УДК 351.74 + 342.95

О. І. Кравченко,
аспірант, Державний університет "Київський авіаційний інститут"
ORCID ID: https://orcid.org/0009-0006-0759-6830

DOI: 10.32702/2306-6814.2025.3.239

ТЕОРЕТИЧНІ ЗАСАДИ ВИЗНАЧЕННЯ ЗАГРОЗ НАЦІОНАЛЬНОЇ БЕЗПЕКИ В УМОВАХ ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА

O. Kravchenko,
Postgraduate student, State University "Kyiv Aviation Institute"

THEORETICAL PRINCIPLES OF DETERMINING NATIONAL SECURITY THREATS IN THE INFORMATION SOCIETY

Досліджено сутність понять у межах обраного предмета дослідження (інформаційна загроза, гібридна війна, інформатизація, цифровізації). Акцентовано, що ці поняття характеризують явища та процеси, які чинять взаємозумовлюючий вплив. Виявлено, що автоматизація передує інформатизації та цифровізації. Вони покликані забезпечувати технологічний і цифровий розвиток суспільства, а також інформаційний. Крім того, цифровізації розглянуто як сучасний етап розвитку інформаційного суспільства, що триває до тепер і передбачає кількісно-якісні зміни в його межах. Наполягається на важливості визначення негативного впливу цифрових технологій на стан розвитку інформаційного суспільства та системи національної безпеки. З метою унеможливлення такого впливу обгрунтована необхідність виваженого використання новітніх технологій. При цьому рекомендовано розглядати національну безпеку, інформаційне суспільство та загрози ним із застосуванням синергетичного підходу. Він дозволив визначити роль стратегічних комунікацій у попередженні загроз нацбезпеці. Доведено, що зазначені аспекти охоплюються терміном демпфування загроз національній безпеці в умовах впливу інформаційного суспільства. Цей процес означає вчасне визначення та попередження загроз у зазначеній сфері, дія яких спрямована на дестабілізацію системи безпеки в цілому та дезінформацію суспільства. Прикладом останньої є поширення державою-агресоркою серед власного, міжнародного й українського суспільства наративів, які містять викривлену та неправдиву інформацію щодо політичних, історичних, економічних, соціальних та інших явищ і процесів. Уважаємо, що протистояти таким наративам та іншим гібридним загрозам складно, але можливо. Для цього має вживатись цілий комплекс публічно-управлінських заходів. Передбачається, що це інституційні заходи, тобто політичні, соціальні, правові, організаційні та інші.

The essence of the concepts within the selected subject of research (information threat, hybrid warfare, informatization, digitalization) is investigated. It is emphasized that these concepts characterize phenomena and processes that have a mutually conditioning effect. It is revealed that automation precedes informatization and digitalization. They are designed to ensure the technological and digital development of society, as well as information. In addition, digitalization is considered as a modern stage of the development of the information society, which continues to this day and involves quantitative and qualitative changes within it. The importance of determining the negative impact of digital technologies on the state of development of the information society and the national security system is emphasized. In order to prevent such an impact, the need for a balanced use of the latest technologies is substantiated. At the same time, it is recommended to consider national security, the information society and threats to it using a synergistic approach. It allowed to determine

the role of strategic communications in preventing threats to national security. It is proven that the mentioned aspects are covered by the term of damping threats to national security under the influence of the information society. This process means the timely identification and prevention of threats in the specified area, the action of which is aimed at destabilizing the security system as a whole and disinforming society. An example of the latter is the dissemination by the aggressor state among its own, international and Ukrainian society of narratives that contain distorted and false information about political, historical, economic, social and other phenomena and processes. We believe that it is difficult, but possible, to resist such narratives and other hybrid threats. For this, a whole complex of public and administrative measures should be taken. It is assumed that these are institutional measures, that is, political, social, legal, organizational and others.

Ключові слова: публічне управління, державна політика, національна безпека, інформаційна безпека, загрози, попередження, реагування, демпфування, інформаційне суспільство, цифрові технології, інформаційні загрози, гібридна війна.

Key words: public administration, public policy, national security, information security, threats, warning, response, damping, information society, digital technologies, information threats, hybrid warfare.

