DOI: 10.52363/2414-5866-2023-1-39
УДК: 351:007:004.056:355.02(477)

Новак В. М. *- магістр публічного адміністрування, аспірант Національного університету цивільного захисту України м. Черкаси*
ORCID: 0009-0003-6516-0742

Novak V. *- Master of Public Administration, PhD student at the National University of Civil Defence of Ukraine*

УРАЗЛИВОСТІ ІНФОРМАЦІЙНИХ КОМУНІКАЦІЙ В УМОВАХ ГІБРИДНИХ ЗАГРОЗ: МЕХАНІЗМИ ДЕРЖАВНОЇ ПРОТИДІЇ

VULNERABILITIES OF INFORMATION COMMUNICATIONS UNDER HYBRID THREATS: STATE COUNTERACTION MECHANISMS

Дослідження присвячене комплексному аналізу механізмів мінімізації вразливостей мережевих комунікацій в системі публічного управління України. Актуальність теми зумовлена стрімкою цифровізацією суспільства, зростанням ролі інформаційних комунікацій у функціонуванні державних інституцій та появою нових викликів для національної безпеки в умовах гібридних загроз. У статті проаналізовано природу та специфіку вразливостей мережевих інформаційних комунікацій як об'єкта публічного управління. Досліджено трансформацію комунікаційних практик в епоху мережевого суспільства, виявлено ключові характеристики масових самокомунікацій та їхній вплив на систему державного управління. Особливу увагу приділено аналізу делокалізованості, неісчислимості та некомпенсованості ризиків сучасних мережевих комунікацій.

Розкрито амбівалентний характер сетевізації комунікаційного простору: з одного боку, розширення можливостей для горизонтальної взаємодії між громадянами та владою, з іншого – зростання системних вразливостей, що потребують нових підходів до публічного управління. Проаналізовано dichotomію рискофобії та рискофілії як суб'єктивних факторів, що впливають на ефективність державного регулювання інформаційної сфери. Сформульовано концептуальні засади механізмів мінімізації вразливостей, що базуються на принципах превентивності, системності та адаптивності публічного управління в умовах постійного ускладнення інформаційного середовища.

Ключові слова: *мережеві комунікації, вразливості, публічне управління, інформаційна безпека, масові самокомунікації, цифровізація, ризики, механізми державного регулювання.*

The study is devoted to a comprehensive analysis of mechanisms for minimizing vulnerabilities of network communications in the public administration system of Ukraine. The relevance of the topic is determined by rapid digitalization of society, growing role of information communications in functioning of state institutions, and emergence of new challenges to national security under hybrid threats conditions. The article analyzes the nature and specifics of vulnerabilities of network information communications as an object of public administration. The transformation of communication practices in the network society era is examined, key characteristics of mass self-communications and their impact on the public administration system are identified. Particular attention is paid to analyzing delocalization, incalculability and non-compensability of risks of modern network communications.

The ambivalent nature of communication space networking is revealed: on one hand, expansion of opportunities for horizontal interaction between citizens and authorities, on the other hand – growth of systemic vulnerabilities requiring new approaches to public administration. The dichotomy of risk-phobia and risk-philia as subjective factors affecting effectiveness of state regulation of information sphere is analyzed. Conceptual foundations of vulnerability minimization mechanisms based on principles of preventiveness, systematicity and adaptability of public administration under conditions of constantly increasing complexity of information environment are formulated.

Keywords: *network communications, vulnerabilities, public administration, information security, mass self-communications, digitalization, risks, state regulation mechanisms.*

Аналіз останніх досліджень і публікацій. Проблематика інформаційних комунікацій у системі публічного управління активно досліджується вітчизняними науковцями, що зумовлено зростанням ролі цифрових технологій у функціонуванні державних інституцій. К. М. Майстренко аналізує комунікації у діяльності органів публічної влади, визначаючи їх як офіційний, юридично цілеспрямований регламентований рух суб'єктів управління до соціальної спільності. Дослідниця наголошує на важливості комунікативного процесу незалежно від форми комунікації, що підтверджує актуальність питання для сучасного публічного управління. Х. Федорищак та Л. Мосора розглядають роль засобів масової інформації у сфері публічної політики, аналізуючи їхній вплив на формування громадської думки та взаємодію влади з суспільством. В. А. Гошовська та Л. А. Пашко у своєму навчальному посібнику систематизують аспекти організаційної культури та ділового спілкування в публічному управлінні, закладаючи теоретичні основи для розуміння комунікативних процесів у державних структурах.

