ISSN 2786-5002 (online)
ISSN 2786-4995 (print)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
імені В. Н. КАРАЗІНА

ФІНАНСОВО-КРЕДИТНІ СИСТЕМИ: ПЕРСПЕКТИВИ РОЗВИТКУ

ЗБІРНИК НАУКОВИХ ПРАЦЬ

Випуск 3(22)2026

Заснований 2021р.

Харків – 2026

УДК 336.7:338.24

Збірник наукових праць «Фінансово-кредитні системи: перспективи розвитку» публікує наукові статті, які містять оригінальні результати розв'язання питанн економіки, обліку, фінансів та банківської справи, управління та інформаційних технологій зазначених напрямків. Журнал виходить 4 рази на рік (березень, червень, вересень, грудень).

ISSN 2786-5002 (online) **ISSN 2786-4995 (print)**

Головний редактор:
Самородов Борис, Харківський національний університет імені В. Н. Каразіна, Україна
Заступник головного редактора:
Азаренкова Галина, Харківський національний університет імені В. Н. Каразіна, Україна
Відповідальний редактор:
Мірошник Олексій, Харківський національний університет імені В. Н. Каразіна, Україна
Технічний редактор:
Покровська Марія, Харківський національний університет імені В. Н. Каразіна, Україна

РЕДАКЦІЙНА КОЛЕГІЯ:

Абдул Азіз Абдул Рахман, Королівський університет, Бахрейн
Адамонене Рута, Університет Миколаса Ромеріса, Литва
Акімова Людмила, Національний університет водного господарства та природокористування, Україна
Бабічев Анатолій, Харківський національний університет імені В. Н. Каразіна, Україна
Балезентіс Томас, Литовський центр соціальних наук, Литва
Баранова Валерія, Харківський національний університет імені В. Н. Каразіна, Україна
Гороховатський Володимир, Харківський національний університет радіоелектроніки, Україна
Данкевич Андрій, Національний університет харчових технологій, Україна
Доерті Боб, професор, Школа бізнесу та суспільства Університету Йорк, Велика Британія
Житар Максим, Національний університет «Київський авіаційний інститут», Україна
Ільїч Людмила, Київський університет імені Бориса Грінченка, Україна
Карас Міхал, Технологічний університет у Брно, Чехія
Мельниченко Олександр, Гданський політехнічний університет, Польща
Нурул Мохаммад, Міжнародний університет Даффоділ, Бангладеш
Семеног Андрій, Сумський державний університет, Україна
Сергієнко Олена, Національний технічний університет «Харківський політехнічний інститут», Україна
Сіманавічіене Жанета, Університет Миколаса Ромеріса, Литва
Ткаченко Наталія, Київський національний університет імені Тараса Шевченка, Україна
Хусам-Алдін Нізар Аль-Малкаві, Британський університет в Дубаї, Об'єднані Арабські Емірати

Збірник наукових праць «Фінансово-кредитні системи: перспективи розвитку» внесений до категорії Б переліку фахових видань України (Наказ Міністерства освіти і науки України № 582 від 24.04.2024, Наказ Міністерства освіти і науки України № 928 від 11.06.2026): С1 Економіка (0311 Economics); С3 Міжнародні відносини (0312 Political sciences and civics, 0314 Sociology and cultural studies); D1 Облік і оподаткування (0411 Accounting and taxation); D2 Фінанси, банківська справа, страхування та фондовий ринок (0412 Finance, banking and insurance); D3 Менеджмент (0413 Management and administration; 0415 Secretarial and office work); D4 Публічне управління та адміністрування (0413 Management and administration); D5 Маркетинг (0414 Marketing and advertising); D7 Торгівля (0414 Marketing and advertising, 0416 Wholesale and retail sales).

Затверджено до друку рішенням Вченої ради Харківського національного університету імені В. Н. Каразіна (протокол № 17 від 05 жовтня 2026 року)

Усі права захищені. Передрук і переклади дозволяються лише зі згоди автора та редакції.
Редакція не завжди поділяє думку автора й не відповідає за фактичні помилки, яких він припустився.

Засновник:
Харківський національний університет імені В. Н. Каразіна,
майдан Свободи 4, м. Харків, 61022, Україна. **www.karazin.ua**

Сайт збірника: **https://periodicals.karazin.ua/fcs** Електронна адреса: **fcs.journal@karazin.ua**
Ідентифікатор медіа у Реєстрі суб'єктів у сфері медіа: R30-04477 (Рішення № 1538 від 09.05.2024 року Національної ради України з питань телебачення і радіомовлення. Протокол № 15)

© Харківський національний університет імені В. Н. Каразіна, 2026

ISSN 2786-5002 (online)
ISSN 2786-4995 (print)

MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE

V. N. KARAZIN KHARKIV NATIONAL UNIVERSITY

FINANCIAL AND CREDIT SYSTEMS: PROSPECTS FOR DEVELOPMENT

COLLECTION OF SCIENTIFIC WORKS

Issue 3(22)2026

Founded in 2021

Kharkiv – 2026

UDC 336.7:338.24

Collection of scientific works "Financial and credit systems: prospects for development" publishes scientific articles that contain original results of solving problems of economics, accounting, finance and banking, management and information technology in these areas. The magazine is published 4 times a year (March, June, September, December).

ISSN 2786-5002 (online) **ISSN 2786-4995 (print)**

Chief Editor:
Samorodov Borys, V. N. Karazin Kharkiv National University, Ukraine
Deputy chief Editor:
Azarenkova Galyna, V. N. Karazin Kharkiv National University, Ukraine
Managing Editor:
Miroshnyk Oleksii, V. N. Karazin Kharkiv National University, Ukraine
Technical Editor:
Pokrovska Mariia, V. N. Karazin Kharkiv National University, Ukraine

EDITORIAL BOARD:

Abdul Aziz Abdul Rahman, Kingdom University, Bahrain
Adamonienė Rūta, Mykolas Romeris University, Lithuania
Akimova Liudmyla, National University of Water and Environmental Engineering, Ukraine
Babichev Anatoliy, V. N. Karazin Kharkiv National University, Ukraine
Balezentis Tomas, Lithuanian Centre for Social Sciences, Lithuania
Baranova Valeria, V. N. Karazin Kharkiv National University, Ukraine
Dankevych Andriy, National university of food technologies, Ukraine
Doherty Bob, Professor, School of Business and Society, University of York, UK
Ilich Lyudmila, Borys Hrinchenko Kyiv University, Ukraine
Gorockovatskyi Volodymyr, Kharkiv National University of Radio Electronics, Ukraine
Husam-Aldin Nizar Al-Malkawi, The British University in Dubai, United Arab Emirates
Karas Michal, Brno University of Technology, Czech Republic
Melnychenko Oleksandr, Gdańsk Polytechnic University, Poland
Nurul Mohammad Zayed, Daffodil International University, Bangladesh
Semenog Andrii, Sumy State University, Ukraine
Sergienko Olena, National Technical University «Kharkiv polytechnic institute», Ukraine
Simanaviciene Zaneta, Mykolas Romeris University, Lithuania
Tkachenko Natalia, Taras Shevchenko National University of Kyiv, Ukraine
Zhytar Maksym, National University "Kyiv Aviation Institute", Ukraine

The Collection «Financial and Credit Systems: Prospects for Development» is included in category B of the professional publications of Ukraine (Order of Ministry of Education and Science of Ukraine 582 from April 24, 2024; Order of Ministry of Education and Science of Ukraine 928 from June 26, 2026) in following specialties: C1 Economics (0311 Economics); C3 International Relations (0312 Political sciences and civics, 0314 Sociology and cultural studies); D1 Accounting and Taxation (0411 Accounting and taxation); D2 Finance, Banking, Insurance and Stock Market (0412 Finance, banking and insurance); D3 Management (0413 Management and administration; 0415 Secretarial and office work); D4 Public Administration and Management (0413 Management and administration); D5 Marketing (0414 Marketing and advertising); D7 Trade (0414 Marketing and advertising, 0416 Wholesale and retail sales).

