

УДК 316.774: 659.4

**Пискун Дмитро Володимирович**

*аспірант*

*ЗВО «Відкритий міжнародний університет розвитку людини «Україна»*

**Pyskun Dmytro**

*Postgraduate Student of the*

*Open International University of Human Development «Ukraine»*

ORCID: 0009-0007-5004-2670

DOI: 10.25313/2617-572X-2025-12-11693

## УПРАВЛІННЯ РЕПУТАЦІЙНИМИ ТА ІНФОРМАЦІЙНИМИ РИЗИКАМИ ПУБЛІЧНИХ ОСІБ: СУЧАСНІ СТРАТЕГІЇ КОМУНІКАТИВНОЇ ПОВЕДІНКИ В ЦИФРОВУ ЕПОХУ

### PUBLIC FIGURES' REPUTATION AND INFORMATION RISK MANAGEMENT: MODERN COMMUNICATION STRATEGIES IN THE DIGITAL AGE

**Анотація.** Вступ. У цифрову епоху публічні особи опиняються в умовах суттєво підвищеної вразливості до репутаційних та інформаційних ризиків, що виникають у середовищі надшвидких комунікацій, соціальних мереж та алгоритмічно керованих інформаційних потоків. Феномени віральності контенту, дезінформації, маніпулятивних кампаній і технологій генеративних медіа створюють нові типи загроз, які традиційні інструменти комунікації вже не здатні ефективно нейтралізувати. У таких умовах миттєві реакції аудиторій, емоційна поляризація та руйнування інституційних каналів довіри значно підсилюють потенційний репутаційний збиток, а навіть дрібні інформаційні інциденти можуть трансформуватися в масштабні кризи, що впливають на соціальний статус, політичні позиції та професійну діяльність публічних діячів.

**Мета.** Метою статті є здійснення комплексного аналізу репутаційних та інформаційних ризиків, з якими стикаються публічні особи в умовах цифрової епохи, а також розроблення й обґрунтування сучасних стратегій комунікативної поведінки, спрямованих на їх ефективне виявлення, попередження та мінімізацію з урахуванням особливостей цифрового медіа-середовища та динаміки онлайн-взаємодії.

**Матеріали і методи.** Матеріалами дослідження є: нормативно-правові акти та рекомендації щодо регулювання цифрової комунікації та захисту персональних даних у медіапросторі; праці вітчизняних та зарубіжних авторів, які здійснюють науково-практичні дослідження в галузі управління репутацією, інформаційних ризиків, комунікаційної поведінки публічних осіб у цифровому середовищі; приклади кризових комунікацій, кейси управління репутаційними інцидентами та матеріали соціальних мереж і медіа, що ілюструють динаміку поширення інформаційних загроз.

В процесі дослідження застосовано такі наукові методи: теоретичного узагальнення та систематизації (для характеристики природи репутаційних та інформаційних ризиків, визначення їхніх джерел і чинників ескалації); аналізу та синтезу (для побудови комплексної моделі стратегій комунікативної поведінки публічних осіб та формування механізмів управління ризиками); формалізації та класифікації (для структурованого представлення джерел інформаційних загроз, фаз динаміки репутаційних криз і інструментів моніторингу); логічного узагальнення (для формулювання висновків щодо інтеграції технологічних, комунікаційних та стратегічних підходів у системі управління репутаційними та інформаційними ризиками публічних осіб).

**Результати.** У статті проведено комплексний аналіз природи та динаміки репутаційних і інформаційних ризиків, притаманних публічним особам у цифровому медіапросторі. Визначено основні чинники їх виникнення й ескалації: зростання інтенсивності інформаційних потоків, алгоритмічне персоналізоване середовище споживання новин, активність онлайн-спільнот та технологічні можливості створення і поширення фейкових або модифікованих матеріалів. На основі міждисциплінарних джерел і сучасних кейсів систематизовано типологію ризиків — від репутаційних і психологічних до стратегічних та операційних. У роботі запропоновано комплекс актуальних стратегій комунікативної поведінки, які здатні мінімізувати негативні наслідки для публічного іміджу. Серед них: проактивне управління цифровою присутністю, системний моніторинг інформаційного поля, застосування інструментів соціального слухання, впровадження

аналітики для раннього виявлення кризових індикаторів, а також адаптивні моделі комунікації, що враховують поведінкову специфіку цифрових аудиторій. Окремо підкреслено значення етичної і прозорої кризової комунікації як основи відновлення довіри та формування довготривалої репутаційної стійкості. Стаття доводить, що ефективне управління репутаційними та інформаційними ризиками є ключовою компетенцією публічних осіб у сучасному цифровому середовищі та вимагає інтеграції технологічних, комунікаційних і стратегічних підходів для забезпечення стабільності та авторитетності їхнього публічного образу.

