних ресурсів та ефективне управління ними, є на сьогодні най-

важливішим завданням забезпечення національної та міжнародної безпеки. При цьому варто також зазначити, що інформаційна сфера може бути як провідним чинником у втіленні найважливіших суспільних проектів, так і перетворитися на фактор хаотизації та затримки соціального, економічного та культурного розвитку.

Інформація вважається одним з основних ресурсів держави, а системи, які стоять в основі її створення, обробки та поширення, сприяють прогресивному розвитку і є основними соціальними інфраструктурами суспільства. Інформаційний простір розглядається як ключовий стратегічний чинник конкурентоспроможності та провідний сектор національної безпеки. До прикладу, спрямованість Конгресу США на стратегію національної інформаційної політики відображено у доповіді Ф. Вайнгартена "Удосконалення федеральної інформаційної політики: погляд Конгресу". В документі зазначається, що Сполучені Штати Америки розглядають інформаційні проблеми як політичні фактори для прийняття рішень, що нерозривно пов'язані з глобальними проблемами американського суспільства.

Світ стає свідком розділеності на країни з високим рівнем інформаційної розвиненості та країни, що перебувають у процесі розвитку цього напряму. В сучасному світі кібербезпека стала ключовим фактором безпеки інформаційного простору, що впливає на стійкість будь-якої держави. Україна, з огляду на її геополітичне розташування та активну протидію російській військовій агресії, є однією з головних мішеней для кібератак, які спрямовуються на критичну інфраструктуру, зокрема енергетичні системи, телекомунікаційні мережі, фінансові установи та інші важливі сектори економіки країни.

У 2022 році, на тлі повномасштабного російського вторгнення, кібератаки стали невід'ємною частиною інформаційної війни, яка ведеться проти України. Ці атаки спрямовані на дестабілізацію політичної ситуації, підрив довіри до влади та поширення панічних настроїв серед населення. Протягом 2023 року кількість кібератак на українські державні та приватні структури зросла на 30% та завдають значної шкоди економіці, інфраструктурі та репутації країни [3].

Кіберзлочинність становить серйозну загрозу для національної безпеки України. Протягом минулого року фахівці Держспецзв'язку зафіксували понад 2 тисячі кіберінцидентів в Україні. Крім того, відбулося багато кібератак на органи державної влади, фінансові установи, підпрємства критичної інфраструктури, логістики та енергетики. Збитки від інтернет-шахрайства зросли на 96% порівняно з попереднім роком і склали більше 1 мільярда гривень. Російська військова агресія супроводжується нарощуванням війни в кіберпросторі, де спостерігається масштабний наступ, організований та підтримуваний на державному рівні [4].

Науковці підкреслюють, що для протистояння вищевказаним загрозам Україні необхідно вжити низку заходів, зокрема: зміцнити кіберзахист критичної інфраструктури; підвищити рівень кіберобізнаності населення; співпрацювати з міжнародними партнерами тощо. Зазначене засвідчує, що кібербезпека є пріоритетним аспектом інформаційної сфери у контексті забезпечення зовнішньополітичної стійкості України [3].

Це підтверджується низкою офіційних документів, зокрема розпорядженням Кабінету Міністрів України від 19 грудня 2023 р. № 1163-р. "Про затвердження плану заходів на 2023-2024 роки з реалізації Стратегії кібербезпеки України" [5].

Окреслені заходи є критично важливими для успішної реалізації Стратегії кібербезпеки України та забезпечення національної безпеки в умовах постійної загрози кібератак та кіберзлочинності. У цьому зв'язку розроблення системи індикаторів стану кібербезпеки (пункт 1 Плану заходів) дозволить систематично оцінювати та контролювати рівень загрози та готовності країни до їхнього подолання. Створення кібервійськ (пункт 2) є необхідним кроком для забезпечення ефективної оборони у кіберпросторі та здійснення відсічі потенційним агресорам. Крім того, забезпечення взаємодії між основними суб'єктами системи кібербезпеки (пункт 3) та впровадження гармонізованого підходу до застосування санкцій (пункт 27) сприятиме координації зусиль та максимізації ефективності заходів. Розробка Національного плану реагування на кібератаки (пункт 32) та впровадження системи аудиту інформаційної безпеки (пункт 40) допоможе у швидкому реагуванні на кіберзагрози та забезпеченні стабільності у кіберпросторі. Заохочення досліджень і наукових пошуків у сфері кібербезпеки (пункт 48) та навчання й підвищення кваліфікації фахівців (пункт 49) є важливими для забезпечення наукового та технічного прогресу у цій сфері. Нарешті, розвиток співробітництва з міжнародними партнерами (пункти 61-62) та залучення міжнародної технічної допомоги (пункт 63) дозволить забезпечити ефективність української кібербезпеки у глобальному контексті [5].