Особливої уваги заслуговує дослідження Л. М. Бєлкіна, Ю. Л. Юринця, М. Л. Бєлкіна та Є. В. Криволапа, присвячене співвідношенню понять «інформаційна безпека», «безпека інформації» та «кібербезпека» в контексті безпекових

стратегій України 2020–2021 років. Автори чітко розмежовують ці категорії та обґрунтовують їхнє значення для національної безпеки в умовах гібридних загроз. Н. Б. Капустіна вводить до наукового обігу концептуальні основи теорії мережевого суспільства М. Кастельса, адаптуючи їх до українського контексту. Фундаментальна праця самого М. Кастельса "The Rise of the Network Society" залишається базовим джерелом для розуміння трансформації суспільних відносин в епоху інформаційних технологій, визначаючи мережеву логіку як основу сучасної соціальної морфології. Водночас аналіз наукових публікацій виявляє недостатню розробленість питання механізмів мінімізації вразливостей саме мережевих комунікацій у системі публічного управління України, що актуалізує необхідність подальших досліджень у цьому напрямі з урахуванням специфіки сучасних викликів національній безпеці.

Постановка проблеми. В умовах стрімкої цифровізації суспільства та трансформації комунікаційного простору проблема вразливостей мережевих інформаційних комунікацій набуває особливої актуальності для системи публічного управління України. Експансія мережі Інтернет, поява нових форм масових самокомунікацій та зростання ролі цифрових платформ у взаємодії влади, бізнесу та громадянського суспільства формують якісно нове середовище, що характеризується нелінійністю, відсутністю єдиного центру координації та складністю прогнозування наслідків комунікативних процесів. Традиційні механізми державного регулювання, які базувалися на контролі централізованих медіа та ієрархічних структур поширення інформації, виявляються недостатньо ефективними перед обличчям викликів мережевого суспільства, де кожен індивідуальний актор потенційно здатен генерувати контент масового охоплення.

Специфіка сучасного етапу розвитку України, позначеного необхідністю протидії гібридним загрозам, дезінформаційним кампаніям та забезпечення кібербезпеки, актуалізує потребу в науковому обґрунтуванні механізмів мінімізації вразливостей мережевих комунікацій. Делокалізованість джерел інформаційних впливів, неісчислимість потенційних ризиків та амбівалентність наслідків комунікативних практик у цифровому просторі вимагають від органів публічної влади переходу від реактивних моделей реагування до проактивних стратегій превентивного управління. При цьому критично важливим є збалансування завдань забезпечення інформаційної безпеки держави з принципами свободи слова, доступу до інформації та розвитку цифрової демократії, що становить складне завдання для теорії і практики державного управління.

Метою статті є теоретичне обґрунтування та систематизація механізмів мінімізації вразливостей мережевих комунікацій у системі публічного управління України. Завдання дослідження полягають у виявленні специфічних характеристик вразливостей інформаційних комунікацій мережевого типу, аналізі їхнього впливу на функціонування інституцій публічної влади та формулюванні концептуальних засад управлінських механізмів, спрямованих на мінімізацію

виявлених вразливостей в умовах цифрової трансформації українського суспільства.

Виклад основного матеріалу дослідження. Трансформація інформаційного простору в епоху цифровізації зумовила появу якісно нових форм комунікативної взаємодії, що суттєво впливають на функціонування системи публічного управління. Як справедливо зазначає М. Кастельс, мережеве суспільство характеризується фундаментальною зміною соціальної морфології, де «саме мережі складають нову соціальну морфологію наших суспільств, а розповсюдження мережевої логіки значною мірою позначається на ході і результаті процесів» [9, с. 494]. Ця теоретична рамка є ключовою для розуміння природи вразливостей, що виникають у сучасних інформаційних комунікаціях.