Approved for publication by the decision of the Academic Council
of V.N. Karazin Kharkiv National University (protocol № 17 dated 05.10.2026)

All rights reserved. Reprints and translations are permitted only with the consent of the author and the Editorial team. The Editorial team do not always share the author's opinion and are not responsible for the factual mistakes he made.

Founder:
V. N. Karazin Kharkiv National University,
Mailing address: Svobody sq., 4, 61022, Kharkiv, Ukraine. **www.karazin.ua**
Collection website: **https://periodicals.karazin.ua/fcs** E-mail: **fcs.journal@karazin**
Media identifier in the Register of the field of Media Entities: R30-04477 (Decision № 1538 dated May 9, 2024 of the National Council of Television and Radio Broadcasting of Ukraine, Protocol № 15)

© V. N. Karazin Kharkiv National University, 2026

Зміст

Фінанси, облік, аудит та оподаткування

Бабенко Максим, Бітнер Ірина, Пивавар Ірина, Литвиненко Андрій
Антикризове управління репутацією бренду банку в епоху цифрових комунікацій 9

Кочорба Валерія
Цифровізація банківського сектору
як чинник зміни поведінкових моделей фінансових рішень 31

Морозова Надія, Годлевський Максим
Стратегічні пріоритети розвитку банківського брендингу
в умовах цифрової трансформації фінансового сектору 46

Ткачук Наталія, Машталяр Ольга
Ретроспективний генезис та стратегічні вектори розвитку банківської системи України 60

Фінанси, облік, аудит та оподаткування

Маслов Роман
Концептуалізація сутності місцевих податків: науковий дискурс 73

Іващенко Марина
Поведінкові фінанси та механізми стимулювання витрат у сучасних відеоіграх 82

Кльоба Лев, Кльоба Руслан, Кльоба Віктор
Перспективи використання штучного інтелекту фінансовими установами України 100

Черкашина Катерина, Пасько Тетяна
Інтегрована модель управління зеленим кредитуванням для сталого фінансування 115

Худавердієва Вікторія
ESG-фінансування як інструмент забезпечення сталого розвитку
міжнародного туризму: сучасні тенденції та перспективи 135

Економіко-математичні методи та моделі фінансового розвитку

Баландіна Наталія
Лінійна алгебра як основа алгоритмів штучного інтелекту в економічних дослідженнях 157

Сучасні макроекономічні тренди та тенденції

Городянська Лариса
Система повоєнного відтворення економічних ресурсів України 171

Банки сучасного та майбутнього

Banks of the present and the future

https://doi.org/10.26565/2786-4995-2026-3-01
UDC 005.334:336.71:659.4

Babenko Maksym
PhD, Associate Professor at the Department of Management, Accounting and Business Communications, V.N. Karazin Kharkiv National University
Svobody Square, 4, Kharkiv, 61022, Ukraine
e-mail: babenkomv2011@gmail.com
ORCID ID: 0000-0001-6792-3465
Bitner Iryna
PhD in Economics, Associate Professor, Associate Professor Department of Banking Business and Financial Technologies, V. N. Karazin Kharkiv National University
4 Svobody Square, Kharkiv, 61022, Ukrain
e-mail: irinabitner@karazin.ua
ORCID ID: 0000-0003-0269-5670
Pyvavar Iryna
PhD in Economics, Associate Professor, Associate Professor at the Department of State Governance, Public Administration and Economic Policy, Simon Kuznets Kharkiv National University of Economics
Nauky Avenue, 9A, Kharkiv, 61166, Ukraine
e-mail: pivavariv@ukr.net
ORCID ID: 0000-0002-6115-0200
Lytvynenko Andrii
PhD in Economics, Associate Professor, Associate Professor at the Department of State Governance, Public Administration and Economic Policy, Simon Kuznets Kharkiv National University of Economics
Nauky Avenue, 9A, Kharkiv, 61166, Ukraine
e-mail: in4.andrey@gmail.com
ORCID ID: 0000-0001-5973-5173

Crisis management of bank brand reputation in the era of digital communications

Abstract. The full-scale war, digitalization, and the growing prevalence of cyber threats have increased the importance of bank brand reputational resilience. The study systematizes reputational risks, proposes a Digital Reputational Resilience Index, and develops a comprehensive crisis management model focused on crisis prevention, rapid response, and the restoration of customer trust. A comprehensive approach is substantiated that integrates digital monitoring, crisis communication, cyber resilience, artificial intelligence technologies, and adaptation to European requirements.

Problem statement. Despite the rapid digitalization of banking services, crisis management of bank brand reputation remains insufficiently systematic amid growing wartime, cyber, and information-related threats. Traditional approaches to reputation management do not fully account for the speed at which information spreads in the digital environment, the development of generative artificial intelligence, the need to rapidly restore customer trust, and increasingly stringent requirements for digital operational resilience in the context of Ukraine's European integration.

Unresolved issues. Despite the considerable body of research on bank reputation, crisis communication, and digital resilience, comprehensive approaches to crisis management of bank brand reputation in the digital environment remain insufficiently developed. Further research is required into the interrelationships between digital and reputational risks, the speed of crisis response, the use of artificial intelligence, banks' ability to restore customer trust, and the development of their reputational resilience.

© Babenko Maksym, Bitner Iryna, Pyvavar Iryna, Lytvynenko Andrii, 2026
This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0.

Purpose of the article. The purpose of the article is to substantiate a comprehensive approach to crisis management of bank brand reputation and to enhance its reputational resilience in the context of digitalization, wartime risks, the development of artificial intelligence, and Ukraine's European integration.

Main material. The study is based on systemic, process-based, and risk-oriented approaches to crisis management of bank brand reputation in the digital environment. The article examines the evolution of bank reputation in the context of digitalization, systematizes the main categories of reputational risks, and analyzes the impact of wartime threats, digital communications, cyber risks, generative artificial intelligence, and European integration processes on customer trust. An original Bank Digital Reputational Resilience Index (IDRS) is proposed, integrating the quality of digital communications, the level of trust, the effectiveness of crisis response, digital and cyber resilience, and bank adaptability. A cyclical reputation crisis management model comprising the PRE-CRISIS, CRISIS, POST-CRISIS, and RESILIENCE stages is developed. Practical recommendations are also formulated to strengthen the reputational resilience of Ukrainian banks, taking into account wartime challenges, advances in AI, and European requirements for digital operational resilience.

Conclusions. Crisis management of bank brand reputation in the digital environment requires the integration of reputational, communication, technological, and security-related components into a unified management system. The proposed Bank Digital Reputational Resilience Index (IDRS) and the developed model enable a comprehensive assessment of a bank's capacity to withstand reputational threats, maintain customer trust, and leverage crisis experience to strengthen its future resilience. For Ukrainian banks, particular importance should be attached to combining digital reliability, effective crisis communication, AI capabilities, and European approaches to digital operational resilience.