ПОСТАНОВКА ПРОБЛЕМИ

Останніми роками актуалізувались питання, пов'язані з функціонуванням сфери національної безпеки по всьому світу. Вплив на цю сферу чинять зовнішні та внутрішні фактори, частина з яких є позасистемними, тобто складно прогнозованими, і масштабними. Серед цих факторів варто виокремити ті, що пов'язані з використанням кінетичної зброї та нетрадиційної зброї, покликаної наносити не меншу шкоду та зумовлювати появу інформаційних загроз. Останні вимагають розвиток інформаційного та цифрового суспільства, інакше яким чином поширювати ту чи іншу інформацію з метою впливу на свідомість населення для зниження рівня системи безпеки в цілому. З огляду на це набувають важливості наукові розвідки, присвячені дослідженню природи та джерел інформаційних загроз, особливостей їхнього спрямування та значення для системи національної безпеки. Усе це засвідчує необхідність дієвого впровадження таких інструментів, що мають відповідати вимогам часу та суспільства щодо вчасності реагування на інформаційні загрози та забезпечення національної безпеки на належному рівні, адже від стану її функціонування залежить і життя та здоров'я людей, і державний суверенітет і територіальна цілісність України. Її населення є найвищою соціальною цінністю, і від стану захисту його інтересів залежить також рівень безпеки в країні. Тому одним із дієвих механізмів щодо забезпечення національної безпеки є розвиток інформаційного суспільства, який має вміти протистояти деструктивному впливу різних факторів. У цьому контексті вважаємо, що визначення загроз як факторів впливу на національну безпеку є актуальним напрямком дослідження.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Організаційні, економічні, матеріально-фінансові, правові, інформаційні та інші аспекти публічного управління національної безпеки є предметом дослідження вчених Л. Антонової, В. Баштанника, С. Бєлая, Д. Грицишена, С. Домбровської, І. Драгана, В. Євдокімова, І. Іськіва, С. Квітки, О. Кравчука, О. Крюкова, С. Крука, Е. Люттвак, С. Намбісана, Н. Нижник, В. Новікова, О. Пархоменко-Куцевіл, І. Парубчака, Г. Почепцова, О. Радченко, Л. Сергієнко, О. Сидорчук, Г. Ситника, В. Торічного, Т. Ярового та ін. [1; 2; 3; 4; 5; 7; 8; 10; 11; 14; 17]. У той же час, відзначимо, що існує необхідність у системному аналізі загроз національної безпеки в умовах розвитку інформаційного суспільства, адже ці загрози набувають усе більшої актуальності, зокрема, у напрямку використання штучного інтелекту.

ПОСТАНОВКА ЗАВДАННЯ

Метою статті є дослідження теоретичних засад і публічно-управлінських аспектів щодо впливу загроз на національну безпеку в умовах розвитку інформаційного суспільства.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Сьогодні ми маємо можливість спостерігати, з одного боку, стрімкий розвиток цифрових технологій, а з другого — посилення їхнього впливу на систему безпеки, що може мати негативний і позитивний характер, а також збільшення обсягів і потоків інформації. У цьому контексті слушно погодитись із позицією групи вчених (С. Домбровською, С. Квіткою, О. Крюковим, В. Луняком, С. Шевченко та ін. [1; 4; 9; 10; 15]), які відзначають важливість розмежування низки понять, пов'язаних із загрозами національної безпеки та розвитком інформатизації та цифровізації. З метою забезпечення коректного визначення цих понять науковці пропонують застосовувати метод історичної формалізації та системного аналізу. Ці методи дозволили авторам визначити етапи становлення інформатизації та цифровізації, а також їхнього впливу на генезу розвитку національної безпеки в Україні, а саме:

1. Комп'ютеризація (1991—1998 рр.).
2. Інформатизація (1999—2008 рр.).
3. Електронний уряд (2008—2018 рр.).
4. Цифровізація (2018 р. — по т/ч).

