УДК 35.07, 004.056
DOI https://doi.org/10.51547/ppp.dp.ua/2024.6.22

Попік Андрій Васильович,
здобувач ступеня доктора філософії (PhD)
спеціальності 281 «Публічне управління та адміністрування»
Національного університету «Чернігівська політехніка»
ORCID ID: 0009-0006-0622-2108

ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІ РИЗИКИ В СИСТЕМІ ПУБЛІЧНОГО УПРАВЛІННЯ: ВИКЛИКИ ТА ШЛЯХИ МІНІМІЗАЦІЇ

INFORMATION AND COMMUNICATION RISKS IN THE PUBLIC ADMINISTRATION SYSTEM: CHALLENGES AND WAYS TO MINIMIZE THEM

У статті досліджуються інформаційно-комунікаційні ризики у системі публічного управління України в умовах цифрової трансформації та воєнного стану. Акцентовано увагу на тому, що ефективність державного управління значною мірою залежить від якості комунікації як всередині державних структур, так і між органами влади та громадськістю. Водночас розширення цифрових технологій та збільшення інформаційних потоків спричиняє появу нових загроз, зокрема: кібератак, поширення дезінформації, маніпулятивних наративів та низького рівня медіаграмотності населення. Підтверджено, що зростання кількості кіберінцидентів та інформаційних атак на державні інституції безпосередньо впливає на ефективність управлінських процесів. Виявлено, що у 2024 році кількість зафіксованих кібератак на державні органи України зросла на 69,8% порівняно з попереднім роком. Одночасно значно збільшилися фінансові втрати громадян через кіберзлочинність, що свідчить про необхідність посилення інформаційної безпеки на всіх рівнях державного управління. У статті розглянуто основні види інформаційно-комунікаційних ризиків у публічному управлінні: технологічні ризики; організаційні ризики; когнітивні ризики; юридичні ризики; соціальні ризики. З метою мінімізації цих загроз запропоновано комплексний підхід, що включає такі напрями: розвиток кібербезпеки державних інформаційних систем та посизахисту персональних даних; стандартизація комунікацій у державному управлінні для підвищення ефективності інформаційного обміну; протидія дезінформації шляхом запровадження інструментів автоматичного виявлення фейкових новин і підвищення рівня медіаграмотності населення; впровадження кризових комунікацій для оперативного реагування на інформаційні атаки та підтримки довіри громадян до державних інституцій; розробка законодавчих ініціатив, спрямованих на посилення інформаційної безпеки та регулювання відповідальності за поширення маніпулятивної інформації.

Ключові слова: *публічне управління, інформаційні ризики, кібербезпека, кризові комунікації, дезінформація, цифрова безпека.*

The article explores information and communication risks in Ukraine's public administration system in the context of digital transformation and martial law. Emphasis is placed on the fact that the effectiveness of public governance largely depends on the quality of communication both within state structures and between government authorities and the public. At the same time, the expansion of digital technologies and the increase in information flows have led to the emergence of new threats, including cyberattacks, the spread of disinformation, manipulative narratives, and the low level of media literacy among the population. It has been confirmed that the rising number of cyber incidents and information attacks on state institutions directly affects the efficiency of administrative processes. In 2024, the number of recorded cyberattacks on Ukrainian government agencies increased by 69.8% compared to the previous year. Simultaneously, the financial losses of citizens due to cybercrime have significantly increased, indicating the need to strengthen information security at all levels of public administration. The article examines the main types of information and communication risks in public administration, including: technological risks, organizational risks, cognitive risks, legal risks, social risks. To mitigate these threats, a comprehensive approach has been proposed, which includes the following directions: strengthening cybersecurity of government information systems and protecting personal data; standardizing communication within public administration to enhance the efficiency of information exchange; combating disinformation by implementing tools for the automatic detection of fake news and increasing the level of media literacy among the population; introducing crisis communication strategies for prompt responses to information attacks and maintaining public trust in government institutions; developing legislative initiatives aimed at strengthening information security and regulating liability for the dissemination of manipulative information.

Key words: *public administration, information risks, cybersecurity, crisis communication, disinformation, digital security.*

Постановка проблеми у загальному вигляді. Сучасна система публічного управління в Україні функціонує в умовах динамічного розвитку інформаційного суспільства, що зумовлює зростання ролі інформаційно-комунікаційних процесів, а ефективність управлінських рішень значною мірою залежить від здатності державних органів забезпечувати якісну комунікацію як всередині системи, так і з громадськістю. Водночас, попри зростаюче використання цифрових технологій та розширення каналів комунікації, публічне управління стикається з низкою ризиків, що можуть суттєво ускладнювати функціонування управлінських процесів.