Keywords: *crisis management, bank reputation, bank brand, reputational resilience, digital communications, reputational risk, digital resilience, artificial intelligence, cyber risks, customer trust.*

Formulas: 1; figures: 1; tables: 5; references: 20.

JEL Classification: G21, M31, M15, O33.

For citation: Babenko Maksym, Bitner Iryna, Pyvavar Iryna, Lytvynenko Andrii. Crisis management of bank brand reputation in the era of digital communications. Financial and Credit Systems: Prospects for Development. №3(22) 2026. P. 9-30. https://doi.org/10.26565/2786-4995-2026-3-01

Introduction. The full-scale invasion has transformed the operating environment of Ukraine's banking sector and the structure of risks faced by financial institutions. Banks operate amid wartime threats, cyberattacks, disruptions to electricity and communications, infrastructure damage, customer migration, and the growing use of remote banking services. Under these circumstances, a bank's ability to ensure the continuity of financial services directly affects the level of customer trust. For a bank brand, reputation becomes particularly important when customers assess the institution based on the speed of service restoration, the availability of information, and the nature of its communication during disruptive events.

The digitalization of banking services has transformed the mechanisms through which reputation is formed. Mobile applications, online banking, social media, messaging platforms, chatbots, and online customer support have become permanent channels of interaction between banks and their customers. Any disruption to a digital service can be immediately reported by users and rapidly disseminated through social media. Under such conditions, an isolated operational problem may escalate into a large-scale information issue even before the bank has completed its technical resolution. Reputational risk arises when customers' perceptions of an event and its representation in the information environment begin to affect trust in the brand. For Ukrainian banks, this situation is further complicated by the interaction between wartime and digital risks. Cyberattacks on financial infrastructure, phishing campaigns, the dissemination of false information, fraudulent messages impersonating banks, and attempts to gain unauthorized access to customer data create threats that simultaneously have technological, informational, and reputational dimensions [1].

Ukraine's European integration trajectory is another important factor transforming the banking environment, as it strengthens requirements for digital operational resilience, ICT risk management, cybersecurity, consumer protection, and transparency in banking activities. Consequently, the convergence of wartime risks, digitalization, advances in artificial intelligence,

and European integration processes is creating new conditions for managing bank brand reputation. This necessitates a comprehensive crisis management approach focused on the early detection of reputational threats, rapid response, consistent digital communication, and the restoration of customer trust following crisis events [1].

Literature review. The issue of reputation management in banking institutions lies at the intersection of research on reputational risk, bank branding, crisis communication, digital transformation, and operational resilience. In the digital environment, these areas are becoming increasingly interconnected, as reputational consequences for a bank may arise not only from communication failures but also from operational disruptions, cyber incidents, information attacks, security breaches affecting digital services, and changes in customer behavior on social media.

The theoretical foundations for studying banks' reputational risk have been established in research addressing its nature, sources, and consequences for financial institutions. Z. K. Sorokivska [10] examines the impact of a bank's reputational risk on retail banking, confirming the close relationship between a financial institution's reputation and customer behavior. A. I. Khrystin [12] investigates the reputational risks faced by contemporary Ukrainian banks, emphasizing the specific features of their manifestation in the domestic banking environment. A more comprehensive perspective is provided by D. Adeabah, C. Andoh, S. Asongu, and A. Gemegah [11], who systematize the main research streams, conceptual approaches, and methods used to analyze reputational risk in the banking sector. Taken together, these studies provide grounds for viewing reputational risk not solely as a marketing or communication-related category, but as a multidimensional risk capable of affecting a bank's interactions with customers and other stakeholders.

A distinct strand of the literature focuses on crisis communication and its impact on organizational trust. A. D. Beldad, E. van Laar, and S. M. Hegner [2] analyze the relationship between the timing of crisis communication, an organization's prior reputation, the type of crisis, and the level of trust following a crisis event. The importance of the temporal dimension of communication response is also examined by S. Xu, W. Huang, and L. Weng [6], who focus on response speed and message characteristics in the digital environment. Y. Kim and Y. Sung [19] examine the relationship between corporate reputation and public crisis communication on social media. In a broader context, W. T. Coombs and D. Laufer [20] systematize contemporary research directions in global crisis management. These studies demonstrate that the effectiveness of crisis response is determined not only by the content of the message, but also by the speed with which it is communicated, the pre-existing level of trust, and the characteristics of the information environment.

The expansion of digital channels has significantly transformed the mechanisms through which reputation and bank brands are formed. L. Fedevych and A. Blavt [5] examine the use of modern social media technologies in the marketing policies of commercial banks, demonstrating the growing importance of digital platforms in banks' interactions with their audiences. M. O. Hodlevskyi and N. L. Morozova [18] explore the specific features of bank branding in the digital environment, where digital channels have become an important space for shaping customers' perceptions of banks. At the same time, A. Siano, A. Vollero, and A. Bertolini [7] conceptualize the shift from brand control to the co-creation of brands by multiple actors within the communication environment, while P. Foroudi et al. [9] emphasize the co-creation of brand image and reputation through stakeholder social networks. This perspective is particularly relevant to banks, as digital brand reputation is shaped simultaneously by an institution's official communications, customer experience, user-generated content, media coverage, and digital communities.

The continued development of digital financial technologies further strengthens the interrelationship between the technological environment and corporate reputation. Y. Jiang and X. Zheng [8] directly link digital media communication, FinTech, and corporate reputation, confirming the need to incorporate technological factors into contemporary reputation management systems. At

the same time, a distinctive feature of digital platforms is the algorithmic nature of information dissemination. The study by W. J. Brady, K. McLoughlin, T. N. Doan, and M. J. Crockett [13] demonstrates the importance of social learning mechanisms in amplifying emotionally charged content on online social networks. In the context of bank reputation, this implies that the scale of the information response to a crisis event may depend not only on the objective significance of the event itself, but also on how information about it is disseminated and how audiences engage with digital content.

An emerging area of reputational risk is associated with the development of artificial intelligence technologies. Ye. Temchenko [3] systematizes the applications of AI in banking, along with the related challenges and strategic implications. M. Yakovlev and V. Liubchak [14] examine the potential of artificial intelligence for detecting and preventing phishing attacks and cyber threats. In the context of crisis reputation management, this makes it possible to consider AI in a dual role: on the one hand, as a technological environment giving rise to new risks associated with synthetic content, automated disinformation, and increasing difficulties in identifying reliable information; and, on the other hand, as a tool for monitoring, analyzing digital signals, and detecting potential crises at an early stage.

The intensification of digital threats has simultaneously increased the relevance of operational and cyber resilience for financial institutions. Ye. Kurii, V. Susukailo, A. Yerofieieva, and M. Nesteriuk [4] analyze the requirements of the Digital Operational Resilience Act (DORA), which establish a new European approach to information and communication technology (ICT) risk management and digital operational resilience. For the banking sector, these requirements have not only technological but also reputational significance, as an institution's ability to maintain the continuity of digital services, respond appropriately to incidents, and protect customer information directly affects perceptions of its reliability.

For Ukraine, these issues have acquired additional significance in the context of the full-scale war. V. Apatskyi [1] examines the functioning of Ukrainian banks amid wartime risks, cyber threats, and uncertainty. N. E. Avanesova and I. V. Bakalo [15] address the challenges of ensuring the financial stability of the banking system under martial law, while U. Ya. Hrudzevych, O. P. Sidelnyk, and O. V. Nahorniuk [16] identify the problems and development priorities of Ukraine's banking system during the war. The European integration trajectory of financial sector development is also reflected in the strategic documents of the National Bank of Ukraine [17]. Taken together, these factors create a specific operating environment in which the reputation of a Ukrainian bank depends not only on traditional brand characteristics but also on its ability to ensure service continuity, digital security, rapid communication, and adaptation to new regulatory requirements.