У продовження думок науковців відзначимо, що розвиток інформатизації та цифровізації відбувається паралельно з розвитком теорії управління як кібернетичної системи. Вона чинить взаємний вплив на систему інформатизації та цифровізації, як наслідок, ці явища та процеси зумовлюють появу нових загроз національній безпеці через збільшення обсягів інформації [1; 3; 5; 7; 8]. Це, у свою чергу, позначається на рівні цієї безпеки. Етапи розвитку автоматизації, інформатизації та цифровізації та їх впливу на глобальну безпеку у світі представлено в табл. 1.

Таблиця 1. Генеза розвитку автоматизації, інформатизації та цифровізації та їх впливу на глобальну безпеку у світі

Назва етапу	Об'єкт впливу	Ключові технології	Характеристика впливу на глобальну безпеку у світі
Автома-тизація (60 р. XX ст.)	Алгоритмізовані процеси та функції у найважливіших сферах суспільної життєдіяльності	Програмні алгоритми розрахунків, автоматизоване робоче місце, упровадження TPS (Transaction Processing System)	Розвиток постіндустріальної економіки. Формування системи національної безпеки в бік акцентування на державній безпеці
Інформа-тизація (80 р. XX ст.)	Бізнес-процеси, різні види управлінської діяльності	Аналітичні інформаційні системи, інформаційні системи управління, упровадження DSS (Decision Support System), ERP (Enterprise Resource Planning)	Стимулювання розвитку мережевої економіки, інформаційної економіки, упровадження моделі new public management, формування системи національної безпеки в бік акцентування на суспільній безпеці
Цифровізація (2000 р. і по т/ч)	Розвиток цифрового ринку та всіх сфер суспільної життєдіяльності за допомогою цифрових технологій (від економічної й управлінської діяльності). Збільшення обсягів і потоків інформації	Цифрові платформи IoT (Internet of Things), системи розподільчого реєстру, доповнена та віртуальна реальність, нейротехнології, мобільні додатки, що допомагають покращувати надання публічних послуг у межах приватного та державного секторів	Цифрова економіка, web-економіка, цифрове урядування. Формування системи національної безпеки в бік акцентування на безпеці окремо взятої особистості

Джерело: складено на підставі [1; 4; 15; 18].

Погоджуємось із закордонними вченими, які обгрунтовують зв'язок між розвитком інформатизації, цифровізації, інновацій, сталим розвитком і національною безпекою [16].

У цьому контексті відзначимо, що останніми роками розвиток цифровізації та інформаційного суспільства супроводжується збільшенням кількості збройних, військових та інших конфліктів. Це накладає відбиток на визначення аспектів інформаційної безпеки, а також інших супутніх понять, як-то, "інформаційна інфраструктура", "інформаційне суспільство" і "гібридна війна". Щодо характеристики цих понять, то відсутній єдиний науковий підхід. На наше переконання, допомогти розібратися з цим питанням може використання терміну "стратегічна комунікація" і "демпфування загроз".

У 2009 році експертами НАТО було сформульоване основне визначення "стратегічної комунікації" як процес скоординованого та належного використання в діяльності та комунікаційних можливостей НАТО механізмів публічної дипломатії, зв'язків із громадськістю, зв'язків із громадськістю військових, інформаційних операцій та психологічних операцій відповідно для підтримки публічної політики та соціальної безпеки, а також операцій і діяльності Альянсу та просування цілей НАТО [1; 5]. Згідно з цим визначенням інші поняття розглядаються в такому ключі:

1. Громадська дипломатія — це цивільні комунікації та зовнішні зусилля НАТО, відповідальні за підвищення обізнаності та формування розуміння та підтримки політики, операцій і діяльності НАТО, на додаток до внутрішніх зусиль членів Альянсу, що перебуває під постійним впливом загроз.

2. Зв'язки з громадськістю — це цивільна участь НАТО через засоби масової інформації для надання громадськості своєчасної, точної, оперативної та ініціативної інформації про політику, операції та діяльність НАТО.

3. Зв'язки з військовою громадськістю — це популяризація військових цілей і завдань НАТО серед аудиторії з метою підвищення обізнаності та розуміння військових аспектів Альянсу. Це включає планування й управління зв'язками зі ЗМІ, внутрішніми комунікаціями та зв'язками з військовою громадськістю.