В українському науковому дискурсі питання комунікацій у публічному управлінні розглядається через призму офіційного, юридично цілеспрямованого регламентованого руху суб'єктів управління. К. М. Майстренко визначає, що комунікації у системі публічного управління є «офіційним, юридично цілеспрямованим регламентованим рухом індивідуальних суб'єктів управління до соціальної спільності із збереженням за цими суб'єктами певної автономності, самостійності, самодіяльності, індивідуальності» [1, с. 94]. Однак таке визначення, попри свою точність, не повною мірою враховує специфіку мережевих комунікацій, де традиційні ієрархічні моделі поступаються місцем горизонтальним зв'язкам і децентралізованим структурам взаємодії.

Вразливості мережевих інформаційних комунікацій у системі публічного управління мають комплексний характер і виявляються на різних рівнях функціонування державних інституцій. На відміну від традиційних загроз, що мали локалізований характер, сучасні вразливості характеризуються делокалізованістю, неісчислимістю та складністю прогнозування наслідків. Це зумовлено самою природою мережевих структур, де, за теорією М. Кастельса, простір потоків замінює просторову логіку традиційного суспільства [9]. Перша група вразливостей пов'язана з технологічними особливостями функціонування мережевих комунікацій. Цифровізація публічного управління, попри свої беззаперечні переваги у плані оперативності, доступності та прозорості, створює нові точки вразливості інформаційної інфраструктури держави. Закон України «Про електронні комунікації» визначає правові та організаційні основи державної політики у цій сфері [8], однак швидкість технологічних змін випереджає можливості нормативно-правового регулювання. Виникає ситуація, коли державні інформаційні системи стають об'єктами потенційних кібератак, несанкціонованого доступу та маніпуляцій з даними.

Друга група вразливостей має організаційно-управлінський характер. В. А. Гошовська та Л. А. Пашко у своєму дослідженні комунікацій у публічному управлінні наголошують на важливості організаційної культури та професійних компетенцій державних службовців [5]. Проте мережеві комунікації вимагають принципово нових навичок і підходів до управлінської діяльності. Традиційна

ієрархічна модель прийняття рішень виявляється неефективною в умовах, коли інформаційні потоки рухаються горизонтально, а джерела інформації множаться експоненційно. Органи публічної влади стикаються з проблемою адаптації до нових форм комунікативної взаємодії, де громадяни не є пасивними реципієнтами державних послуг, а активними учасниками формування публічної політики через цифрові платформи та соціальні мережі.

Третя група вразливостей стосується інформаційної безпеки та захисту даних. Л. М. Бєлкін, Ю. Л. Юринець, М. Л. Бєлкін та Є. В. Криволап у своєму дослідженні чітко розмежовують поняття «інформаційна безпека», «безпека інформації» та «кібербезпека», наголошуючи на їхньому різному змістовному наповненні та функціональному призначенні [3]. Вразливість мережевих комунікацій у цьому контексті виявляється у складності забезпечення комплексного захисту інформаційних ресурсів держави, персональних даних громадян та критичної інфраструктури від зовнішніх і внутрішніх загроз. Закон України «Про основні засади забезпечення кібербезпеки України» визначає базові принципи державної політики у цій сфері [7], однак практична реалізація цих принципів стикається з численними викликами технічного, організаційного та фінансового характеру.

Особливої актуальності проблема вразливостей мережевих комунікацій набуває в контексті гібридних загроз національній безпеці України. Х. Федорищак та Л. Мосора, аналізуючи роль засобів масової інформації у сфері публічної політики, підкреслюють, що медіа стали «інструментом конструювання політичних порядків та відносин між владою й громадськістю» [2, с. 87]. У сучасних умовах ця роль набуває особливого значення, оскільки інформаційний простір перетворюється на арену протиборства, де поряд з традиційними ЗМІ активно функціонують численні канали цифрових комунікацій. Вразливість полягає у можливості використання мережевих комунікацій для поширення дезінформації, маніпулювання громадською думкою та дестабілізації суспільно-політичної ситуації. Делокалізованість джерел інформації ускладнює ідентифікацію та нейтралізацію дезінформаційних впливів. Стратегія кібербезпеки України, затверджена Указом Президента України від 26.08.2021 № 447/2021 [8], визначає пріоритетні напрями протидії кіберзагрозам, однак динамічність інформаційного середовища вимагає постійної адаптації механізмів державного реагування.