Thus, the existing literature provides a sufficiently comprehensive examination of individual aspects of the research problem, including banks' reputational risk [10–12], crisis communication and the role of response speed [2, 6, 19, 20], the transformation of brands and reputation under the influence of digital channels [5, 7–9, 18], the opportunities and risks associated with artificial intelligence [3, 14], digital and operational resilience [4], and the specific features of Ukrainian banks' operations in the context of war and European integration [1, 15–17]. At the same time, these research areas are predominantly examined in isolation.

A comprehensive approach to crisis management of bank brand reputation remains insufficiently developed. Such an approach should integrate reputational, communication, operational, cyber, and AI-related risks into a unified system and encompass the entire crisis management cycle—from the early detection of digital signals and risk assessment to rapid communication, the restoration of trust, and the use of crisis experience to strengthen the bank's future reputational resilience. The comprehensive assessment of such resilience also requires further methodological development, taking into account the quality of digital communications, the level of customer trust, the effectiveness of crisis response, digital and cyber resilience, and bank adaptability. Addressing this research gap determines the subsequent logic of the present study.

Purpose, objectives and research methods. The purpose of the article is to substantiate a comprehensive approach to crisis management of bank brand reputation and to identify directions for strengthening its reputational resilience in the context of digitalization, the full-scale war, the development of artificial intelligence, and Ukraine's European integration.

To achieve this purpose, the following objectives were defined: to clarify the concept of "bank reputational resilience"; to systematize the main reputational risks faced by banks in the digital environment; to determine the impact of wartime, technological, and informational factors on bank brand reputation; to examine the role of digital communications and artificial intelligence in preventing and overcoming reputational crises; to substantiate an approach to assessing a bank's digital reputational resilience; and to formulate recommendations for improving crisis management of Ukrainian banks' reputation in the context of European integration.

The scientific novelty of the study lies in developing a comprehensive approach to crisis management of bank brand reputation in the digital environment by integrating reputational, communication, operational, cyber, and AI-related risks into a unified management system. The Bank Digital Reputational Resilience Index (IDRS) is proposed, combining five components: the quality of digital communications, digital trust, the effectiveness of crisis response, digital and cyber resilience, and adaptability. A cyclical model of bank brand reputation crisis management, PRE-CRISIS → CRISIS → POST-CRISIS → RESILIENCE, is developed. Its distinctive feature is the transformation of crisis experience into managerial changes aimed at enhancing the bank's preparedness for future crises.

The methodological framework of the study combines systemic, process-based, and risk-oriented approaches to examining crisis management of bank brand reputation. The systemic approach is used to consider reputation as the outcome of interactions between the bank, its customers, digital platforms, the media, and other actors within the information environment. The process-based approach is applied to examine the sequence of crisis management actions, from monitoring and identifying potential threats to response, restoration of trust, and evaluation of outcomes. The risk-oriented approach is used to systematize reputational risks associated with digital services, cyber threats, information attacks, and crisis communication.

The study employs analysis and synthesis to examine scholarly approaches to reputation management and crisis communication; classification methods to systematize banks' reputational risks; comparative analysis to identify the specific features of banks' crisis communication; content analysis to examine digital messages and banks' responses in crisis situations; and generalization to formulate practical recommendations for strengthening bank brand reputational resilience.

Research results. Bank reputation has traditionally been viewed as the result of accumulated experience arising from the interactions of customers and other stakeholders with a financial institution. It has been shaped by the bank's financial stability, quality of service, fulfillment of obligations, regulatory compliance, corporate culture, and public image. Under this model, banks had considerably greater control over the content and channels through which information about their activities was disseminated. The principal instruments for building reputation included advertising, public relations, mass media, official communications, and direct interaction with customers.

The spread of digital technologies has gradually transformed the mechanism of bank reputation formation. The Internet has enabled customers to publicly express their assessments of banks' activities and disseminate information to broad audiences. User reviews, comments on specialized online platforms, social media posts, and forum discussions have become additional sources of information about banks. As a result, reputation has increasingly been shaped by both banks' official communications and independent user-generated content.

The next stage is associated with the development of social media and mobile digital services. Banks have become participants in continuous online communication. Within the same digital environment, customers can ask questions, submit complaints, share their experiences of

using banking services, and receive responses from the bank. Accordingly, digital reputation is shaped through a substantially greater number of interactions than traditional reputation, while a bank's response to a particular situation becomes visible to other users.

This stage can be defined as interactive reputation. Its distinctive feature is the two-way nature of communication. Customers are no longer passive recipients of information but become active participants in shaping the bank's information image. Reputation is influenced by user ratings and assessments, public responses from bank representatives, discussions within digital communities, and the activities of bloggers and the media. The reactions of other users to individual messages are also important, including content sharing, comments, ratings, and other forms of digital engagement [5].

The current stage is characterized by a shift toward real-time reputation. An information-related event can gain considerable visibility within a short period, while its perception may change depending on the responses of the bank, customers, the media, and digital communities. A technical failure, payment delay, or report of a potential cyberattack may become the subject of public discussion even before the bank has completed its internal assessment of the situation. Under such conditions, the time interval between the emergence of a problem, its public dissemination, and the formation of a reputational response is significantly reduced [6].

The evolution of bank brand reputation can be represented as a sequential transition from predominantly controlled communication to a distributed and dynamic process of reputation formation (Fig. 1).

Stage	Main environment	Key actors shaping reputation	Nature of reputation
Traditional reputation	Mass media, advertising, offline interactions	Bank, mass media, customers	Relatively stable
Digital reputation	Website, online banking, online media	Bank, customers, digital media	Dynamic
Interactive reputation	Social media, messaging platforms, review platforms	Bank, customers, bloggers, digital communities	Two-way and networked
Real-time reputation	Digital ecosystem, social media, AI platforms	Bank, customers, bloggers, algorithms, digital communities, malicious actors	Continuously evolving

Fig. 1. Evolution of Bank Brand Reputation in the Context of Digitalization
Source: developed by the authors based on [7, 8].

At the current stage, a bank can no longer be regarded as the sole actor managing its own reputation. Reputation is formed within a distributed digital environment in which various stakeholder groups and technological systems interact [9]. This process can be conceptualized as a combination of several information flows: the bank's official communication, customer responses,

dissemination through social media, interpretation by the media and bloggers, algorithmic amplification, and subsequent audience reactions.

Malicious actors may also become involved in this process by disseminating false information, creating phishing messages, or impersonating the bank's official communication channels. Consequently, contemporary reputation is formed in an environment where reliable information, subjective user assessments, journalistic content, commercial content, and deliberate disinformation may simultaneously compete for audience attention.

Changes in the mechanism of reputation formation also affect approaches to reputation management. Whereas the traditional model primarily focused on creating a desired image of the bank and communicating it through controlled channels, the digital environment requires continuous monitoring of information flows and rapid responses to changes in brand perception. Reputation management is gradually evolving from a predominantly communication-oriented function into a cross-functional process involving marketing, public relations, customer service, IT, cybersecurity, risk management, and bank management [9].