4. Інформаційні операції — це військові поради та координація військової інформаційної діяльності НАТО з метою справляти бажаний вплив на волю, розуміння та можливості супротивників та інших за допомогою схвалених Північноатлантичною радою наративів на підтримку операцій, місій і цілей Альянсу.

5. Психологічні операції — це спланована психологічна діяльність із застосуванням методів комунікації та інших засобів, спрямована на визнану аудиторію з метою впливу на сприйняття, ставлення та поведінку, впливаючи на досягнення політичних і військових цілей" [там само].

На підставі аналізу вищенаведених визначень можемо зауважити, що для нашого дослідження особливу цінність мають "зв'язки з громадськістю" і "психологічні операції". Даний висновок зроблено з огляду на те, що загрози, які виникають у площині інформаційної безпеки, мають розмиті межі впливу та значною мірою відзначаються на системі національної безпеки в цілому.

На даний час визначення терміну "стратегічні комунікації" можна знайти в різних професійних і наукових джерелах. У контексті цієї дослідницької роботи, розглядаючи гібридну війну росії з Україною, слід звернути увагу загалом на концепцію стратегічної комунікації в Україні. На жаль, така концепція не становить базис для чинної Стратегії інформаційної безпеки України (2021 р.)

[6]. На цій підставі пропонуємо під час оновлення зазначеної стратегії врахувати практику щодо визначення перспективних векторів стратегічної комунікації, під якою розглядаємо засіб асиметричного захисту від інформаційної агресії росії у цій війні. До речі, уперше в Україні поняття "стратегічна комунікація" було визначено у 2015 році в прийнятій "Воєнній доктрині України" [6; 11; 12].

Воєнна доктрина України [6] визначає поняття "стратегічна комунікація" як узгоджене та доцільне використання комунікаційних можливостей держави — публічної дипломатії, зв'язків з громадськістю, військових відносин, інформаційно-психологічних операцій, діяльності для досягнення цілей держави. Ця доктрина також має містити визначення "стратегічного наративу", під яким доречно розуміти спеціально підготовлений текст, призначений для вербальної презентації в процесі стратегічної комунікації з метою інформаційного впливу на цільову аудиторію. Провідний теоретик Нідерландської академії оборони Г. Дімітріу дає таку характеристику наративу: "в основі стратегії стратегічної комунікації лежить єдиний, ретельно сконструйований стратегічний наратив, заснований на існуючих ідеях і цінностях" [1, с. 155; 5].

Приклад дій росії в Грузії, Україні, Сирії та ЄС показує, що стратегічний наратив також використовується для інтерпретації власних дій або дій іншої сторони, щоб приховати свої справжні наміри — інформаційний вплив на власне суспільство та населення інших держав із метою трансформації їхньої свідомості. у 2016 році, через два роки після окупації частини України та півроку після інтервенції в Сирії, політика росії в Європі стала системною та скоординованою. росія почала використовувати всі доступні інструменти гібридного впливу. Насамперед, це масова пропаганда, спрямована на канали публічної дипломатії та європейські ЗМІ за участю російських мовників (наприклад, Russia Today, Sputnik), яка стала інформаційною зброєю, засобом цілеспрямованого просування російської ідеології та ідеї "руского миру". У країнах Європи почали формуватися мережі лояльних до них політичних і громадських організацій, ЗМІ тощо, лояльних до росії. Здійснюючи гібридну агресію в Європі, через корупційні схеми, підкуп і шантаж, росія активізувала формування про російського лобі серед європейських політиків, громадських лідерів та громадських діячів. До них відноситься фінансова та інша допомога про російським політичним силам у Європі (наприклад, партія "Національний фронт Франції") або надання високих посад у великих корпораціях колишнім політикам, які все ще зберігають вплив (наприклад, призначення колишнього канцлера Німеччини Герхарда Шредера до ради директорів Nord Stream 1 і Nord Stream 2, і також "Роснафти") [1, с. 156; 5].