Особливу вразливість становить феномен «інформаційних бульбашок» та «ехо-камер» у соціальних мережах, де користувачі отримують інформацію переважно від джерел, що підтверджують їхні попередні переконання. Це створює фрагментований інформаційний простір, де різні групи населення живуть у паралельних інформаційних реальностях. Для органів публічної влади це означає ускладнення комунікації з громадянами, необхідність диференційованих підходів до різних цільових аудиторій та ризик втрати довіри до офіційних джерел інформації.

Розробка ефективних механізмів мінімізації вразливостей мережевих комунікацій у системі публічного управління має базуватися на комплексному підході, що поєднує технологічні, організаційні, правові та комунікативні інструменти. Н. Б. Капустіна, розглядаючи концептуальні основи теорії мережевого суспільства М. Кастельса, наголошує на необхідності адаптації управлінських практик до мережевої логіки функціонування сучасного соціуму [4]. Це означає, що механізми мінімізації вразливостей не можуть обмежуватися простим посиленням контролю або обмеженням доступу до інформації, а мають бути спрямовані на формування резільєнтності (стійкості) системи публічного управління до інформаційних викликів.

Перший принцип – превентивність. Механізми мінімізації вразливостей мають бути орієнтовані не стільки на реагування на вже виниклі загрози, скільки на їх попередження та раннє виявлення. Це вимагає створення системи постійного моніторингу інформаційного простору, аналізу трендів та слабких сигналів, що можуть свідчити про наростання вразливостей. Комунікації у діяльності органів публічної влади, як зазначає К. М. Майстренко, мають бути проактивними, а не реактивними [1]. Органи державної влади повинні не лише відповідати на інформаційні виклики, але й формувати порядок денний, активно комунікувати з громадянами та запобігати виникненню інформаційних криз.

Другий принцип – системність. Вразливості мережевих комунікацій не можуть бути усунені точковими заходами. Необхідний комплексний підхід, що охоплює всі рівні публічного управління – від центральних органів виконавчої влади до органів місцевого самоврядування. В. А. Гошовська та Л. А. Пашко підкреслюють важливість організаційної культури та інституційних механізмів у забезпеченні ефективної комунікації [5]. Системний підхід передбачає координацію дій різних суб'єктів публічного управління, узгодження стратегій та тактик, створення єдиного інформаційного простору для обміну даними про загрози та вразливості.

Третій принцип – адаптивність. Динамічність інформаційного середовища вимагає постійної адаптації механізмів мінімізації вразливостей до нових викликів. Як зазначають Л. М. Бєлкін та співавтори, безпекові стратегії України мають враховувати швидкість технологічних змін та еволюцію загроз [3]. Це означає необхідність регулярного перегляду та оновлення підходів до забезпечення інформаційної безпеки, впровадження нових технологій захисту, підвищення кваліфікації персоналу та вдосконалення нормативно-правової бази.

На практичному рівні мінімізація вразливостей мережевих комунікацій вимагає реалізації конкретних заходів у кількох ключових напрямах. По-перше, технологічне забезпечення. Закон України «Про електронні комунікації» створює правову основу для розвитку захищеної інформаційно-комунікаційної інфраструктури [8]. Практична реалізація цих положень передбачає впровадження сучасних систем кіберзахисту, шифрування даних, багаторівневої автентифікації користувачів, систем виявлення та запобігання вторгненням.

Критично важливим є забезпечення кібербезпеки критичної інформаційної інфраструктури держави, що передбачає регулярне проведення аудитів безпеки, тестування на проникнення та оновлення програмного забезпечення.

По-друге, організаційно-управлінське забезпечення. Необхідне формування інституційної спроможності органів публічної влади ефективно функціонувати в умовах мережевих комунікацій. Це включає розробку та впровадження стандартів інформаційної безпеки, протоколів кризової комунікації, механізмів координації між різними органами влади. Х. Федорищак та Л. Мосора наголошують на важливості професіоналізації комунікативної діяльності в органах публічної влади [2]. Це вимагає підготовки фахівців з цифрових комунікацій, медіаграмотності державних службовців, формування культури інформаційної безпеки на всіх рівнях публічного управління.