Основним з таких ризиків сьогодні є військові дії на території нашої країни. Інформаційні атаки, кібератаки, поширення дезінформації та маніпулятивних наративів стають потужними інструментами гібридної війни, спрямованими на підрив довіри до державних інституцій та дестабілізацію управлінських процесів. Крім того, обмеженість ресурсів, пошкодження інфраструктури зв'язку та необхідність оперативного прийняття рішень у кризових умовах лише посилюють ці виклики.

Тож, забезпечення ефективних інформаційно-комунікаційних зв'язків у період воєнного стану стає не просто питанням оптимізації управлінських процесів, а життєво необхідним елементом національної безпеки. Від швидкості та достовірності комунікацій залежать координація дій органів влади, підтримка громадянського суспільства, протидія ворожій пропаганді та формування стійкості держави. Саме тому особливу увагу слід приділити розробці механізмів мінімізації негативного впливу інформаційних загроз і впровадженню дієвих стратегій кризових комунікацій.

Аналіз останніх досліджень і публікацій. У сучасній науковій літературі приділяється значна увага дослідженню інформаційно-комунікаційних ризиків у системі публічного управління. Зокрема, у роботі О. Сяської, О. Поліщук, О. Савченко (Сяська О., 2024) аналізуються виклики, пов'язані з упровадженням електронного урядування, блокчейн-технологій і штучного інтелекту, а також їхній вплив на безпеку та ефективність державного управління. Дослідники акцентують увагу на необхідності розвитку кіберзахисту та вдосконалення інформаційних політик у публічному управлінні. О. Михайлова (Михайлова О., 2022) досліджує роль комунікативних процесів як інструменту формування соціальних зв'язків між урядом та органами публічної влади різних рівнів. Автор наголошує на необхідності адаптації комунікаційних стратегій до сучасних викликів і формування механізмів кризових комунікацій, особливо в умовах війни. О. Михайловська (Михайловська О.,) акцентує увагу на впливі інформаційно-комунікаційних загроз у період кризових ситуацій, зокрема, в умовах воєнного стану, розглядаючи сучасні інструменти зміцнення стійкості державних комунікацій, роль цифрових платформ у формуванні довіри до органів влади, а також розробляє практичні рекомендації щодо вдосконалення механізмів інформаційної безпеки.

Незважаючи на наявність досліджень, питання мінімізації інформаційно-комунікаційних ризиків у публічному управлінні, особливо в умовах кризових ситуацій, потребує подальшого вивчення. Більшість наукових праць зосереджуються на загальних аспектах впровадження інформаційних технологій, тоді як специфічні ризики та загрози, пов'язані з комунікаційними процесами, залишаються недостатньо дослідженими, що підкреслює необхідність розробки комплексних підходів та практичних рекомендацій щодо підвищення стійкості системи публічного управління до інформаційних загроз.

Мета статті є аналіз інформаційно-комунікаційних ризиків у системі публічного управління, виявлення їхнього впливу на ефективність державного управління та розробка підходів до їх мінімізації в умовах сучасних викликів, зокрема дії воєнного стану.

Виклад основного матеріалу. Система публічного управління відіграє ключову роль у забезпеченні сталого розвитку суспільства, ефективного прийняття управлінських рішень та реалізації державної політики. В умовах цифровізації та швидкої зміни інформаційного простору особливої актуальності набуває проблема інформаційно-комунікаційних ризиків, які можуть призводити до викривлення даних, втрати довіри до органів влади та дестабілізації суспільно-політичної ситуації.

В умовах воєнного стану інформаційні загрози посилюються, адже зовнішні та внутрішні фактори впливають на систему публічного управління не лише через кібератаки та дезінформацію, але й через низьку координацію між органами влади та громадськістю. У таких обставинах забезпечення безперебійних і достовірних комунікацій стає критично важливим для збереження керованості держави та підтримки суспільної довіри. У науковій літературі дослідники виділяють різні категорії інформаційно-комунікаційних ризиків у публічному управлінні. Зокрема, розглядаються проблеми реалізації комунікаційних

стратегій у публічному управлінні, що включають організаційні та когнітивні аспекти [2].