Аналізуючи діяльність росії в Європі, можна з упевненістю сказати, що вона використовує практично весь арсенал стратегічних комунікацій для досягнення власних політичних цілей. У тому числі: зв'язки з громадськістю, публічна дипломатія, зв'язки зі ЗМІ, діяльність у кіберпросторі, включаючи соціальні мережі, залучення ключових лідерів, внутрішні комунікації, інформаційні операції, психологічні операції, розвідувальна підтримка подій, демонстрація військової діяльності, введення помилок.

Гібридна війна росії проти Європи має ознаки м'якої війни, переважно інформаційної. Для цього росія створила цілу систему пропаганди та дезінформації. На підтвердження цієї тези наводяться дані дослідження Аналітичної групи гібридної війни Українського кризового медіа-центру (UCMC), проведеного спільно з Естонським центром Східного партнерства, а також дані досліджень UCMC за підтримки The Black Sea Trust for Regional Cooperation та The German Marshal Found [2]. Дослідження показали, що середнє співвідношення негативних і позитивних новин про Європу становить 85% на 15%. Європа згадується негативно в середньому 18 разів на день на опитаних каналах. Іншими словами, як пишуть російські ЗМІ, життя в Європі дуже складне — риторика, яка постійно нав'язується через незліченну кількість міфів за факти. Однак є дві країни, які зображені позитивно: Білорусь і Швейцарія. На думку дослідників, це лише тому, що російська "еліта" зберігає свої гроші в швейцарських банках і фактично вважає Білорусь частиною росії.

Отже, російська дезінформація є дуже цілеспрямованою та дисциплінованою. 88% усіх негативних новин можна розділити на шість наративів. Після створення таких наративів, вони частково підкріплюються фейковими новинами, але здебільшого навмисно маніпульованими інтерпретаціями реальних подій [14]. Ці наративи утримують увагу цільової аудиторії в бажаних рамках і є більш довговічними порівняно з фейковими новинами, тому що навіть якщо вони кидають виклик аргументам, вони не провалюються.

На наше переконання, основні наративи рф такі:

1. "Жахи життя" — повсякденне життя в Європі нестабільне, небезпечне та несправедливе.

2. "Гниюча Європа" — Європа не єдина і розпадається внаслідок розмивання моральних цінностей.

3. Протести. У Європі тривають нескінченні протести, тому що її інститути слабкі та нестабільні.

4. Тероризм. Європа небезпечна, тому що зазнає постійних нападів, яких вона заслуговує.

5. Криза біженців — Європа її спровокувала і вона не може впоратися.

6. Санкції. Санкції шкодять ЄС набагато більше, ніж росії, але США не дозволяють ЄС скасувати санкції [1; 5].

Сьогодні рф продовжує використовувати одній і ті самі наративи. Зважаючи на прагнення рф дестабілізувати ситуацію в Україні, до цих 6 наративів (від початку повномасштабної агресії проти України) може бути додано ще, а саме:

1. "Велика Вітчизняна війна" — перш за все росія врятувала Європу від фашизму (підвищивши роль росіян у Другій світовій війні, тим самим зменшивши роль інших європейських народів, зокрема поляків та українців).

2. "російський газ" — без російського газу Європа замерзне (цей наратив має вплинути на думку європейців про будівництво "Північного потоку-2").

Це дозволяє Кремлю порівнювати згадану "нестабільність" Заходу та ЄС зі "стабільністю" росії, яку слід плекати. Після створення наративи виявляються дуже стійкими до будь-якої перевірки фактів.

Таким чином, потребують застосування дієві механізми демпфування загроз національної безпеки в умовах розвитку інформаційного суспільства. Щодо кон-

струкції "демпфування загроз" у сфері національної безпеки, то можемо розглядати цей процес як інституційну діяльність з реагування (нейтралізації) і попередження загроз цій сфері, що представляє собою динамічну систему, яка знаходиться під постійним впливом зовнішніх і внутрішніх факторів. Загалом термін демпфер (нім. Dampfer "глушник, амортизатор" ← dampfen "заглушувати") відноситься до термінології галузі технічних наук, і означає пристрій для гасіння (демпфування) або запобігання коливанням, що виникають у машинах. Механізм державного управління також учені розглядають як пристрій, що приводить у рух певну систему [1; 11]. Відтак, маємо приклад парадигмального та синергетичного розвитку системи публічного (державного) управління, об'єктом якого є національна безпека. На неї чинять потужний вплив ті чи інші загрози, нейтралізувати які доцільно ще початковому етапі, тобто вчасно їх прогнозувати та попереджати. Протистояти інформаційному впливу складно, але можливо.