Перспективи. У подальших наукових дослідженнях пропонується зосередити увагу на розробці комплексних моделей оцінки ефективності стратегій комунікативної поведінки публічних осіб у цифровому медіапросторі, а також на впровадженні інтегрованих систем моніторингу та аналітики для раннього виявлення інформаційно-репутаційних ризиків. Реалізація цих напрямів дозволить удосконалити методику управління репутаційними ризиками, підвищити ефективність превентивних та кризових комунікаційних заходів, а також сприятиме формуванню стійкого та авторитетного публічного образу в умовах динамічного цифрового середовища.

**Ключові слова:** репутація, інформація, ризики, публічні особи, комунікативна поведінка, цифровізація, інформаційна безпека, алгоритмічні платформи.

**Summary.** Introduction. In the digital age, public figures find themselves in a situation of significantly increased vulnerability to reputational and information risks arising in an environment of ultra-fast communications, social networks, and algorithmically controlled information flows. The phenomena of content virality, disinformation, manipulative campaigns, and generative media technologies create new types of threats that traditional communication tools are no longer able to effectively neutralize. In such conditions, instant audience reactions, emotional polarization, and the destruction of institutional channels of trust significantly increase potential reputational damage, and even minor information incidents can transform into large-scale crises that affect the social status, political positions, and professional activities of public figures.

Purpose. The purpose of this article is to conduct a comprehensive analysis of the reputational and informational risks faced by public figures in the digital age, as well as to develop and justify modern communication strategies aimed at effectively identifying, preventing, and minimizing these risks, taking into account the characteristics of the digital media environment and the dynamics of online interactions.

Materials and methods. The research materials include: regulatory acts and recommendations on regulating digital communication and protecting personal data in the media space; works by domestic and foreign authors conducting scientific and practical research in the field of reputation management, information risks, and communication behavior of public figures in the digital environment; examples of crisis communications, cases of reputation incident management, and materials from social networks and the media illustrating the dynamics of the spread of information threats.

The following scientific methods were used in the research: theoretical generalization and systematization (to characterize the nature of reputation and information risks, identify their sources and escalation factors); analysis and synthesis (to build a comprehensive model of communication behavior strategies of public figures and develop risk management mechanisms); formalization and classification (to provide a structured representation of the sources of information threats, the phases of reputation crisis dynamics, and monitoring tools); logical generalization (to formulate conclusions on the integration of technological, communication, and strategic approaches in the system of reputation and information risk management for public figures).

Results. The article provides a comprehensive analysis of the nature and dynamics of reputational and informational risks inherent to public figures in the digital media space. The main factors contributing to their emergence and escalation are identified: the growth in the intensity of information flows, the algorithmic personalized news consumption environment, the activity of online communities, and the technological capabilities for creating and disseminating fake or modified materials. Based on interdisciplinary sources and contemporary cases, a typology of risks has been systematized – from reputational and psychological to strategic and operational. The paper proposes a set of relevant strategies for communicative behavior that can minimize negative consequences for public image. These include proactive management of digital presence, systematic monitoring of the information field, the use of social listening tools, the introduction of analytics for early detection of crisis indicators, as well as adaptive communication models that take into account the behavioral specifics of digital audiences. The importance of ethical and transparent crisis communication as the basis for restoring trust and building long-term reputational stability is emphasized separately. The article argues that effective management of reputation and information risks is a key competence of public figures in today's digital environment and requires the integration of technological, communication, and strategic approaches to ensure the stability and credibility of their public image.

Discussion. Further research should focus on developing comprehensive models for assessing the effectiveness of public figures' communication strategies in the digital media space, as well as on implementing integrated monitoring and analytics systems for early detection of information and reputation risks. The implementation of these areas will improve the methodology for managing reputation risks, increase the effectiveness of preventive and crisis communication measures, and contribute to the formation of a stable and authoritative public image in a dynamic digital environment.

**Key words:** reputation, information, risks, public figures, communicative behavior, digitalization, information security, algorithmic platforms.

**Постановка проблеми.** Стрімка цифровізація комунікаційного середовища та зростання впливу соціальних медіа принципово змінюють умови формування та підтримання репутації публічних осіб. У ситуації, коли інформаційні потоки характеризуються високою швидкістю, фрагментарністю та віральністю, публічні діячі стають особливо вразливими до різноманітних репутаційних і інформаційних загроз. Дезінформаційні кампанії, маніпулятивні повідомлення, алгоритмічне підсилення конфліктного контенту та неконтрольоване поширення фейкових або викривлених матеріалів створюють ризики, що можуть завдати істотної шкоди публічному іміджу та довірі аудиторії.