Основні види інформаційно-комунікаційних ризиків. О. Клюцевський аналізує управлінські ризики, пов'язані з проведенням державних реформ, акцентуючи увагу на економічних, фінансово-кредитних та соціальних ризиках [4]. Науковцями обговорюються і проблеми впровадження нових інформаційних технологій у публічному управлінні, що стосуються технологічних та юридичних аспектів [1]. У дисертаційних дослідженнях також приділяється увага класифікації інформаційно-комунікаційних ризиків у системі публічного управління. Зокрема, у роботі Т. Амро [5] розглядаються комунікативні технології та шляхи вдосконалення комунікаційної безпеки публічного управління, що включають аналіз організаційних та когнітивних ризиків. А. Колодка, присвячує своє дослідження механізмам кризового менеджменту в умовах інформаційних загроз у гібридних середовищах, де акцентується на технологічних та юридичних аспектах ризиків [6]. Таким чином, науковці виділяють різні види інформаційно-комунікаційних ризиків, зокрема технологічні, організаційні, когнітивні та юридичні (Таблиця 1).

Зауважимо, що перелік ризиків не обмежується представленими у таблиці 1. У процесі розвитку цифрових технологій та змін у суспільно-політичному середовищі можуть виникати нові загрози, що потребують постійного моніторингу та адаптації стратегій управління інформаційно-комунікаційною безпекою.

Вплив інформаційно-комунікаційних ризиків на систему публічного управління. У сучасних умовах інформаційно-комунікаційні ризики становлять серйозну загрозу для системи публічного управління України. Зокрема, кількість кібератак на державні органи та критичну інфраструктуру країни стрімко зростає. За даними Державної служби спеціального зв'язку та захисту інформації України [7], у 2024 році було опрацьовано 4315 кіберінцидентів, що на 69,8% більше порівняно з 2023 роком, коли було зафіксовано 2541 інцидент. На рисунку 1. Представлено динаміку зростання українського ринку кібербезпеки в період 2016–2029 років. Як можна побачити: фактичні дані (2016–2023) демонструють поступове зростання обсягу ринку; прогнозовані дані (2024E–2029E) показують очікуване зростання ринку до 209 млн доларів у 2029 році. Тобто, графік демонструє стійку тенденцію до зростання інвестицій та витрат на кібербезпеку, що може бути зумовлено зростаючими інформаційними загрозами, цифровізацією державних послуг та посиленням регулювання у сфері інформаційної безпеки.

Рис. 1. Обсяг Українського ринку кібербезпеки 2016–2029[E] [8]

Зазначимо, що після початку повномасштабної війни втрати громадян України від кіберзлочинності суттєво зросли. Якщо у 2021 році вони становили 484 млн грн, то у 2022 році збільшилися до 968 млн грн. Кібератаки, зокрема віруси-вимагачі та витоки даних, не лише порушують роботу бізнесу, спричиняючи простої, але й вимагають значних фінансових ресурсів для відновлення.

Таблиця 1

Основні види інформаційно-комунікаційних ризиків

Види ризиків	Характеристика
Технологічні ризики	пов’язані з кібератаками, витоками даних, технічними збоями в державних інформаційних системах і можуть призводити до втрати критично важливої інформації або її спотворення.
Організаційні ризики	недостатня координація між державними установами, невизначеність відповідальних осіб за комунікаційні процеси, бюрократичні перепони у прийнятті рішень.
Когнітивні ризики	вплив фейкових новин, маніпуляцій та дезінформаційних кампаній на громадську думку, що може посилити недовіру до органів влади та викликати соціальну нестабільність.
Юридичні ризики	недостатня правова регламентація інформаційної діяльності, відсутність чітких механізмів відповідальності за поширення неправдивої інформації в державних структурах.
Соціальні ризики	низький рівень медіаграмотності населення, що робить суспільство вразливим до інформаційних атак та пропаганди.

Рис. 2. Динаміка кіберзагроз, міжнародної підтримки та розвитку ШІ/ML спеціалістів в Україні [8]

Однак, особливої уваги потребують кібератаки на державні реєстри. У грудні 2024 року росія здійснила масовану кібератаку на українські державні реєстри, що призвело до тимчасового призупинення їхньої роботи. Такі реєстри містять важливу інформацію про громадян України, зокрема дані про народження, смерть, шлюби та власність, тому важливість пошуку шляхів мінімізації інформаційно-комунікаційних ризиків не викликає сумніву.