Дезінформаційні кампанії та маніпуляції інформацією — усе це складові патернів інформаційних операцій, які російська сторона використовує проти України. Ці операції спрямовані на дестабілізацію українського суспільства, підрив авторитету уряду та формування негативного сприйняття України на міжнародній арені. Ефективна протидія дезінформації та захист інформаційного простору є не лише питанням внутрішньополітичної безпеки, але й ключовим аспектом зовнішньополітичної стратегії для будь-якої країни, оскільки успішність протистояння загрозам в інформаційній сфері обумовлює не лише безпека інфраструктури та економіки країни, але й її міжнародний авторитет та стійкість до зовнішніх викликів.

"Біла книга" Міністерства оборони США та Об'єднаного комітету начальників штабів США, а також Стратегія діяльності в інформаційному середовищі визначають, що "інформація стала зброєю, а дезінформація стала інструментом державної політики", в якій виділяється роль інформації в міжнародних відносинах. У документах вказується, що у відносинах між державами інформація та дезінформація не лише фундаментально змінилися, але й стали набагато критичнішими/гострішими [6].

Нещодавно Оксфордським університетом досліджено інформаційну діяльність 28 країн, якими організовано низку маніпуляцій інформацією. Серед цих країн досліджено російські міжнародні інформаційні маніпуляції, однак зазначається, що це далеко не єдина країна, яка бере участь у цій діяльності. Дослідниками до-

ведено, що інформаційні маніпуляції стали глобальним явищем, визначним інструментом у стратегічній зовнішній політиці багатьох урядів на двосторонньому, регіональному та глобальному рівнях [7]. Такі дії створюють серйозні виклики для зовнішньополітичної стратегії країни, порушують дипломатичні відносини, підривають довіру до України та ускладнюють міжнародну співпрацю.

Підвищення обізнаності громадян щодо кіберзагроз і патернів інформаційних операцій є важливою складовою ефективної стратегії протидії. Це передбачає не лише знання основ кібербезпеки, але й розуміння того, як працюють та впливають ці загрози на суспільство. Громадяни повинні бути обізнані з методами захисту особистої інформації в мережі, вміти розпізнавати підроблену чи недостовірну інформацію та виявляти спроби маніпулювання ними. Згідно зі звітом Всесвітнього економічного форуму про глобальні ризики за 2022 рік, існуючі заходи кібербезпеки стають застарілими через дедалі складніші та частіші кіберзлочини [8].

З огляду на те, що кількість і серйозність кібератак продовжує зростати, а в установах та організаціях існує тривожна відсутність стратегій запобігання, важливою є підготовка фахівців для виявлення потенційних кіберзагроз, а також розвиток компетентностей персоналу з метою забезпечення власного захисту. Відповідно до Звіту про розслідування витоку даних за 2023 рік (Data Breach Investigations Report 2023), необхідно акцентувати увагу на цьому аспекті [9].

При цьому важливою є також потреба дотримання належного рівня кібергігієни, що означає вчасне оновлення програмного забезпечення, складних паролів та обережне ставлення до посилань та отриманих файлів. Лише шляхом спільних зусиль громадян, уряду та приватного сектору можна забезпечити ефективний захист від кіберзагроз, спроб інформаційного маніпулятивного впливу та зміцнити зовнішньополітичну стійкість України.

Сучасні наукові дослідження виокремлюють новий тип загроз національній безпеці держави — транскордонні загрози. Їх відмінність полягає в тому, що вони одночасно мають ознаки як внутрішніх, так і зовнішніх загроз для національної безпеки та мають глобальний характер. Такі загрози, як правило, виникають всередині, однак джерела їх походження переважно зовнішні [10].

Цей підхід відображає російську комплексну агресію проти України, що включає захоплення території, інтенсивний інформаційно-психологічний вплив на суспільство, дискредитацію української історії, культури та мови, а також спроби нав'язати українському суспільству або його окремим частинам викривлену картину світу для підтримки ворожих військово-політичних інтересів. Отже, особлива небезпека у інформаційній сфері полягає в тому, що цілеспрямований інформаційний вплив країни-агресора на Україну спрямований на зміну світогляду та моралі як окремих громадян, так і суспільства в цілому, підтримуючи чужоземні інтереси, мотиви та спосіб життя. З огляду на це, набуває особливого значення глибокий аналіз сутності та проявів нових методів прихованого деструктивного впливу, а також виявлення дій, які суперечать національним інтересам України.