По-третє, нормативно-правове забезпечення. Закон України «Про основні засади забезпечення кібербезпеки України» та Стратегія кібербезпеки України створюють базову правову рамку [7; 8], однак динамічність загроз вимагає постійного оновлення законодавства. Необхідна розробка спеціалізованих нормативних актів, що регулюють окремі аспекти інформаційної безпеки – від захисту персональних даних до протидії дезінформації, від забезпечення кіберстійкості критичної інфраструктури до регулювання діяльності цифрових платформ.

По-четверте, комунікативне забезпечення. Мінімізація вразливостей передбачає не лише технічний захист, але й формування довіри громадян до офіційних джерел інформації, підвищення медіаграмотності населення, розвиток критичного мислення щодо інформації, що споживається через мережеві канали. К. М. Майстренко підкреслює важливість діалогу між владою та громадськістю [1]. Органи публічної влади мають активно використовувати можливості цифрових комунікацій для інформування громадян, залучення їх до процесів прийняття рішень, оперативного реагування на запити та скарги.

Аналіз міжнародного досвіду свідчить про різноманітність підходів до мінімізації вразливостей мережевих комунікацій. М. Кастельс у своєму фундаментальному дослідженні показує, як різні країни адаптуються до викликів інформаційної епохи, розробляючи власні моделі управління інформаційними потоками [9]. Європейський Союз робить акцент на захисті персональних даних та конфіденційності (GDPR), США – на забезпеченні національної кібербезпеки та протидії кіберзлочинності, країни Північної Європи – на цифровій інклюзії та електронному урядуванні. Для України адаптація міжнародного досвіду має враховувати специфіку національного контексту – геополітичну ситуацію, рівень розвитку цифрової інфраструктури, особливості політичної культури та рівень довіри до державних інституцій. Н. Б. Капустіна справедливо зазначає необхідність критичного переосмислення західних теорій відповідно до української реальності [4]. Механізми мінімізації вразливостей мають бути адаптовані до умов перехідного суспільства, де традиційні та мережеві форми

комунікації співіснують, часто конфліктують, але поступово інтегруються у єдиний комунікативний простір.

Важливим аспектом є врахування досвіду країн Центральної та Східної Європи, що пройшли шлях демократичних трансформацій та інтеграції до європейського інформаційного простору. Естонія, наприклад, демонструє успішну модель електронного урядування та кібербезпеки, Польща – ефективні механізми протидії дезінформації, Чехія – розвиток медіаграмотності та критичного мислення. Ці практики можуть бути адаптовані до українського контексту з урахуванням національних особливостей та пріоритетів. Стратегія кібербезпеки України [8] визначає євроатлантичну інтеграцію як один з пріоритетних напрямів, що передбачає гармонізацію українського законодавства з європейськими стандартами, участь у міжнародних ініціативах з кібербезпеки, обмін досвідом та кращими практиками. Це створює сприятливі умови для імплементації перевірених міжнародних підходів до мінімізації вразливостей мережевих комунікацій.

Розвиток механізмів мінімізації вразливостей мережевих комунікацій у системі публічного управління має відбуватися у кількох взаємопов'язаних напрямах. По-перше, технологічний напрям передбачає впровадження нових технологій захисту інформації, розвиток штучного інтелекту для моніторингу та аналізу інформаційних загроз, використання блокчейн-технологій для забезпечення прозорості та незмінності даних. Органи публічної влади мають активно інвестувати у розвиток цифрової інфраструктури, забезпечуючи її стійкість та надійність.

Інституційний напрям вимагає формування спеціалізованих структур, відповідальних за кібербезпеку та інформаційну безпеку на всіх рівнях публічного управління. Це включає створення центрів реагування на кіберінциденти, координаційних рад з питань інформаційної безпеки, спеціалізованих підрозділів у органах державної влади. Необхідна чітка регламентація повноважень та відповідальності, механізмів взаємодії між різними суб'єктами забезпечення інформаційної безпеки.