ВИСНОВКИ

На підставі проведеного дослідження можна зробити такі висновки:

1. Дослідження наукових напрацювань дозволило систематизувати поняття у межах обраного предмета дослідження (інформаційна загроза, гібридна війна, інформатизація, цифровізації). Акцентовано, що ці поняття характеризують явища та процеси, які чинять взаємозумовлюючий вплив (одні обумовлюють трансформацію інших). При цьому вважаємо, що інформатизація та цифровізація є процесами, що потрібно розглядати з позиції періодизації, ураховуючи, що висхідним пунктом у їх розвитку стала автоматизація. Вони покликані забезпечувати технологічний та цифровий розвиток суспільства, а також інформаційний. Щодо цифровізації, то вона представлена як сучасний етап розвитку інформаційного суспільства, що триває й донині та передбачає кількісно-якісні зміни в його межах. З метою унеможливлення негативного впливу цифровізації на розвиток інформаційного суспільства обгрунтована необхідність виваженого використання новітніх технологій.

2. У цьому контексті відзначено парадигмальність розвитку інформаційного суспільства, цифрових технологій і системи безпеки. Ця парадигмальність полягає в тому, що вищевказані явища та процеси набувають нових рис під дією зовнішніх і внутрішніх факторів, частина з яких маю загрозливий характер. На цій підставі рекомендовано розглядати національну безпеку, інформаційне суспільство та загрози ним із застосуванням також синергетичного підходу. Він дає підстави наполягати на важливості визначення стратегічних комунікацій як дієвого інструмента в протистоянні гібридним загрозам. Ця гібридність у статті розглядається як можливість застосування нетрадиційної зброї (не кінетичної) із метою масового ураження противника, який представлений населенням.

3. Доведено, що зазначені аспекти охоплюються терміном демпфування загроз національній безпеці в умовах впливу інформаційного суспільства. Цей процес означає вчасне визначення та попередження загроз у зазначеній сфері, дія яких спрямована на дестабілізацію системи безпеки в цілому та дезінформацію суспільства. Прикладом останньої є поширення державою-агресоркою серед власного, міжнародного й українського суспільства наративів, які містять викривлену та неправдиву інформацію щодо політичних, історичних, економічних, соціальних та інших явищ і процесів. Уважаємо, що протистояти таким наративам та іншим гібридним загрозам складно, але можливо. Для цього має вживатись цілий комплекс публічно-управлінських заходів. Передбачається, що це інституційні заходи, тобто політичні, соціальні, правові, організаційні та інші. Даний висновок зроблено з огляду на те, що саме держава — це соціальний інститут, і її політична, правова, організаційна та інші підсистеми включають відповідні інститути.

4. На підставі зазначеного вважаємо, що перспективи подальших наукових досліджень мають бути пов'язані з розкриттям публічно-управлінських заходів для протидії та реагування на загрози національній безпеці в умовах розвитку інформаційного суспільства, особливо в умовах впливу цифрових технологій.

Література:

1. Домбровська С.М., Помаза-Пономаренко А.Л., Крюков О.І., Порока С.Г. Інформаційні загрози та комунікативна інфраструктура в державному секторі: монографія. Харків: НУЦЗУ, 2024. 244 с.

2. Золотухін Д.Ю., Гребенюк В.М., Іванов О. Ю. Гібридна війна Російської Федерації на Балканах: монографія. Київ: НА СБУ, 2020. 260 с.

3. Лопатченко І.М., Батир Ю.Г., Помаза-Пономаренко А.Л. Державне регулювання у сфері інформаційної безпеки України в умовах воєнного стану // Вісник Національного університету цивільного захисту України. 2024. № 1 (20). С. 14—24.