For Ukrainian banks, this transformation has an additional dimension. In the context of the full-scale war, information concerning the availability of banking services, the stability of digital services, cyber incidents, and the security of customer funds is of heightened public importance. Consequently, reputation is becoming increasingly closely linked to a bank's actual ability to ensure business continuity and communicate clearly with customers during crisis events.

Contemporary bank brand reputation should therefore be viewed as a dynamic outcome of interactions among the bank, customers, the media, digital platforms, algorithms, and other actors within the information environment. This shift in perspective has direct implications for crisis management, as any element of digital interaction may become a source of a reputational crisis.

A bank's reputational risk has a distinctive nature due to the close relationship between customer trust, financial behavior, and the information environment. Negative information may influence customers' decisions regarding the use of banking services, their activity across digital channels, their willingness to recommend the institution to other users, and their overall perception of the bank's reliability [10].

In the digital environment, reputational risk rarely emerges as an isolated event. For example, a technical failure may trigger negative customer comments on social media. If the bank fails to provide a timely explanation, the volume of negative mentions may increase. In the absence of clear communication, the media or bloggers may become involved in the information flow. At the same time, malicious actors may exploit the situation to disseminate phishing messages. As a result, a single operational problem may generate a set of interconnected reputational risks [11].

Taking this into account, the main categories of a bank's reputational risks are classified according to their source of origin and the nature of their impact on digital reputation (Table 1).

The proposed classification makes it possible to view reputational risk more broadly than merely as a consequence of ineffective communication. Its source may be a technical incident, a cyber threat, a breach of regulatory requirements, or the actions of third parties within the digital environment. At the same time, one type of risk may trigger others. This interconnectedness is a distinctive feature of the contemporary digital banking environment.

For example, a crisis may develop through the following sequence: an operational failure may trigger negative customer reactions and the dissemination of information across social media and media channels, which, in turn, may increase customer distrust and stimulate fraudulent messaging, ultimately placing additional pressure on customer support services.

Another scenario may originate from a cyber incident. Following a potential cyberattack, information about the incident may reach customers, after which negative rumors and false messages may spread, increasing customers' concerns about the security of their funds and adversely affecting their level of trust in the bank.

Table 1. Classification of Banks' Reputational Risks in the Digital Environment

Risk category	Main manifestations	Potential reputational consequences
Operational risks	Mobile application failures, online banking unavailability, payment delays, service disruptions	Reduced perceptions of service reliability and quality
Cyber risks	Cyberattacks, data breaches, phishing, compromise of digital channels	Loss of trust in the bank's security and digital infrastructure
Information-related risks	Fake messages, rumors, manipulative content, false publications	Formation of a negative or distorted image of the bank
Communication risks	Delayed response, inconsistent messages, language that is difficult for customers to understand	Intensification of negative reactions and erosion of trust
Social risks	Large-scale dissemination of negative reviews, public conflicts with customers, information campaigns	Rapid deterioration in the sentiment of digital mentions
Regulatory risks	Violation of regulatory requirements, sanctions, claims by regulators	Reduced confidence in the bank's reliability and compliance with established requirements
Ethical risks	Non-transparent terms and conditions, manipulative advertising, improper handling of customer data	Perception of the bank as irresponsible
AI-related risks	Deepfakes, automated disinformation, synthetic reviews, impersonation of official communications	Rapid dissemination of false information and increased difficulty in refuting it

Source: developed by the authors based on [11, 12].

Thus, reputational risk should be analyzed as the result of interactions among risks of different origins rather than as a separate category arising exclusively from failures in public relations or marketing communications [11].

Assessing reputational risk requires not only identifying the occurrence of a negative event but also determining the speed at which its effects progress across different information and response levels. In this context, four consecutive levels can be distinguished:

- Event – the occurrence of an operational, cyber, regulatory, or other problem;
- Information response – the emergence of messages or reactions from customers, employees, the media, or third parties;
- Reputational response – a change in attitudes toward the bank and in the level of trust;
- Behavioral response – changes in customer behavior, including contacting customer support, discontinuing the use of particular services, switching to competitors, or sharing negative experiences.

This sequence makes it possible to distinguish the initial cause of a crisis from its reputational consequences. It also demonstrates that the speed and quality of a bank's communication can influence the progression of a problem from one level to another [2].

Digital algorithms play a particularly important role within this system. Algorithmic mechanisms employed by social media and search platforms determine which content receives greater visibility. Emotionally charged messages or content generating high levels of engagement may spread more rapidly than neutral explanations provided by the bank. As a result, a reputational crisis may develop according to dynamics that are not directly controlled by the bank [13].

The situation becomes even more complex with the use of generative artificial intelligence. Synthetic content can be produced on a large scale and adapted to different digital channels. For banks, this creates a need to monitor not only their own information channels but also the broader external digital environment, where content impersonating or misrepresenting the institution's official position may emerge [14].

The specific nature of contemporary bank reputational risks is determined by three key characteristics:

- the diversity of risk sources;
- the interdependence of individual risk events;
- the high speed of information dissemination.

These characteristics alter the logic of crisis management. To ensure a timely response, banks need to monitor not only direct manifestations of reputational risk but also operational, cyber, informational, regulatory, and technological factors that may trigger them [11].

Therefore, further development of crisis management of bank brand reputation should be based on the principle of integrated risk and digital communication management. Within such a model, reputational resilience depends on the bank's ability to identify a problem in a timely manner, assess its potential to generate wider information effects, coordinate the actions of responsible units, provide customers with reliable information, and manage the restoration of trust following the resolution of a crisis.

The full-scale war has changed the nature of risks faced by the Ukrainian banking sector. In addition to financial and operational risks, banks now face cyberattacks, disruptions to electricity and communications, infrastructure damage, information attacks, and fraudulent campaigns. For banks, these risks are directly linked to reputation, as the stability of digital services, access to funds, and transaction security shape customers' everyday experience. At the same time, the Ukrainian banking system continues to demonstrate operational resilience and ensure the functioning of critical financial services despite wartime constraints [15, 16].

Cyber risks and information threats have become particularly significant. A cyberattack, data breach, or phishing incident may have consequences extending far beyond the technical problem itself, as customers begin to question the bank's security and the safety of their funds. A similar effect may arise from the dissemination of fake messages or fraudulent content impersonating the bank's communications. In such situations, the speed of response, the reliability of information provided, and the clarity of recommendations for customers directly influence perceptions of the bank brand [14].

The war has also increased the importance of banking service continuity. When customers conduct a substantial proportion of their financial transactions remotely, the stability of mobile applications, online banking, and customer support channels becomes an integral part of their assessment of the bank. Reliability, therefore, is no longer merely a characteristic declared by the bank in its communications; it is demonstrated through actual performance during crisis events [15]. In this context, the concept of "reputation through resilience" can be introduced, referring to the development of trust based on a bank's ability to maintain critical services, protect customers, and ensure clear communication under conditions of external risk.

The second major factor transforming the reputation of Ukrainian banks is European integration. The alignment of Ukraine's financial sector with European Union standards involves the development of approaches to consumer protection, transparency, cybersecurity, technology risk management, and digital operational resilience. For banks, this implies a change in the criteria by which customers and other stakeholders assess the reliability of financial institutions. The National Bank of Ukraine identifies the European integration of the financial sector as one of the key directions of its development [17].