Варто зауважити, що паралельно з кібератаками, Україна стикається з масштабними інформаційними атаками. Фахівці кібердепартаменту Служби безпеки України щомісяця фіксують понад тисячу інформаційних атак на українське суспільство. Метою цих атак є дестабілізація ситуації в країні та підрив довіри громадян до державних інституцій. Важливо те, що дезінформація має значний вплив на емоційний стан населення. Згідно з дослідженням, 69% опитаних українців зазначили, що дезінформація негативно впливає на їхній емоційний стан, викликаючи такі почуття, як гнів, тривога та стрес [9]. Такі статистичні дані підкреслюють необхідність розробки та впровадження ефективних стратегій мінімізації інформаційно-комунікаційних ризиків у системі публічного управління України. Водночас захист державних інформаційних систем, протидія дезінформації та підвищення рівня медіаграмотності населення є головними напрямами для забезпечення інформаційної безпеки країни.

Будь-які інформаційні ризики негативно впливають на ефективність публічного управління, а саме: 1) дестабілізацію прийняття управлінських рішень через поширення недостовірної або маніпулятивної інформації; 2) втрати довіри громадськості до державних органів, що ускладнює імплементацію реформ та державних ініціатив; 3) послаблення національної безпеки через витік стратегічно важливої інформації або інформаційні атаки з боку ворожих держав; 4) погіршення комунікації між державними органами, що призводить до дублювання функцій, несвоєчасного реагування на кризові ситуації та втрати ефективності управлінських процесів.

Рівні негативного впливу різних типів інформаційно-комунікаційних ризиків на ефективність публічного управління представлені в Таблиці 2.

Таблиця 2

Типи інформаційно-комунікаційних ризиків та рівень їх впливу на ефективність публічного управління

Тип ризику	Характеристика
Кібератаки (≈70%) – зафіксоване зростання кіберінцидентів в Україні у 2024 році.	У 2024 році кількість кібератак на Україну зросла на 69,8%, досягнувши 4315 інцидентів, порівняно з 2541 у 2023 році, що свідчить про значне посилення загрози для державних установ та критичної інфраструктури, що безпосередньо впливає на ефективність публічного управління.
Дезінформація (≈85%) – частка опитаних, які відчувають негативний вплив дезінформації.	Дезінформація та пропаганда мають потужний вплив на формування громадської думки, особливо в умовах воєнного конфлікту. Постійний потік фейкових новин та маніпуляцій може призводити до паніки, недовіри до державних інституцій та дестабілізації суспільства.
Координаційні проблеми (≈60%) – оцінка впливу недостатньої координації між державними органами.	Недостатня координація між державними органами та відомствами може призводити до дублювання функцій, затримок у прийнятті рішень та неефективного використання ресурсів. Хоча конкретні статистичні дані щодо цього аспекту обмежені, аналітичні огляди вказують на значний вплив таких проблем на загальну ефективність управління.
Юридичні ризики (≈50%) – рівень впливу недосконалого законодавства у сфері інформаційної безпеки.	Недосконалість нормативно-правової бази у сфері інформаційної безпеки та відсутність чітких механізмів відповідальності за поширення дезінформації можуть ускладнювати боротьбу з інформаційними загрозами. Це створює прогалини в законодавстві, які можуть бути використані для підриву державних інституцій.
Соціальна вразливість (≈65%) – частка населення, яка вразлива до інформаційних атак.	Низький рівень медіаграмотності населення робить суспільство вразливим до інформаційних атак. Люди, які не вміють критично оцінювати отриману інформацію, легше піддаються впливу фейкових новин, що може призводити до масових дезінформаційних кампаній та підриву суспільної довіри.

Джерело: складено автором відповідно до аналітичних даних та експертних думок у сфері інформаційної безпеки та публічного управління [9; 10; 11].

Шляхи мінімізації інформаційно-комунікаційних ризиків. Як можна побачити, інформаційно-комунікаційні ризики у системі публічного управління є складним викликом, який вимагає комплексного підходу та поєднання технологічних, організаційних, освітніх і правових механізмів. З огляду на сучасні загрози, що включають кіберзлочинність, дезінформаційні кампанії, маніпулятивні наративи та недостатню координацію між державними органами, можна виділити кілька ключових стратегій мінімізації цих ризиків (Рис. 3).

У цілому мінімізація інформаційно-комунікаційних ризиків у системі публічного управління потребує комплексного підходу, що включає як технологічні рішення, так і організаційні та законодавчі зміни. Тож, лише комплексний підхід може забезпечити інформаційну стійкість держави в умовах сучасних викликів.