Проблема ускладнюється тим, що традиційні підходи до формування комунікаційної політики та управління кризами не враховують специфіки цифрової екосистеми, у якій інформаційні інциденти здатні швидко ескалувати та виходити за межі локальних контекстів. Водночас у сучасних умовах бракує цілісних моделей і стратегій, які б дозволяли своєчасно виявляти, оцінювати й мінімізувати репутаційні та інформаційні ризики з урахуванням поведінкових особливостей онлайн-спільнот та функціонування алгоритмічних платформ.

Отже, актуальність дослідження зумовлена потребою розробити сучасні, ефективні та адаптивні стратегії комунікативної поведінки публічних осіб, здатні забезпечувати стійкість до загроз цифрового середовища, підтримувати довіру аудиторії та формувати стабільний репутаційний капітал у ситуації інформаційної турбулентності.

**Аналіз останніх досліджень і публікацій.** Значний внесок у формування теоретичних підходів та концептуальних засад управління репутаційними й інформаційними ризиками публічних осіб у цифровому середовищі зроблено як вітчизняними, так і зарубіжними науковцями.

Так, наприклад, Баланчук Д. [1] аналізує трансформацію репутаційних стратегій під впливом алгоритмічної логіки цифрових платформ та підкреслюють роль технологічної аналітики у попередженні кризових ситуацій. Дерев'янка О. [2] досліджує механізми соціального слухання (social listening) як ключового інструменту раннього виявлення інформаційних загроз для політичних лідерів та медіаперсон.

Зокрема, Тарасенко Т. [3] розглядає взаємозв'язок між динамікою цифрового дискурсу та формуванням репутаційної вразливості публічних осіб, акцентуючи увагу на нерівномірності та емоційності інформаційних потоків у соціальних мережах. У свою чергу, Чупріна М. [4] досліджує адаптивні моделі комунікації та визначає їхню ефективність у залежності від поведінкової специфіки цифрових аудиторій. Важливий внесок у вивчення стратегій кризових комунікацій зроблено також Помянська Н. [5], яка пропонує багаторівневу систему реагування на репутаційні інциденти на основі поєднання

предиктивної аналітики та швидкого публічного інформування.

Узагальнення існуючих наукових напрацювань свідчить про те, що сучасні дослідження зосереджуються на технологічних, поведінкових та комунікаційних аспектах формування репутаційної стійкості публічних осіб у цифрову епоху. Це створює підґрунтя для подальшого вдосконалення методичних підходів і розвитку комплексних стратегій управління інформаційно-репутаційними ризиками.

**Метою статті** є здійснення комплексного аналізу репутаційних та інформаційних ризиків, з якими стикаються публічні особи в умовах цифрової епохи, а також розроблення й обґрунтування сучасних стратегій комунікативної поведінки, спрямованих на їх ефективне виявлення, попередження та мінімізацію з урахуванням особливостей цифрового медіа-середовища та динаміки онлайн-взаємодій.

**Матеріали і методи.** Матеріалами дослідження є: нормативно-правові акти та рекомендації щодо регулювання цифрової комунікації та захисту персональних даних у медіапросторі; праці вітчизняних та зарубіжних авторів, які здійснюють науково-практичні дослідження в галузі управління репутацією, інформаційних ризиків, комунікаційної поведінки публічних осіб у цифровому середовищі; приклади кризових комунікацій, кейси управління репутаційними інцидентами та матеріали соціальних мереж і медіа, що ілюструють динаміку поширення інформаційних загроз.

В процесі дослідження застосовано такі наукові методи: теоретичного узагальнення та систематизації (для характеристики природи репутаційних та інформаційних ризиків, визначення їхніх джерел і чинників ескалації); аналізу та синтезу (для побудови комплексної моделі стратегій комунікативної поведінки публічних осіб та формування механізмів управління ризиками); формалізації та класифікації (для структурованого представлення джерел інформаційних загроз, фаз динаміки репутаційних криз і інструментів моніторингу); логічного узагальнення (для формулювання висновків щодо інтеграції технологічних, комунікаційних та стратегічних підходів у системі управління репутаційними та інформаційними ризиками публічних осіб).

**Виклад основного матеріалу.** У сучасному цифровому середовищі репутація публічних осіб формується та трансформується значно швидше, ніж будь-коли раніше, оскільки інформаційні потоки стають дедалі інтенсивнішими, динамічнішими та менш контрольованими. Висока швидкість поширення контенту, вплив соціальних мереж і присутність дезінформаційних загроз створюють новий рівень вразливості, що потребує переосмислення підходів до комунікаційної поведінки та управління репутаційними ризиками.