4. Луняк В.Е. Шляхи вдосконалення механізмів публічного управління у сфері цифровізації в контексті забезпечення інноваційного розвитку // Публічне управління: концепції, парадигма, розвиток, удосконалення. 2024. № 9. С. 119—132.

5. Новіков В.О. Дисфукнціоналізація інституційної системи та механізмів публічного управління в умовах інформаційно-гібридних війн // Вісник Національного університету цивільного захисту України. Серія: Державне управління. 2020. Вип. 2 (13). С. 345—354.

6. Офіційний веб-сайт Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/2469-19. (дата звернення 17.01.2025).

7. Помаза-Пономаренко А.Л., Новіков В.О. Шляхи трансформації інституційних механізмів публічного управління в Україні: від інформаційних загроз до гібридних війн // Державне будівництво. 2023. № 1. URL: https://periodicals.karazin.ua/db/issue/archive. (дата звернення 17.01.2025).

8. Помаза-Пономаренко А.Л., Тарадуда Д.В. Службово-бойова діяльність сил охорони правопорядку та міжнародне гуманітарне право // Державне управління: удосконалення та розвиток. 2024. № 3. URL: https://www.nayka.com.ua/index.php/dy/article/view/3229. (дата звернення 17.01.2025).

9. Помаза-Пономаренко А.Л., Тарадуда Д.В. Особливості управління й експлуатації об'єктів критичної

інфраструктури в контексті забезпечення інформаційної безпеки // Успіхи і досягнення у науці. 2024. № 3. Том 2. С. 208—220.

10. Почепцов Г. Токсичний інфопростір. Як зберегти ясність мислення і свободу дії. Харків: Віват, 2022. 384 с.

11. Радченко О.В. Родові ознаки категорії "механізм" в соціальних науках // Публічне управління: теорія та практика. 2013. Вип. 3. С. 19—25.

12. Свідоцтво про реєстрацію авторського права на твір від 11.07.2024 р. № 128240 // Спеціальна інформаційна система Українського національного офісу інтелектуальної власності та інновацій. URL: https://sis.nipo.gov.ua/uk/search/simple/ (дата звернення 17.01.2025).

13. Свідоцтво про реєстрацію авторського права на твір від 05.08.2024 р. № 128848 // Спеціальна інформаційна система Українського національного офісу інтелектуальної власності та інновацій. URL: https://sis.nipo.gov.ua/uk/search/simple/ (дата звернення 17.01.2025).

14. Luttwak E.N. Coup d'tat: A Practical Handbook. Harvard University Press, Cambridge, Massachusetts, London, England, 1979. 728 p.

15. Kvitka S., BorodinYe., Yemelyanov V. & Ivashova L. The foresight of national economy's digital development. Revista inclusiones. 2020. 7 (SI) P. 112—125.

16. Nambisan S., Lyytinen K., Majchrzak A., Song M. Digital Innovation Management: Reinventing innovation management research in a digital world // Mis Quarterly. 2017. Vol. 41. No. 1. pp. 223-238.

17. Pomaza-Ponomarenko A., Krukov O., Kravchuk O., Hubenko I., Taraduda D. Managing emergencies: utilising historical insights for strategic enhancement // AD ALTA: Journal of Interdisciplinary Research. 2024. Pp. 135—139.

18. The World Bank Digital Adoption Index. URL: https://www.worldbank.org/en/publication/wdr2019. (дата звернення 17.01.2025).

References:

1. Dombrovska, S.M., Pomaza-Ponomarenko, A.L., Kryukov, O.I. and Poroka, S.G. (2024), Informatsiyni zahrozy ta komunikatyvna infrastruktura v derzhavnomu sektori [Information threats and communication infrastructure in the power sector], NUTSZU, Kharkiv, Ukraine.

2. Zolotukhin, D.Yu., Grebenyuk, V.M. and Ivanov, O.Yu. (2020), Hibrydna viyna Rosiys'koyi Federatsiyi na Balkanakh [Hybrid war of the Russian Federation in the Balkans], NA SBU, Kyiv, Ukraine.