Висновки. Інформаційно-комунікаційні ризики у системі публічного управління України є однією з сучасних загроз ефективному державному управлінню, особливо в умовах воєнного стану. Відповідно до проведеного дослідження, можемо засвідчити, що інформаційні загрози, зокрема кібератаки, дезінформація, маніпулятивні наративи та недостатня координація між державними органами, можуть суттєво ускладнювати функціонування управлінських процесів, підривати довіру до державних інституцій та дестабілізувати суспільно-політичну ситуацію. Аналіз літературних джерел та статистичних даних підтвердив, що останніми роками масштаби кіберзагроз в Україні зростають, а поширення дезінформації та низький рівень медіаграмотності населення лише посилюють вразливість держави перед інформаційними атаками. У цьому контексті особливого значення набуває розробка стратегій інформаційної безпеки та кризових комунікацій, що дозволять забезпечити оперативне реагування на загрози та мінімізувати їхній негативний вплив. У ході дослідження було визначено основні види інформаційно-комунікаційних ризиків та представлено основні стратегії зменшення інформаційно-комунікаційних, зокрема: розвиток кібербезпеки, стандартизація комунікацій, протидія дезінформації, кризові комунікації, удосконалення нормативно-правової бази. Отже, забезпечення стійкості системи публічного управління до інформаційних загроз має бути пріоритетним завданням державної політики, а впровадження комплексного підходу дозволить зменшити ризики, підвищити довіру громадян до державних інституцій та сприяти збереженню інформаційної стійкості України в умовах сучасних викликів.

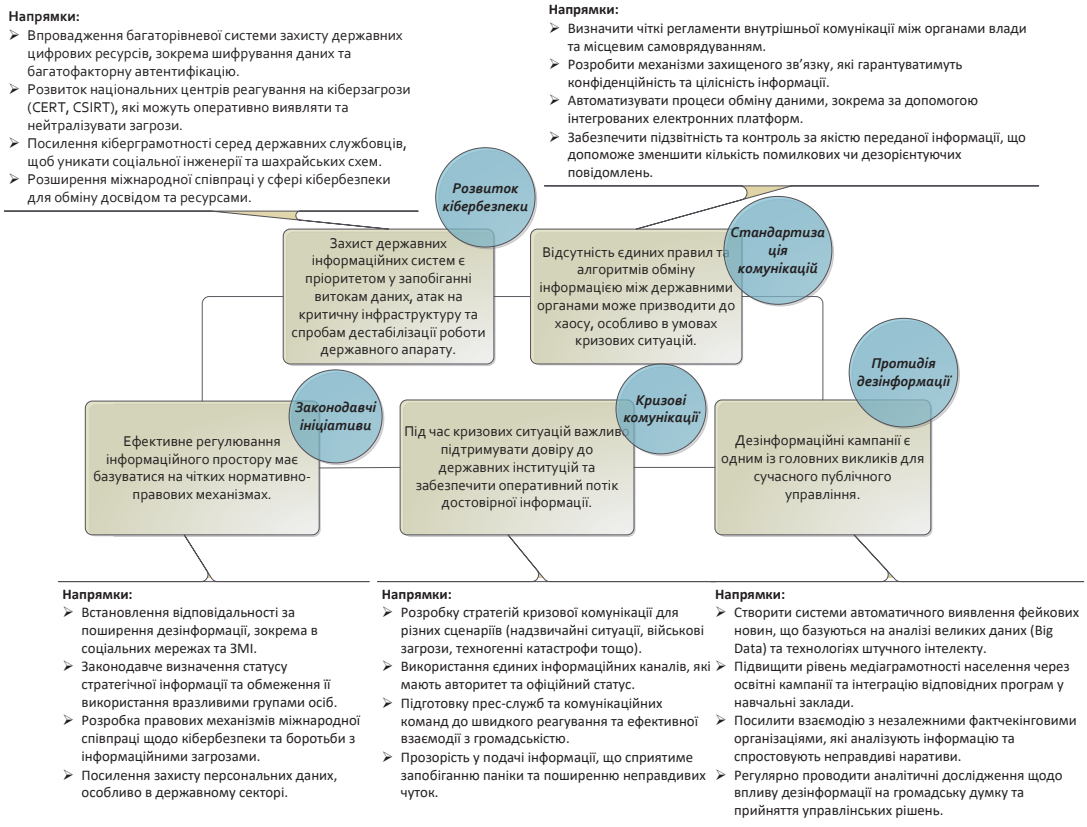

Рис. 3. Основні стратегії мінімізації інформаційно-комунікаційних ризиків

Джерело: побудовано автором

REFERENCES:

1. Siaska, O. V., Polishchuk, O. Yu., Savchenko, O. R. (2024). Novi informatsiini tekhnolohii v publichnomu upravlinni: problemy ta perspektyvy [New information technologies in public administration: problems and prospects]. *Vcheni zapysky TNU imeni V.I. Vernadskoho*. Seriia: Publichne upravlinnia ta administruvannia, Tom 35 (74) № 1. S. 157-163 [in Ukrainian].