Репутаційні ризики можна трактувати як потенційні втрати довіри, легітимності або соціального

капіталу, спричинені поширенням негативної, маніпулятивної або некоректно інтерпретованої інформації про публічну особу. Інформаційні ризики, у свою чергу, охоплюють загрози, пов'язані з циркуляцією недостовірних даних, витоками конфіденційної інформації, модифікованим контентом (зокрема *deepfake*) і неправомірним використанням персональних цифрових даних [6].

У цифровому середовищі ці два типи ризиків тісно взаємопов'язані: інформаційні інциденти нерідко стають каталізатором репутаційних криз, а сама вразливість репутації збільшує силу інформаційних атак. До ключових джерел інформаційно-репутаційних загроз належать [7]:

1. Дезінформація та маніпулятивні наративи — навмисне створення та поширення неправдивих тверджень.

2. Деформація контексту — подання фактів без необхідних обставин або в інтерпретаціях, що змінюють їх зміст.

3. Витоки конфіденційних матеріалів — фінансові дані, приватні повідомлення, службові документи.

4. Соціотехнічні атаки — злам акаунтів, підміна особистостей, фальсифікація цифрових слідів.

5. Стихійні або скоординовані кампанії тиску — тролінг, масові напади бот-мереж, «рейдінг».

6. Алгоритмічні ефекти платформ — вірусне поширення емоційно зарядженого контенту, яке збільшує потенційну шкоду.

Поширення інформаційно-репутаційних ризиків у цифровому медіапросторі характеризується високою швидкістю та мережевою нелінійністю. Типову динаміку можна описати у вигляді кількох фаз [8]:

1. Пусковий момент (*trigger*) — виникнення контенту або події, яка привертає увагу аудиторії.

2. Локальна циркуляція — обговорення серед обмеженої групи користувачів чи медіа.

3. Експансія та реплікація — поширення через алгоритмічні рекомендації, інфлюенсерів, меми.

4. Медіатизація — включення традиційних ЗМІ, що збільшує охоплення та поглиблює кризу.

5. Пік ескалації — максимальний обсяг негативу, ухвалення рішень аудиторією у «режимі реального часу».

6. Стабілізація або тривала пляма — формування стійких негативних асоціацій або поступове відновлення репутації.

Особливої уваги потребує роль алгоритмів соціальних мереж, які підсилюють поширення контенту з високою емоційністю, що створює структурну схильність до віральності репутаційних загроз.

Репутаційні втрати можуть мати комплексний характер і включати: професійні наслідки (втрата партнерств, послаблення експертного статусу); фінансові ризики (зниження вартості контрактів, витрати на юридичну та PR-підтримку); соціально-психологічні наслідки (публічний тиск, загрози, соціальна стигматизація); правові наслідки (судові

процеси, розслідування, порушення прав на приватність). У довгостроковій перспективі репутаційна шкода здатна сформувати стійкі негативні наративи, що впливають на публічну легітимність та соціальний капітал особи.

Крім того, в цифровому середовищі публічні особи стають об'єктами підвищеної уваги та вразливими до швидких інформаційних флуктуацій. Узагальнення основних характеристик цих ризиків подано в таблиці, що систематизує природу загроз, їх динаміку, наслідки та ключові механізми управління (табл. 1)

Репутаційні та інформаційні ризики публічних осіб у цифровому медіапросторі становлять комплексний феномен, що виникає на перетині соціальної психології, медіалогії, кібербезпеки та комунікаційних технологій. Їхня природа визначається високою швидкістю циркуляції інформації, низьким бар'єром доступу до публікації, а також алгоритмічними характеристиками сучасних платформ. Динаміка репутаційних інцидентів у цифровому середовищі характеризується експоненційністю та високим потенціалом до віральності, що потребує систематичного моніторингу, чітких комунікаційних протоколів та інтеграції юридичних, технічних і стратегічних засобів реагування.

Ефективне управління такими ризиками можливе лише на основі інтегрованого підходу, який охоплює превентивні дії, оперативну кризову комунікацію та довгострокове відновлення довіри аудиторій. Такі стратегії сприяють зменшенню негативних наслідків інформаційних інцидентів та забезпечують стійкість репутації публічних осіб у динамічному цифровому середовищі. Разом з тим, ефективне управління публічним іміджем у цифровому середовищі потребує впровадження цілісних стратегій комунікації, що поєднують технологічні інструменти, поведінкову аналітику та адаптивні моделі взаємодії з аудиторіями. Висока швидкість циркуляції інформації, вразливість до дезінформаційних впливів та алгоритмічна природа цифрових платформ висувають до публічних осіб вимогу системно контролювати свою цифрову присутність та оперативно реагувати на комунікативні виклики [10].