Освітній напрям передбачає підготовку кваліфікованих фахівців з кібербезпеки, цифрових комунікацій та управління інформаційними ризиками. В. А. Гошовська та Л. А. Пашко наголошують на важливості професійної підготовки державних службовців [5]. Необхідне впровадження спеціалізованих освітніх програм, курсів підвищення кваліфікації, сертифікації фахівців з інформаційної безпеки. Не менш важливим є підвищення загальної медіаграмотності населення, формування культури безпечної поведінки в мережі.

Дослідницький напрям вимагає поглибленого вивчення природи вразливостей мережевих комунікацій, розробки методології їх оцінки та прогнозування. Теорія мережевого суспільства М. Кастельса [9] надає концептуальну рамку для такого аналізу, однак необхідні емпіричні дослідження української специфіки, моніторинг динаміки загроз, аналіз ефективності

впроваджених механізмів захисту. Критично важливим є забезпечення балансу між безпекою та відкритістю, між захистом від загроз та дотриманням прав і свобод громадян. Як зазначають Л. М. Бєлкін та співавтори, безпекові стратегії не повинні призводити до обмеження демократичних прав та свобод [3]. Механізми мінімізації вразливостей мають бути пропорційними загрозам, прозорими у своєму застосуванні та підконтрольними демократичним інститутам.

Висновки дослідження та перспективи подальших розвідок у цьому напрямі. Вразливості мережевих комунікацій у системі публічного управління України мають системний характер і виявляються на технологічному, організаційно-управлінському та інформаційно-безпековому рівнях. Теоретичне обґрунтування природи цих вразливостей через призму концепції мережевого суспільства М. Кастельса засвідчило, що трансформація від ієрархічних до мережевих структур комунікації зумовлює якісно нові виклики для органів публічної влади, пов'язані з делокалізованістю джерел інформації, неісчислимістю потенційних ризиків та складністю прогнозування наслідків комунікативних процесів. Аналіз чинного законодавства України у сфері кібербезпеки та електронних комунікацій виявив наявність базової нормативно-правової рамки, проте актуалізував потребу в її постійному оновленні відповідно до динаміки технологічних змін та еволюції загроз національній безпеці.

Сформульовані концептуальні засади механізмів мінімізації вразливостей, що базуються на принципах превентивності, системності та адаптивності, визначають стратегічні орієнтири для вдосконалення публічного управління в умовах цифрової трансформації. Встановлено, що ефективна мінімізація вразливостей вимагає інтегрованого підходу, що поєднує технологічне забезпечення кіберзахисту, організаційно-управлінську модернізацію державних інституцій, удосконалення нормативно-правового регулювання та розвиток комунікативних компетенцій як державних службовців, так і громадян. Адаптація міжнародного досвіду до українського контексту має враховувати специфіку геополітичної ситуації, рівень розвитку цифрової інфраструктури та особливості політичної культури, зберігаючи при цьому баланс між забезпеченням безпеки та дотриманням демократичних прав і свобод.

Перспективи подальших наукових розвідок у цьому напрямі пов'язані з поглибленим емпіричним дослідженням ефективності впроваджених механізмів мінімізації вразливостей, розробкою методології оцінки рівня кіберстійкості органів публічної влади, аналізом впливу штучного інтелекту та блокчейн-технологій на трансформацію вразливостей мережевих комунікацій. Актуальним напрямом є дослідження механізмів формування медіаграмотності та критичного мислення громадян як інструменту підвищення резильєнтності суспільства до інформаційних загроз. Потребує подальшого наукового обґрунтування питання оптимального співвідношення державного регулювання та саморегулювання у сфері мережевих комунікацій, а також розробка моделей публічно-приватного партнерства для забезпечення кібербезпеки критичної інфраструктури держави.