The European Digital Operational Resilience Act (DORA) serves as an important benchmark for digital resilience in Ukraine's financial sector. It establishes requirements for ICT risk management, digital incident response, digital operational resilience testing, and the management of risks associated with third-party technology providers. European practice demonstrates that technological, cyber, and reputational risks are becoming increasingly interconnected. The development of artificial intelligence further expands this spectrum of risks by creating new opportunities for fraud, disinformation, and attacks on digital systems [4].

The current Ukrainian context is shaping a specific model of bank brand reputation. It is based on consistency between a bank's public communications and its actual ability to ensure service stability, protect customers, and respond effectively to crisis situations. The war has increased the importance of resilience as a source of trust, while European integration introduces new requirements for digital security, transparency, and bank accountability [15]. Reputational resilience should therefore be viewed as the outcome of the interaction between a bank's

operational capabilities, the quality of its digital communications, and its ability to adapt to new technological and regulatory requirements.

Contemporary bank communication is no longer limited to social media. Customers interact with a bank brand through mobile applications, websites, chatbots, contact centers, email, messaging platforms, social media, review platforms, and other digital services. An additional information context is shaped by the media, search engines, thematic communities, and AI-powered platforms. Together, these channels form an integrated environment in which customers obtain information about the bank and develop their own assessments of its activities [18].

It is therefore appropriate to introduce the concept of a "bank digital reputation ecosystem." This is proposed to be understood as the set of digital channels, platforms, information resources, and actors through which perceptions of a bank are formed, disseminated, and transformed. A distinctive feature of this ecosystem is the interconnectedness of its channels: information originating in one environment can rapidly spread to others.

For example, a technical failure in a mobile application may initially be identified by users. Some customers may contact customer support, while others may post about the problem on social media or review platforms. If the disruption persists, information about it may reach the media or thematic online communities. Search engines may begin displaying relevant content in response to user queries, while social platform algorithms may amplify posts that generate high levels of engagement. As a result, an initial operational problem becomes part of a broader information process.

Within this system, each channel performs a distinct function. Mobile applications and websites provide direct access to banking services; chatbots and contact centers provide operational customer support; social media and messaging platforms facilitate public communication; the media and bloggers influence the broader information environment; review platforms aggregate customer experiences; search engines determine the accessibility and visibility of information to users; and AI-powered platforms may generate additional summaries based on available digital content.

For a bank's reputation, consistency of information across channels becomes particularly important. If customers receive different explanations through the mobile application, social media, and customer support services, this increases uncertainty and may intensify negative reactions. Crisis communication therefore requires coordination across all major digital customer touchpoints.

The digital reputation ecosystem has another distinctive feature: its formation involves actors that are not directly controlled by the bank. Customers, journalists, bloggers, administrators of online communities, and other users create their own content and influence its dissemination. In addition, the visibility of information is shaped by digital platform algorithms. Consequently, a bank can control its own communications but cannot fully control the broader information context in which these communications are perceived [9].

Reputation management in the digital environment therefore requires managing not merely individual channels but the entire system of digital interactions. The bank's task is to ensure message consistency, continuously monitor the information environment, and respond promptly to changes in brand perception [18].

One of the key characteristics of a digital reputational crisis is the speed of information dissemination. In traditional media, there was a certain time lag between the occurrence of an event and its widespread coverage. In the digital environment, this interval has been substantially reduced. Users can disseminate information immediately after a problem occurs, while its subsequent spread depends on audience reactions and platform algorithms [19].

This makes it possible to view a reputational crisis as a race against time. Three temporal parameters can be distinguished in its development:

T_1 – the time at which the problem occurs or is detected;

T_2 – the time at which information about the problem gains significant public visibility;

T_3 – the time of the bank's first official response.

A favorable scenario for the bank is $T_1 < T_3 < T_2$. In this case, the bank is able to provide official information before negative information gains significant public visibility.

If $T_1 < T_2 < T_3$, information about the problem gains significant public visibility before the bank formulates and communicates its official position. In such a situation, an information vacuum emerges. This vacuum may be filled by speculation, unverified reports, user comments, or deliberate disinformation.

Response speed should therefore be regarded as an independent parameter of crisis reputation management. At the same time, rapid response should not imply the dissemination of unverified information. A bank must simultaneously minimize the time between detecting a problem and issuing its first official response while ensuring the accuracy and reliability of the information communicated.

In this context, it is appropriate to distinguish between initial and comprehensive crisis communication. The initial communication should acknowledge the existence of a problem, once confirmed, and explain the next steps to customers. Comprehensive communication may follow once the causes and scale of the incident have been established. This approach helps prevent prolonged silence by the bank while complete information about the incident is still unavailable.

Response speed also remains important after the initial communication. Crisis-related information requires regular updates, as customers assess not only whether the bank has issued an initial response but also whether they continue to receive new information as the situation develops. In the absence of updates, the initial message may quickly lose its effectiveness, allowing external sources to once again dominate the information environment.

For Ukrainian banks, the issue of response speed is particularly relevant in cases of cyberattacks, digital service disruptions, and fraudulent campaigns. In such situations, customers need to understand quickly whether a service is operational, whether their funds are secure, whether they need to change a password or block a payment card, and where they can obtain reliable information. The absence of clear guidance may intensify distrust regardless of how quickly the bank resolves the underlying technical problem [14].

Thus, the digital environment transforms the temporal structure of a reputational crisis. Its scale is determined not only by the nature of the initial event but also by the relationship between the speed of information dissemination and the speed of the bank's response [2]. Effective crisis management should therefore involve continuous monitoring of the digital environment, the establishment of threshold values for triggering a crisis response, and the development of communication scenarios in advance.

To summarize the proposed approach, the interaction between digital channels and the time factor can be represented as a sequential model comprising the following stages: the occurrence of a crisis event, its detection, the initial information response, information dissemination, the bank's official communication, information updates, stabilization of the information environment, and restoration of customer trust. Within this model, digital communications serve as the link between an operational event and its reputational consequences. The faster a bank detects a problem, assesses its potential to generate wider information effects, and ensures consistent communication, the greater its ability to limit the reputational impact of the event.

The development of generative artificial intelligence is transforming the environment in which bank brand reputation is formed. AI technologies facilitate the creation of text, images, audio, and video content that can imitate a bank's official communications. False messages concerning account restrictions, changes in service terms, technical problems, or security threats may spread through social media, messaging platforms, and other digital channels even before the bank issues an official response.

Emerging reputational risks include deepfake videos and audio, synthetic images, imitation of a bank's communication style, automated generation of negative content, bot networks, and large-scale fake reviews. The combination of AI-generated content and cybercrime poses a particular threat: a fraudulent message may simultaneously damage the bank's reputation and direct customers to malicious online resources.

Another challenge is the speed at which such content can be scaled and disseminated. A single information attack can be adapted to different audiences and distributed simultaneously across multiple channels. For banks, this creates a need to monitor not only their own communications but also the broader information environment surrounding the brand.

At the same time, AI has a dual nature: it both increases reputational risk and expands the opportunities for its early detection. Automated analysis of digital sources makes it possible to monitor changes in the volume of bank-related mentions, message sentiment, the emergence of recurring narratives, and anomalous spikes in online activity.

Artificial intelligence can support crisis management through a sequential process involving the monitoring of the information environment, anomaly detection, analysis of information sentiment and content, assessment of the scale of potential risk, forecasting its dissemination, selection of the optimal response scenario, and monitoring of the recovery process. However, the final decision regarding the bank's public position should remain with the bank's professionals. AI should be used to facilitate the rapid collection and analysis of information, identify potential problems, and support managerial decision-making [14].