Однією з ключових стратегій є проактивне управління цифровою присутністю, яке передбачає наперед сформовану і послідовно підтримувану публічну комунікацію, що створює позитивний інформаційний фон. Така стратегія включає планомірне оприлюднення релевантного контенту, розвиток персонального бренду та формування чіткої комунікативної позиції. Проактивність зменшує вразливість до кризових ситуацій, оскільки забезпечує накопичення соціального капіталу та підвищує довіру аудиторії. Важливим елементом сучасного управління репутаційними ризиками виступає системний моніторинг інформаційного поля, який дає змогу відстежувати зміни в медіадискурсі, оцінювати ін-

Таблиця 1

**Репутаційні та інформаційні ризики публічних осіб у цифровому медіапросторі**

| №  | Аналітичний компонент                | Основні положення                                                                                                                                                                                                                                      |
|----|--------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1  | Природа ризиків                      | Репутаційні ризики — загроза втрати довіри та легітимності; інформаційні ризики — поширення недостовірних даних, витоки та маніпуляції. Тісно взаємопов'язані: інформаційні інциденти запускають репутаційні кризи.                                    |
| 2  | Джерела ризиків                      | 1) Дезінформація й маніпулятивні наративи; 2) Викривлення контексту; 3) Витоки приватних даних; 4) Кібератаки й підміна особистостей; 5) Тролінг і скоординовані кампанії; 6) Алгоритмічне посилення негативу в соцмережах.                            |
| 3  | Динаміка поширення                   | Фази: (1) триггер → (2) локальне поширення → (3) експансія через алгоритми й інфлюенсерів → (4) медіатизація → (5) пік кризи → (6) стабілізація або формування довготривалої негативної «плями». Характеристика: швидкість, віральність, нелінійність. |
| 4  | Чинники ескалації                    | Емоційна зарядженість контенту; участь лідерів думок; аудиторна поляризація; алгоритмічна вірусність; відсутність швидкої реакції; наявність візуальних матеріалів (відео, скріншоти).                                                                 |
| 5  | Наслідки для публічної особи         | Професійні (втрата партнерств), фінансові (збитки, витрати на PR/юристів), соціально-психологічні (стигматизація, тиск), правові (позови, розслідування), стратегічні (довгострокова репутаційна шкода).                                               |
| 6  | Методи моніторингу та оцінки         | Показники: обсяг згадувань, тональність, охоплення, швидкість реплікації, структура хвиль, виявлення бот-мереж. Інструменти: системи SMM-аналітики, sentiment analysis, alarms, фактчек-платформи.                                                     |
| 7  | Превентивні механізми                | Цифрова гігієна; контроль доступу до акаунтів; розвиток публічної комунікації; кризові протоколи; медіатренінги; регулярний моніторинг інформаційного поля.                                                                                            |
| 8  | Оперативна реакція під час інциденту | Швидка й фактологічна заява; багатоканальна комунікація; співпраця з фактчекерами; юридичні дії; дезавування фейків; локалізація негативу шляхом корекції наративів.                                                                                   |
| 9  | Відновлення після кризи              | Аналіз причин; довгострокова інформаційна стратегія; відновлення довіри через послідовну діяльність; контроль показників репутаційної динаміки; формування позитивного наративу.                                                                       |
| 10 | Стратегічні принципи управління      | Інтегрованість (PR + юридія + кібербезпека); превентивна готовність; прозора комунікація; адаптивність до алгоритмів соцмереж; етичність застосовуваних практик.                                                                                       |

Джерело: сформовано автором на основі даних [9]

тенсивність згадувань та виявляти потенційні загрози на ранніх етапах. Моніторинг забезпечує своєчасне реагування, локалізацію негативу та формування обґрунтованих комунікативних рішень на основі фактичних даних.

Ефективність моніторингу суттєво зростає завдяки застосуванню інструментів соціального слухання (social listening). Ці технології дозволяють не лише фіксувати згадки про публічну особу, а й аналізувати емоційний фон, поведінкові патерни, темпоральну динаміку обговорень та взаємодії між різними сегментами аудиторії. Соціальне слухання формує глибше розуміння контекстів, що визначають потенціал ескалації ризиків. Додатковим захисним механізмом виступає впровадження аналітичних рішень для раннього виявлення кризових індикаторів. До таких інструментів належать алгоритми тонального аналізу, кластерний контент-аналіз, виявлення нетипових аномалій у поведінці інформаційних потоків та ідентифікація скоординованих маніпулятивних кампаній. Використання аналітики забезпечує перехід від реактивної до предиктивної моделі управління ризиками. Не менш важливим напрямом є розроблення адаптивних моделей комунікації, орієнтованих на специфіку цифрових аудиторій.