Зважаючи на це, протидія дезінформації та захист інформаційного простору набувають вирішального значення для зовнішньополітичної стратегії України. У сучасному глобалізованому світі, коли інформація перебуває в основі всіх сфер життя та взаємодії між країнами, важливо мати механізми, які дозволяють розпізнавати та протидіяти дезінформації. Неправдива або спотворена інформація може порушувати міжнародний порядок, підривати довіру між державами та спричиняти конфлікти.

Один із ефективних способів протистояти загрозам у інформаційному просторі — це застосування передового досвіду країн-учасниць НАТО у розвитку системи державних комунікацій — стратегічних, кризових та урядових. Впровадження такого механізму на усіх рівнях державного управління дозволить успішно реалізовувати єдину комунікативну політику, спрямовану на вирішення питань кібербезпеки та захисту в інформаційному просторі. До прикладу, застосування окремих стандартів інформаційної безпеки серії ISO 2700X стосуються різноманітних проблем у сфері інформаційної безпеки: міжнародний стандарт визначає ISO 27001 як Систему управління інформаційною безпекою (СУІБ); ISO 27701 — забезпечує функціонування Системи управління захистом даних; ISO 27017 надає вказівки щодо Системи заходів інформаційної безпеки для хмарних обчислень, а ISO 27005 містить рекомендації щодо роботи Системи управління ризиками інформаційної безпеки [11].

Окрім того, цей досвід може бути використаний як основа для розвитку кібердипломатії — нової галузі міжнародних відносин, яка спрямована на використання кіберпростору для досягнення зовнішньополітичних цілей. Кібердипломатія включає в себе використання інформаційно-комунікативних технологій для мждержавної комунікації, вплив на глобальні дискусії через соціальні медіа з метою зміни ставлення міжнародних партнерів. Такий підхід дозволить Україні активно впливати на міжнародне оточення та ефективно протистояти загрозам у інформаційному просторі.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

Підсумовуючи зазначимо, що безпекові аспекти інформаційної сфери стають все більш критичним елементом національної та зовнішньополітичної стратегії України. Військова російська агресія, окрім наземного ведення бойових дій, включає також кібератаки, дезінформаційні кампанії та маніпуляції інформацією, створює серйозні загрози для національної безпеки та міжнародного статусу України.

Для зміцнення зовнішньополітичної стійкості необхідно розробляти та впроваджувати комплексні стратегії протидії дезінформації та кіберзагрозам. Це включає необхідність підвищення кібербезпеки, розвиток кібердипломатії, співпрацю з міжнародними партнерами, підвищення обізнаності громадян щодо кіберзагроз та розробку механізмів взаємодії між суб'єктами забезпечення безпеки інформаційного простору.

З огляду на складність і різноманітність загроз інформаційній безпеці, особливо з російського боку,

важливо активно впроваджувати стратегії протидії дезінформації та захисту інформаційного простору, що є ключовим елементом зовнішньополітичної стратегії України, оскільки вплив інформації на міжнародні відносини стає усе більш суттєвим. Важливо використовувати передовий досвід країн-учасниць НАТО та розвивати кібердипломатію як інструмент впливу на глобальні дискусії та ставлення міжнародних партнерів. Це допоможе Україні ефективно протистояти загрозам інформаційного простору та зміцнити власну позицію на міжнародній арені.

Література:

1. Okinawa Charter on the Global Information Society. United Nations. Economic and Social Commission for Western Asia. URL: https://archive.unescwa.org/okinawa-charter-global-information-society

2. World Summit on the Information Society (WSIS). "Wsis Action Lines: Supporting the Implementation of Sdgs. URL: https://sustainabledevelopment.un.org/index.php?page=view&type=30022&nr=102&menu=3170

3. Резнікова О. О. Національна стійкість в умовах мінливого безпекового середовища: монографія. Київ: НІСД, 2022. 532 с. URL: https://niss.gov.ua/sites/default/files/2022-03/reznikova-ukraineresilience2022_02.pdf

4. Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест / відп. ред. О. Довгань; упоряд. О. Довгань, Л. Литвинова, С. Дорогих; Державна наукова установа "Інститут інформації, безпеки і права НАПрН України"; Національна бібліотека України ім. В.І.Вернадського. К., 2023. № 9. 351 с. URL: https://ippi.org.ua/sites/default/files/2023-9.pdf