In 2026, artificial intelligence is becoming both a source of new reputational threats and a technological tool for brand protection. A bank's ability to rapidly distinguish a genuine crisis event from an artificially generated information signal, assess the scale of the threat, and promptly initiate coordinated communication is becoming a competitive advantage.

A comprehensive approach is required to assess a bank's ability to maintain customer trust and manage the reputational consequences of crisis situations. Individual indicators, such as the number of negative mentions, customer response time, or the level of cybersecurity, characterize only specific dimensions of the problem. To provide a comprehensive assessment of a bank's ability to withstand reputational threats in the digital environment, an original Index of Digital Reputation Resilience (IDRS) is proposed.

Unlike existing approaches that focus primarily on assessing individual aspects of reputation, trust, or operational resilience, the proposed index integrates five interrelated components:

- quality of digital communications (C);
- level of digital trust (T);
- speed and effectiveness of crisis response (R);
- digital and cyber resilience (S);
- ability to adapt communication to the nature and scale of the crisis (A) (Table 2).

Table 2. Structure of the Bank Digital Reputational Resilience Index

Component	Assessment dimension	Examples of indicators
C – Communication	Quality of digital communication	Consistency of messages across different channels; clarity of information; regularity of updates; availability of official communication channels
T – Trust	Level of digital trust	Sentiment of reviews; proportion of positive/negative mentions; customer trust assessment; willingness to use digital services
R – Response	Effectiveness of crisis response	Time to initial response; time to provide a comprehensive explanation of the situation; speed of information updates; proportion of customer inquiries that received a response
S – Security	Digital and cyber resilience	Number and scale of incidents; availability of digital services; measures to counter fraud; protection of customer data
A – Adaptability	Ability to adapt communication	Alignment of messages with the type of crisis; use of different communication channels; adaptation of messages to target audiences; ability to modify the communication strategy

Source: developed by the authors.

The composite indicator is proposed to be calculated using formula (1):

$$IDRS = w_1C + w_2T + w_3R + w_4S + w_5A, \quad (1)$$

де w_1-w_5 – are the weighting coefficients assigned to the respective components, with their sum equal to 1.

To ensure comparability, the indicators within each component should be normalized to a scale from 0 to 100. The weighting coefficients may be determined using expert assessment or based on surveys of banking sector professionals. At the initial stage of methodological testing, in the absence of empirically substantiated differences in the relative importance of the components, equal weighting is appropriate, with each of the five components assigned a weight of 0.20. Further testing of the methodology should involve refining the weighting coefficients based on expert assessments and empirical data, taking into account the specific characteristics of the bank and the nature of the crisis situation.

The proposed structure makes it possible to view reputational resilience as the result of interactions among several components. For example, a rapid bank response cannot compensate for poor communication quality if customers receive inconsistent messages. Similarly, a high level of digital security does not guarantee the preservation of trust if the bank fails to provide customers with sufficient information during an incident. The interdependence of these components is a fundamental distinction between the proposed approach and reputation assessment based on a single indicator.

To interpret the resulting value, a scale for assessing a bank's digital reputational resilience is proposed (Table 3).

Table 3. Interpretation of the Bank Digital Reputational Resilience Index (IDRS)

IDRS value	Level of reputational resilience	Characteristics
80–100	High	The bank has an established digital reputational resilience system and is capable of responding effectively to crisis situations
60–79	Sufficient	The main mechanisms are functioning, although certain components require improvement
40–59	Moderate	Noticeable reputational vulnerabilities exist, along with a risk of crisis escalation
20–39	Low	The response system has significant deficiencies, and customer trust is vulnerable to crisis events
0–19	Critical	The bank faces significant problems with digital communication, response, or resilience, creating a high risk of long-term reputational losses

Source: developed by the authors.

An important feature of the proposed index is its potential use not only for the overall assessment of a bank but also for monitoring changes in reputational resilience over time. For example, the IDRS may be calculated quarterly or following significant crisis events. Changes in the index before, during, and after a crisis make it possible to assess not only the initial level of resilience but also the bank's ability to restore customer trust.

The relationship among the individual components should also be analyzed separately. A low value of R may indicate a slow crisis response; a low C may signal communication problems; a low S may reveal digital and cyber vulnerabilities; a low T may indicate declining customer trust; and a low A may reflect insufficient adaptability of crisis communication. This approach makes it possible to move from merely identifying a problem to determining a specific area for managerial intervention.

The IDRS can be used as a tool for diagnosing and monitoring a bank's digital reputational resilience. Its practical value lies in integrating communication, behavioral, technological, and security-related characteristics into a single indicator. This makes it possible to assess reputation not as a static outcome of brand perception but as a dynamic characteristic of a bank's ability to maintain trust, respond to crisis events, and restore its reputational position in the digital environment.

The proposed model of bank reputation crisis management is based on a cyclical approach in which reputational risk management encompasses the periods before, during, and after a crisis. This approach assumes that crisis management measures are not limited to an immediate response to a negative event. They should begin at the stage of identifying potential threats, continue throughout crisis containment and crisis communication, and conclude with an assessment of the consequences and corresponding adjustments to management processes.

At the PRE-CRISIS stage, the primary focus is on monitoring the digital environment, identifying reputational risks, analyzing potential scenarios, and preparing response procedures. This makes it possible to reduce the time interval between the emergence of a problem and the bank's initial response. At the CRISIS stage, the priorities include verifying information, determining the scale of the incident, coordinating the actions of responsible units, communicating promptly with customers, and maintaining the availability of banking services. The POST-CRISIS stage involves assessing reputational consequences, analyzing customer responses and the digital information environment, restoring trust, and identifying the factors that contributed to the development of the crisis.

The RESILIENCE stage occupies a distinct position within the model. Its purpose is to transform the lessons learned from a crisis into specific changes in the management system. This includes reviewing crisis protocols, improving digital services, adjusting communication scenarios, enhancing staff competencies, strengthening monitoring, and updating the early warning system. Thus, the end of the active phase of a crisis does not signify the end of crisis management activities.

The cyclical nature of the model means that the findings derived from the analysis of a previous crisis are incorporated into preparations for future risks. If a particular communication channel proves insufficiently effective, the procedures governing its use are revised; if a problem results from delayed detection of an information threat, monitoring tools are strengthened; and if a crisis reveals weaknesses in a digital service, the relevant processes are reviewed. As a result, each crisis becomes a source of information that enhances the bank's preparedness for future challenges.

This approach makes it possible to view reputational resilience not as a fixed state of the bank but as its capacity to continuously adapt to emerging risks, maintain customer trust, and restore normal interactions following crisis events. The RESILIENCE stage therefore serves as both the concluding and preparatory component of the model, ensuring the transition from analyzing a past crisis to preparing the bank for future ones.

Table 4 presents the main stages of the bank reputation crisis management model and the key actions undertaken at each stage.

Table 4. Bank Reputation Crisis Management Model in the Digital Environment

Stage	Main objective	Key actions
1. PRE-CRISIS	Prevention and preparedness	Monitoring the digital environment; risk identification; forecasting; scenario planning
2. CRISIS	Crisis containment and management	Incident detection; information verification; rapid response; clarification of the situation; customer support
3. POST-CRISIS	Restoration of trust	Analysis of responses; compensatory and corrective actions; restoration of customer trust; assessment of reputational consequences
4. RESILIENCE	Enhancing preparedness for future crises	Analysis of lessons learned; staff training; digital improvements; process adjustments; development of new scenarios

Source: developed by the authors based on [4, 20].