З огляду на їхню фрагментованість, емоційність та різноманітність поведінкових установок, комунікативні стратегії мають бути персоналізованими, контекстно чутливими та гнучко налаштованими під характеристики окремих платформ. Адаптивність охоплює корекцію тону, вибір відповідних форматів (відео, лонгрід, короткі меседжі), багатоканальність взаємодії та оптимізацію повідомлень під алгоритмічні параметри соціальних мереж [11].

Таким чином, комплекс стратегій комунікативної поведінки, що включає проактивне управління цифровою присутністю, системний моніторинг, соціальне слухання, аналітику для раннього виявлення кризових сигналів та адаптивні моделі комунікації, формує ефективну інфраструктуру для мінімізації репутаційних ризиків. Впровадження цих підходів сприяє підвищенню стійкості публічних осіб до інформаційних загроз та забезпечує стратегічну стабільність їхнього публічного іміджу у динамічному цифровому середовищі. Разом з тим, технологічний компонент полягає у застосуванні інструментів аналітики даних, соціального слухання, автоматизованого моніторингу та алгоритмічних систем виявлення кризових індикаторів. Ці рішення забезпечують можливість швидко фіксувати найменші зміни

в інформаційному полі, ідентифікувати аномальні патерни поширення контенту та прогнозувати ризики ще до того, як вони набудуть масштабного характеру. Завдяки цьому технологічні механізми стають фундаментом предиктивного управління репутацією [12].

Комунікаційний вимір охоплює здатність публічних осіб формувати прозору, послідовну та автентичну взаємодію з аудиторіями. Він передбачає проактивне створення змістовного контенту, адаптацію повідомлень до специфіки цифрових платформ і своєчасне реагування на суспільні настрої. Ефективна комунікація сприяє мінімізації впливу дезінформації, зменшенню емоційної напруги в кризових ситуаціях та збереженню довіри, яка є критично важливим ресурсом у публічній діяльності. Стратегічний компонент передбачає комплексне мислення та побудову довгострокових моделей управління репутацією. Він включає формування стійкої цифрової ідентичності, розроблення кризових протоколів, визначення ключових репутаційних показників і систематичну оцінку комунікативних практик. Саме стратегічний підхід забезпечує узгодженість дій, передбачуваність поведінкових рішень і здатність утримувати контроль над наративами навіть у нестабільних інформаційних середовищах.

У сукупності технологічні, комунікаційні та стратегічні рішення формують цілісну систему управління репутаційними та інформаційними ризиками, що дозволяє публічним особам підтримувати авторитетність і стабільність свого образу. Така інтеграція не лише знижує вразливість до зовнішніх загроз, а й забезпечує ефективне позиціонування в умовах конкуренції та високої інтенсивності інформаційних потоків, що є визначальним фактором успіху у цифрову епоху [13].

Ефективне управління репутаційними та інформаційними ризиками в цифровому середовищі є необхідною умовою збереження стабільності, довіри та легітимності публічних осіб. Інтеграція технологічних, комунікаційних і стратегічних підходів формує комплексну систему захисту, яка забезпечує стійкість публічного образу та підвищує здатність успішно функціонувати в умовах динамічного медіапростору.

**Висновки.** Враховуючи зазначене, варто відмітити, що в сучасному цифровому медіапросторі публічні особи постають перед унікальними викликами,

пов'язаними з високою швидкістю циркуляції інформації, широким охопленням аудиторії та алгоритмічною вірусністю контенту. Репутаційні та інформаційні ризики у цьому середовищі мають комплексну природу і виникають як через об'єктивні події або помилки, так і через навмисні дезінформаційні кампанії, витоки конфіденційних даних або спотворення контексту. Висока динаміка поширення негативу, експоненціальна вірусність та взаємопов'язаність інформаційних і репутаційних загроз формують ситуації, коли невчасне реагування може призвести до тривалої шкоди репутації та соціального капіталу.

Комплексне управління цими ризиками є ключовою компетенцією публічних осіб і передбачає інтеграцію технологічних, комунікаційних та стратегічних підходів. Технологічна складова включає системний моніторинг, соціальне слухання та аналітичні інструменти для раннього виявлення кризових індикаторів, що забезпечує можливість прогнозування загроз і швидкої реакції. Комунікаційна складова полягає у проактивному управлінні цифровою присутністю, адаптації повідомлень до поведінкових і психологічних характеристик аудиторій, багатоканальній взаємодії та прозорій комунікації під час кризових ситуацій. Стратегічна складова забезпечує формування стійкої цифрової ідентичності, розроблення кризових протоколів, визначення ключових репутаційних показників та систематичну оцінку комунікативних практик.