2. Mykhailova O.H. Suchasni stratehii komunikatsii u publichnomu upravlinni ta administruvanni v umovakh nevyznachenosti [Modern communication strategies in public management and administration under conditions of uncertainty]. *Problemy suchasnykh transformatsii. Seriia: pravo, publichne upravlinnia ta administruvannia.* 2022. № 5. URL: https://reicst.com.ua/pmtl/article/view/2022-5-02-03/2022-5-02-03 [in Ukrainian].

3. Mykhailovska, O. V., Mykhailovskyi, I. M., Pylypenko, O. O. Vplyv komunikatsii na efektyvnist publichnoho upravlinnia v umovakh kryz [The impact of communications on the effectiveness of public administration in crises]. *Problemy suchasnykh transformatsii. Seriia: pravo, publichne upravlinnia ta administruvannia*. 2024. (12). URL: https://doi.org/10.54929/2786-5746-2024-12-02-07 [in Ukrainian].

4. Kliutsevskyi V.I. Proiavy upravlinskykh ryzykiv u sferi publichnoho upravlinnia v Ukraini [Manifestations of management risks in the field of public administration in Ukraine]. *Publichne upravlinnia i administruvannia v Ukraini*. 2019. (14). S. 54-58 [in Ukrainian].

5. Amro T. A. Vplyv komunikatyvnykh tekhnolohii na efektyvnist publichnoho upravlinnia v Ukraini v umovakh voiennoho stanu [The Impact of Communication Technologies on the Effectiveness of Public Administration in Ukraine under Martial Law]. Dysertatsiia na zdobuttia naukovoho stupenia doktora nauk : 25.00.05 / Mizhrehionalna Akademiia upravlinnia personalom, Kyiv, 2023 [in Ukrainian].

6. Kolodka A.V. Mekhanizmy kryzovoho menedzhmentu v umovakh informatsiinykh zahroz v hibrydnykh seredovyshchakh [Crisis management mechanisms in the context of information threats in hybrid environments]. Dysertatsiia na zdobuttia naukovoho stupenia doktora filosofii: 281 “Publichne upravlinnia ta administruvannia” / Instytut derzhavnoho upravlinnia ta naukovykh doslidzhen z tsyvilnoho zakhystu, Kyiv, 2023 [in Ukrainian].

7. Derzhavna sluzhba spetsialnoho zviazku ta zakhystu informatsii Ukrainy [Державна служба спеціального зв’язку та захисту інформації України]. (2024). CERT-UA mynuloho roku opratsiuvala 4315 kiberintsydentiv. URL: https://cip.gov.ua/ua/news/cert-ua-minulogo-roku-opracyuvala-4315-kiberincidentiv [in Ukrainian].

8. Ohliad rynku kiberbezpeky v Ukraini [Overview of the cybersecurity market in Ukraine]. (2024). URL: https://skilky-skilky.info/wp-content/uploads/2024/01/Ohliad-rynku-kiberbezpky-v-Ukraini.pdf [in Ukrainian].

9. AOAV. (2024). Ukraine: AOAV explosive violence data on harm to civilians. URL: https://aoav.org.uk/2024/ukraine-casualty-monitor/

10. Natsionalna spilka zhurnalistiv Ukrainy [Національна спілка журналістів України]. (2024). Propahanda ta dezinformatsiia: shcho naibilshe vplyvaie na ukrainskyi infoprostir. URL: https://nsju.org/novini/propaganda-ta-dezinformacziya-shho-najbilshe-vplyvaye-na-ukrayinskyj-infoprostir/ [in Ukrainian].

11. Forbes. (2024). Kiberataky staiut realnymy zahrozamy u sviti. URL: https://forbes.ua/company/kiberataki-stayut-realnimi-zagrozami-u-sviti-mayk-pompeo-kolishniy-derzhsekretar-ssha-a-nini-nezalezhniy-nevikonavchiy-direktor-naglyadovoi-radi-kiivstar-08022024-19064