3. Lopatchenko I.M., Batyr Y.G. and Pomaza-Ponomarenko, A.L. (2024), "State regulation in the sphere of information security of Ukraine under martial law", Visnyk Natsional'noho universytetu tsyvil'noho zakhystu Ukrayiny, vol. 1 (20), pp. 14—24.

4. Lunyak, V.E. (2024), "Ways to improve public administration mechanisms in the sphere of digitalization in the context of ensuring innovative development", Publichne upravlinnya: kontseptsiyi, paradyhma, rozvytok, udoskonalennya, vol. 9, pp. 119—132.

5. Novikov, V.O. (2020), "Dysfunctionalization of the institutional system and mechanisms of public administration in the conditions of information and hybrid wars", Visnyk Natsional'noho universytetu tsyvil'noho zakhystu Ukrayiny, vol. 2 (13), pp. 345—354.

6. Official website of the Verkhovna Rada of Ukraine (2024), "Legislation", available at: https://zakon.rada.gov.ua/laws (Accessed 17 Jan 2025).

7. Pomaza-Ponomarenko, A.L. and Novikov, V.O. (2023), "Ways of transformation of institutional mechanisms of public administration in Ukraine: from informational threats to hybrid wars", Derzhavne budivnytstvo, [Online], vol. 1 (33), available at: https://periodicals.karazin.ua/db/article/view/22921 (Accessed 17 Jan 2025).

8. Pomaza-Ponomarenko, A.L. and Taraduda, D.V. (2024), "Service and combat activities of law enforcement forces and international humanitarian law", Derzhavne upravlinnya: udoskonalennya ta rozvytok, [Online], vol. 3. available at: https://www.nayka.com.ua/index.php/dy/article/view/3229. (Accessed 17 Jan 2025).

9. Pomaza-Ponomarenko, A.L. and Taraduda, D.V. (2024), "Features of management and operation of critical infrastructure facilities in the context of ensuring information security", Uspikhy i dosyahnennya u nautsi, vol. 3, issue 2, pp. 208—220.

10. Pocheptsov, G. (2022), Toksychnyy infoprostir. Yak zberehty yasnist? myslennya i svobodu diyi [Toxic infospace. How to preserve clarity of thought and freedom of action], Vivat, Kharkiv, Ukraine.

11. Radchenko, O.V. (2013), "Generic features of the category "mechanism" in the social sciences", Publichne upravlinnya: teoriya ta praktyka, Issue 3, pp. 19—25.

12. Special information system of the Ukrainian National Office of Intellectual Property and Innovation (2024), "Certificate of copyright registration for the work dated July 11, 2024, No. 128240", available at: https://sis.nipo.gov.ua/uk/search/simple/ (Accessed 17 Jan 2025).

13. Special information system of the Ukrainian National Office of Intellectual Property and Innovation (2024), "Certificate of copyright registration for the work dated August 05, 2024, No. 128848", available at: https://sis.nipo.gov.ua/uk/search/simple/ (Accessed 17 Jan 2025).

14. Luttwak, E.N. (1979), Coup d'tat: A Practical Handbook, Harvard University Press, Cambridge, Massachusetts, London, England.

15. Kvitka, S., Borodin, Ye., Yemelyanov, V. and Ivashova, L. (2020), "The foresight of national economy's digital development", Revista inclusiones, vol. 7 (SI), pp. 112—125.

16. Nambisan, S., Lyytinen, K., Majchrzak, A. and Song, M. (2017), "Digital Innovation Management: Reinventing innovation management research in a digital world", Mis Quarterly, vol. 41, No. 1, pp. 223—238.

17. Pomaza-Ponomarenko, A., Krukov, O., Kravchuk, O., Hubenko, I. and Taraduda, D. (2024), "Managing emergencies: utilising historical insights for strategic enhancement", AD ALTA: Journal of Interdisciplinary Research, vol. 2, pp. 135—139.

18. The World Bank Digital Adoption Index (2019), "World Development Report 2019", available at: https://www.worldbank.org/en/publication/wdr2019. (Accessed 17 Jan 2025).

Стаття надійшла до редакції 17.01.2025 р.