Реалізація цих підходів дозволяє публічним особам зменшити вразливість до негативних інформаційних впливів, своєчасно локалізувати і нейтралізувати потенційні загрози, а також створити передумови для довгострокового підтримання авторитетності й довіри. Проактивне формування позитивного інформаційного поля, системний моніторинг і адаптивні комунікаційні моделі формують цілісну систему управління репутаційними ризиками, що підвищує стійкість публічних осіб у динамічному цифровому середовищі та забезпечує ефективне позиціонування в умовах конкуренції за увагу аудиторії.

Таким чином, інтеграція технологічних, комунікаційних і стратегічних підходів до управління репутаційними та інформаційними ризиками є не лише практичною потребою, а й невід'ємною компетенцією, визначальною для успішної діяльності публічних осіб у цифрову епоху.

### Література

1. Шульга Н. П., Баланчук Д. В. Феномен ризику репутації банку. *Економіка та держава*. 2019. № 6. С. 21–26
2. Дерев'яно О. Г. Механізми впливу репутаційного менеджменту на бізнес-результати. *Стратегія економічного розвитку України*. 2018. № 42. С. 5–18.
3. Тарасенко Т. М. Запровадження інноваційних технологій управління репутацією органів місцевого самоврядування: теорія та практика. *Публічне управління і адміністрування в Україні*. 2022. Випуск 28. С. 158–164.
4. Жалдак Г. П., Чуприна М. О. Управління репутаційними ризиками підприємства з урахуванням концепції корпоративної соціальної відповідальності. *Ринкова економіка: сучасна теорія і практика управління*. 2021. Том 20 № 1(47). С. 175–184
5. Помянська Н. Ю. Управління діловою репутацією на синергетичних засадах. *Науковий вісник Херсонського державного університету*. 2014. Випуск 9. Частина 4. С. 57–61.
6. Методичний посібник щодо аспектів управління ризиками, як складової системи внутрішнього контролю у розпорядника бюджетних коштів. Київ. Міністерство фінансів України. 2022. 22 с.
7. Ржевська Н. Вплив інформаційного суспільства на формування категоріального апарату політичної науки: інформаційна демократія як політична категорія. *Вісник Львів. ун-ту. Філософсько-політологічні студії*. 2010. № 1. С. 81–245.
8. Фесенко В. Особливості та тенденції розвитку політичної культури в українському суспільстві. *Українська правда*. 2018. URL: <https://blogs.pravda.com.ua/authors/fesenko/5ab61e2b1e0ad/> (дата звернення: 01.12.2025).
9. Плєскач М. В. Сутність поняття та основні елементи механізму адміністративно-правового забезпечення кібернетичної безпеки людини. *Часопис Київського університету права*. 2020. № 4. С. 201–209. <https://doi.org/10.36695/2219-5521.4.2020.36>. URL: <https://chasprava.com.ua/index.php/journal/article/view/568> (дата звернення: 01.12.2025).
10. Фурман А. Управління репутацією у воєнний час. *Ліга: Закон Бізнес*. 2022. URL: [https://biz.ligazakon.net/analytics/215083\\_upravlnnya-reputatsyu-u-vonniy-chas](https://biz.ligazakon.net/analytics/215083_upravlnnya-reputatsyu-u-vonniy-chas) (дата звернення: 01.12.2025).
11. Sadeghi B., Richards D., Formosa P., McEwan M., Bajwa M. H. A., Hitchens M., Ryan M. Modelling the ethical priorities influencing decision-making in cybersecurity contexts. *Organizational Cybersecurity Journal: Practice, Process and People*. 2023. Vol. 3 No. 2, pp. 127–149. DOI: <https://doi.org/10.1108/OCJ-09-2022-0015>
12. Тарасюк А. В. Теоретико-правове підґрунтя інформаційної етики в системі забезпечення кібербезпеки. *Правова позиція*. 2020. № 4 (29). С. 48–52. URL: <http://biblio.umsf.dp.ua/jspui/bitstream/123456789/4264/1/12%20%20d0%a2%d0%b0%d1%80%d0%b0%d1%81%d1%8e%d0%ba%20%20d0%90.%20%20d0%92..pdf> (дата звернення: 17.11.2025).
13. Шлемкевич Т. Інформаційно-комунікаційні чинники впливу на громадянське суспільство в сучасній Україні. *Політикус*. 2019. № 5. С. 38–43.