5. Розпорядження Кабінету Міністрів України від 19 грудня 2023 р. № 1163-р. "Про затвердження плану заходів на 2023-2024 роки з реалізації Стратегії кібербезпеки України". URL: https://www.kmu.gov.ua/npas/pro-zatverdzhennia-planu-zakhodiv-na-20232024-roky-z-realizatsii-stratehii-kiberbezpeky-ukrainy-i191223-1163

6. Strategy for operations in the information environment. 2023. URL: https://media.defense.gov/2023/Nov/17/2003342901/-1/-1/1/2023-department-of-defense-strategy-for-operations-in-the-information-environment.pdf

7. Bradshaw, S, Howard, P. Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation. URL: https://ora.ox.ac.uk/objects/uuid:cef7e8d9-27bf-4ea5-9fd6-855209b3e1f6

8. The Importance of Cyber Security Awareness Training for Employees. URL: https://www.elev8me.com/insights/the-importance-of-cyber-security-awareness-training-for-employees

9. Data Breach Investigations Report 2023. Summary of Findings. URL: https://www.verizon.com/business/resources/reports/dbir/2023/summary-of-findings/

10. Аналіз загроз національній безпеці у сфері внутрішньої політики. Національний інститут стратегічних досліджень. URL: https://niss.gov.ua/sites/default/files/2023-07/ad_analiz-zagroz_14072023.pdf

11. Andre Saeckel. Standards for information security — an overview. URL: https://www.dqsglobal.com/intl/learn/blog/standards-for-information-security-an-overview

References:

1. Society United Nations. Economic and Social Commission for Western Asia (2000), "Okinawa Charter on the Global Information", available at: https://archive.unescwa.org/okinawa-charter-global-information-society (Accessed 15 April 2024).

2. UN (2016), "World Summit on the Information Society (WSIS). "Wsis Action Lines: Supporting the Implementation of Sdgs", available at: (Accessed 15 April 2024). https://sustainabledevelopment.un.org/index.php?page=view&type=30022&nr=102&menu=3170

3. Reznikova, O.O. (2022), Natsional'na stijkist' v umovakh minlyvoho bezpekovoho seredovyscha [National stability in the conditions of a changing security environment], NISD, Kyiv, Ukraine, available at: https://niss.gov.ua/sites/default/files/2022-03/reznikova-ukraineresilience2022_02.pdf (Accessed 15 April 2024).

4. Dovhan', O. (2023), Kiberbezpeka v informatsijnomu suspil'stvi: Informatsijno-analitychnyj dajdzhest [Cyber security in the information society: Informational and analytical digest], Derzhavna naukova ustanova "Instytut informatsii, bezpeky i prava NAPrN Ukrainy"; Natsional'na biblioteka Ukrainy im. V.I.Vernads'koho, Kyiv, Ukraine, available at: https://ippi.org.ua/sites/default/files/2023-9.pdf (Accessed 15 April 2024).

5. Cabinet of Ministers of Ukraine (2023), Resolution "On the approval of the action plan for 2023-2024 for the implementation of the Cybersecurity Strategy of Ukraine", available at: https://www.kmu.gov.ua/npas/pro-zatverdzhennia-planu-zakhodiv-na-20232024-roky-z-realizatsii-stratehii-kiberbezpeky-ukrainy-i191223-1163 (Accessed 15 April 2024).

6. U.S. Department of Defense (2023), "Strategy for operations in the information environment", available at: https://media.defense.gov/2023/Nov/17/2003342901/-1/-1/1/2023-department-of-defense-strategy-for-operations-in-the-information-environment.pdf (Accessed 15 April 2024).

7. Bradshaw, S and Troops, H.P. (2017), "Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation", available at: https://ora.ox.ac.uk/objects/uuid:cef7e8d9-27bf-4ea5-9fd6-855209b3e1f6 (Accessed 15 April 2024).

8. elev8 (2023), "The Importance of Cyber Security Awareness Training for Employees", available at: https://www.elev8me.com/insights/the-importance-of-cyber-security-awareness-training-for-employees (Accessed 15 April 2024).

9. Verizon (2024), "Data Breach Investigations Report 2023. Summary of Findings", available at: https://www.verizon.com/business/resources/reports/dbir/2023/summary-of-findings/ (Accessed 15 April 2024).

10. NISS (2023), "Analysis of threats to national security in the field of domestic policy", available at: https://niss.gov.ua/sites/default/files/2023-07/ad_analiz-zagroz_14072023.pdf (Accessed 15 April 2024).

11. Saeckel, A. (2022), "Standards for information security — an overview", available at: https://www.dqsglobal.com/intl/learn/blog/standards-for-information-security-an-overview (Accessed 15 April 2024).

Стаття надійшла до редакції 26.04.2024 р.