Список використаних джерел:

1. Майстренко К. М. Комунікації у діяльності органів публічної влади. Публічне урядування. 2022. № 1(29). С. 93-98. DOI: https://doi.org/10.32689/2617-2224-2022-1(29)-13
2. Федорищак Х., Мосора Л. Місце та роль засобів масової інформації у сфері публічної політики. Наукові праці Міжрегіональної Академії управління персоналом. Політичні науки та публічне управління. 2022. № 1(61). С. 86-91. DOI: https://doi.org/10.32689/2523-4625-2022-1(61)-13
3. Бєлкін Л. М., Юринець Ю. Л., Бєлкін М. Л., Криволап Є. В. Співвідношення понять «інформаційна безпека», «безпека інформації», «кібербезпека» в контексті безпекових стратегій України 2020–2021 років. Scientific Works of National Aviation University. Series: Law Journal «Air and Space Law». 2022. № 3(64). С. 78–86.
4. Капустіна Н. Б. Мережеве суспільство: введення в концептуальні основи теорії М. Кастельса. Правове життя сучасної України : матеріали Міжнар. наук.-практ. конф. (м. Одеса, 15 трав. 2020 р.). Одеса : Гельветика, 2020. Т. 1. С. 21-24.
5. Гошовська В. А., Пашко Л. А. Комунікації в публічному управлінні: аспекти організаційної культури та ділового спілкування : навч. посіб. Київ : К.І.С., 2016. 130 с.
6. Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 10.11.2022).
7. Закон України «Про електронні комунікації» від 16.12.2020 № 1089-IX. URL: https://zakon.rada.gov.ua/laws/show/1089-20 (дата звернення: 10.11.2022).
8. Указ Президента України «Про рішення Ради національної безпеки і оборони України "Про Стратегію кібербезпеки України"» від 26.08.2021 № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021 (дата звернення: 10.11.2022).
9. Castells M. The Rise of the Network Society. The Information Age: Economy, Society and Culture. Vol. I. Oxford: Blackwell Publishers, 1996. 556 p.

References:

1. Maistrenko, K.M. (2022), "Communications in the activities of public authorities", Publichne uriaduvannia, vol. 1(29), pp. 93-98. DOI: https://doi.org/10.32689/2617-2224-2022-1(29)-13
2. Fedoryshchak, Kh. and Mosora, L. (2022), "The place and role of mass media in the sphere of public policy", Naukovi pratsi Mizhrehionalnoi Akademii upravlinnia personalom. Politychni nauky ta publichne upravlinnia, vol. 1(61), pp. 86-91. DOI: https://doi.org/10.32689/2523-4625-2022-1(61)-13
3. Bielkin, L.M., Yurynets, Yu.L., Bielkin, M.L. and Kryvolap, Ye.V. (2022), "The relationship between the concepts of 'information security', 'information safety',

'cybersecurity' in the context of Ukraine's security strategies 2020-2021", Scientific Works of National Aviation University. Series: Law Journal "Air and Space Law", vol. 3(64), pp. 78-86.

4. Kapustina, N.B. (2020), "Network society: introduction to the conceptual foundations of M. Castells' theory", Pravove zhyttia suchasnoi Ukrainy : materialy Mizhnar. nauk.-prakt. konf. [Legal life of modern Ukraine: materials of International scientific-practical conference], Helvetyka, Odesa, Ukraine, May 15, vol. 1, pp. 21-24.

5. Hoshovska, V.A. and Pashko, L.A. (2016), Komunikatsii v publichnomu upravlinni: aspekty orhanizatsiinoi kultury ta dilovoho spilkuvannia [Communications in public administration: aspects of organizational culture and business communication], K.I.S., Kyiv, Ukraine.

6. The Verkhovna Rada of Ukraine (2017), The Law of Ukraine "On the basic principles of ensuring cybersecurity of Ukraine", available at: https://zakon.rada.gov.ua/laws/show/2163-19 (Accessed 10 November 2022).

7. The Verkhovna Rada of Ukraine (2020), The Law of Ukraine "On Electronic Communications", available at: https://zakon.rada.gov.ua/laws/show/1089-20 (Accessed 10 November 2022).

8. President of Ukraine (2021), Decree "On the decision of the National Security and Defense Council of Ukraine 'On the Cybersecurity Strategy of Ukraine'", available at: https://zakon.rada.gov.ua/laws/show/447/2021 (Accessed 10 November 2022).

9. Castells, M. (1996), The Rise of the Network Society. The Information Age: Economy, Society and Culture, vol. I, Blackwell Publishers, Oxford, UK.