### References

1. Shulha, N. P., & Balanchuk, D. V. (2019). Fenomen ryzyku reputatsii banku [The phenomenon of bank reputation risk]. *Ekonomika ta derzhava*, № (6), Pp. 21–26 [in Ukrainian].
2. Derevianko, O. H. (2018). Mekhanizmy vplyvu reputatsiinoho menedzhmentu na biznes-rezultaty [Mechanisms of influence of reputation management on business results]. *Stratehiia ekonomichnoho rozvytku Ukrainy*, № (42), Pp. 5–18 [in Ukrainian].
3. Tarasenko, T. M. (2022). Zaprovadzhennia innovatsiinykh tekhnolohii upravlinnia reputatsiieiu orhaniv mistsevoho samovriadiuvannia: teoriia ta praktyka [Implementation of innovative technologies for managing the reputation of local self-government bodies: theory and practice]. *Publichne upravlinnia i administruvannia v Ukraini*, № 28, Pp. 158–164 [in Ukrainian].
4. Zhaldak, H. P., & Chuprina, M. O. (2021). Upravlinnia reputatsiinykh ryzykamy pidpriemstva z urakhuvanniam kontseptsii korporativnoi sotsialnoi vidpovidalnosti [Management of enterprise reputation risks considering the concept of corporate social responsibility]. *Rynkova ekonomika: suchasna teoriia i praktyka upravlinnia*, № 20(1/47), Pp. 175–184 [in Ukrainian].
5. Pomianska, N. Yu. (2014). Upravlinnia dilovoiu reputatsiieiu na synerhetychnykh zasadakh [Management of business reputation on synergistic principles]. *Naukovyi visnyk Khersonskoho derzhavnoho universytetu*, № 9/4, Pp. 57–61 [in Ukrainian].
6. Ministerstvo finansiv Ukrainy. (2022). Metodychnyi posibnyk shchodo aspektiv upravlinnia ryzykamy yak skladovoi systemy vnutrishnoho kontroliu u rozporiadnyka biudzhetykh koshtiv [Methodical guide on aspects of risk management as a component of the internal control system]. Kyiv, 22 s. [in Ukrainian].
7. Rzhavska, N. (2010). Vplyv informatsiinoho suspilstva na formuvannia katehorialnoho aparatu politychnoi nauky: informatsiina demokratiia yak politychna katehoriia [Influence of the information society on the formation of the categorical apparatus of political science: information democracy as a political category]. *Visnyk Lvivskoho universytetu. Filozofsko-politohichni studii*, № 1, Pp. 81–245 [in Ukrainian].
8. Fesenko, V. (2018). Osoblyvosti ta tendentsii rozvytku politychnoi kultury v ukrainskomu suspilstvi [Features and trends of political culture development in Ukrainian society]. *Ukrainska pravda*. URL: <https://blogs.pravda.com.ua/authors/fesenko/5ab61e2b1e0ad/> [in Ukrainian].

9. Pleskach, M. V. (2020). Sutnist poniattia ta osnovni elementy mekhanizmu administratyvno-pravovoho zabezpechennia kibernetychnoi bezpeky liudyny [Essence of the concept and main elements of the administrative and legal mechanism for ensuring human cyber security]. *Chasopys Kyivskoho universytetu prava*, № 4, Pp. 201–209. <https://doi.org/10.36695/2219-5521.4.2020.36>. URL: <https://chasprava.com.ua/index.php/journal/article/view/568> [in Ukrainian].
10. Furman, A. (2022). Upravlinnia reputatsiiei u voiennyi chas [Reputation management during wartime]. *Liha: Zakon Biznes*. URL: [https://biz.ligazakon.net/analytics/215083\\_upravlnnya-reputatsyu-u-vonniy-chas](https://biz.ligazakon.net/analytics/215083_upravlnnya-reputatsyu-u-vonniy-chas) [in Ukrainian].
11. Sadeghi, B., Richards, D., Formosa, P., McEwan, M., Bajwa, M. H. A., Hitchens, M., & Ryan, M. (2023). Modelling the ethical priorities influencing decision-making in cybersecurity contexts. *Organizational Cybersecurity Journal: Practice, Process and People*, № 3(2), Pp. 127–149. <https://doi.org/10.1108/OCJ-09-2022-0015>
12. Tarasiuk, A. V. (2020). Teoretyko-pravove pidgruntia informatsiinoi etyky v systemi zabezpechennia kiberbezpeky [Theoretical and legal basis of information ethics in the system of cybersecurity]. *Pravova pozytsiia*, № 4(29), Pp. 48–52. URL: <http://biblio.umsf.dp.ua/jspui/bitstream/123456789/4264/1/12%20Тапасюк%20А.%20В..pdf> [in Ukrainian].
13. Shlemkevych, T. (2019). Informatsiino-komunikatsiini chynnyky vplyvu na hromadianske suspilstvo v suchasni Ukraini [Information and communication factors influencing civil society in modern Ukraine]. *Politykus*, (5), 38–43 [in Ukrainian].

Стаття надійшла до редакції 09.12.2025