Bank reputation crisis management should be viewed as a continuous cycle rather than as a set of actions undertaken only when a problem arises. The end of the acute phase of a crisis does not signify the end of reputation management efforts. The experience gained should be used to improve digital services, communication practices, monitoring systems, and preparedness for future crises [20]. It is the RESILIENCE stage that transforms crisis experience into a resource for strengthening the bank's reputational resilience.

The analysis of contemporary approaches to crisis management, digital resilience, and the maintenance of banking stability amid wartime risks and digital transformation [15, 20], the potential use of artificial intelligence for detecting digital threats [14], and European requirements for ICT risk management and digital operational resilience [4] made it possible to formulate a comprehensive set of practical recommendations for strengthening the reputational resilience of Ukrainian banks, as systematized in Table 5.

Table 5. Practical Recommendations for Strengthening the Reputational Resilience of Ukrainian Banks

Area	Practical recommendations
Organizational	Establish a cross-functional crisis team comprising representatives of PR, marketing, IT, cybersecurity, and customer support; introduce a unified response protocol for digital crises
Communication	Adhere to the principle of "one problem — one clear explanation"; promptly acknowledge confirmed problems; use clear and accessible language; regularly update information across all digital channels
Technological	Use social listening and AI-based monitoring; automatically detect anomalous spikes in information activity; employ tools for detecting deepfakes and early warning systems for reputational threats
Reputational	Build customer trust before a crisis occurs; demonstrate the bank's reliability through practical actions; ensure transparency and consistency of communication; use lessons learned from crises to improve internal processes
European integration	Align digital resilience management with European approaches; strengthen consumer protection, ICT risk management, and the transparency of digital interactions with customers

Source: developed by the authors based on the research findings.

Effective crisis reputation management requires a shift from responding to individual information incidents toward a continuous system of monitoring, early warning, and preparedness. For Ukrainian banks, such a system should simultaneously account for wartime threats, advances in AI, the digitalization of the customer experience, and gradual alignment with European standards of digital resilience.

Discussion. The findings of this study confirm the need to broaden the traditional approach to bank brand reputation management in the context of digitalization. A reputational crisis in the contemporary banking environment does not necessarily originate directly within the communication domain: its initial source may be an operational failure, a cyber incident, an information attack, fraudulent content, a regulatory issue, or another event that, through digital channels, leads to changes in customers' perceptions of the bank. Reputational risk should therefore be viewed as the outcome of interactions among technological, informational, communication, and behavioral factors.

This conclusion is consistent with the findings of D. Adeabah, C. Andoh, S. Asongu, and A. Gemegah [11], who demonstrate the multidimensional nature of reputational risk in banking. At the same time, the approach proposed in this study extends this perspective by incorporating digital and cyber resilience, crisis response speed, communication adaptability, and digital trust into the crisis management system. This is particularly important for the banking sector because a technical problem can rapidly progress from the operational level to the informational level, subsequently become a reputational issue, and ultimately influence customer behavior.

The findings concerning the importance of response speed are consistent with those of A. D. Beldad, E. van Laar, and S. M. Hegner [2], S. Xu, W. Huang, and L. Weng [6], as well as Y. Kim and Y. Sung [19], who associate the characteristics and timeliness of crisis communication with audience responses and subsequent levels of trust. However, in the digital banking environment, the temporal dimension acquires additional significance. Banks effectively compete not only with alternative interpretations of a crisis event but also with the speed at which user-generated content, media reports, social media posts, algorithmically amplified content, and potential disinformation are disseminated. Therefore, the proposed relationship between the time at which a problem occurs or is detected, the time at which information about the problem gains significant public visibility, and the time of the bank's official response makes it possible to translate the theoretical principle of timely crisis communication into the practical management of digital reputational crises. м

The findings also extend the arguments advanced by A. Siano, A. Vollero, and A. Bertolini [7] and P. Foroudi et al. [9] regarding the shift from controlled brand formation toward its co-creation by multiple actors within the digital environment. For a bank brand, this highlights the limitations of the traditional reputation management model, which is primarily focused on managing the bank's own communication channels. A bank can control the content of its official communications but cannot fully control customer-generated content, publications by the media and bloggers, the operation of digital platform algorithms, or the actions of malicious actors. The concept of the bank digital reputation ecosystem proposed in this study accounts for this multiplicity of actors and channels and shifts the focus from managing individual communications to coordinating the entire system of digital interactions.

An important outcome of the study is the proposed Index of Digital Reputation Resilience (IDRS). Unlike approaches that assess reputation primarily through current brand perceptions, the IDRS is designed to evaluate a bank's ability to maintain and restore trust during digital crises. The integration of the Communication, Trust, Response, Security, and Adaptability components makes it possible to account for the communication, behavioral, managerial, and technological dimensions of reputational resilience. Of particular practical relevance is the possibility of analyzing not only the composite index value but also its individual components, thereby enabling the identification of specific areas of weakness, such as insufficient response speed, deficiencies in digital communication, declining trust, technological vulnerabilities, or limited adaptability.

At the same time, at this stage, the IDRS should be regarded as a conceptual and methodological tool rather than an empirically validated scale. The proposed equal weighting of the five components provides an initial basis for testing the index; however, the actual importance of Communication, Trust, Response, Security, and Adaptability may vary depending on the type of bank, the characteristics of its customer base, its level of digitalization, and the nature of the crisis event. For example, during a cyberattack or a large-scale disruption of digital services, the Security component may potentially have greater importance, whereas during an information attack or the dissemination of false information, Communication, Response, and Trust may carry greater weight. Therefore, the weighting coefficients require further empirical validation.

The proposed cyclical model, PRE-CRISIS → CRISIS → POST-CRISIS → RESILIENCE, extends the process-based approach to crisis management [20] by ensuring that management activities do not end when the active phase of a crisis has been resolved. A distinctive feature of the model is the inclusion of the RESILIENCE stage, during which the lessons learned from a crisis are translated into changes in monitoring procedures, response scenarios, digital infrastructure, communication protocols, and the coordination of responsible units. Thus, a crisis event is viewed not only as a threat to reputation but also as a source of organizational learning that can enhance the bank's preparedness for future crises.

This approach is particularly relevant to the Ukrainian banking system operating under the conditions of the full-scale war. The findings are consistent with the conclusions of V. Apatskyi [1], N. E. Avanesova and I. V. Bakalo [15], and U. Ya. Hrudzevych, O. P. Sidelnyk, and O. V.

Nahorniuk [16] regarding the particular importance of banking sector resilience amid wartime risks. From a reputation management perspective, however, an important finding is that operational resilience acquires a communication dimension: for customers, a bank's ability to maintain access to funds, digital services, and customer support channels becomes direct evidence either confirming or challenging the brand's claimed reliability. This provides grounds for introducing the concept of "reputation through resilience," whereby trust is sustained not only through communication messages but also through the bank's actual performance during crisis events.

The findings regarding the role of artificial intelligence demonstrate its dual significance for crisis management. On the one hand, advances in AI increase the capacity to create deepfakes, synthetic content, automated disinformation, and large-scale fraudulent messaging. On the other hand, AI can be used to monitor the digital environment, detect anomalous changes in the volume and sentiment of mentions, identify potential information attacks, and support the selection of appropriate response scenarios, which is consistent with the general findings of previous studies [3, 14]. At the same time, the analysis indicates that the complete automation of crisis communication would be inappropriate. AI technologies should primarily perform analytical and decision-support functions, while final decisions concerning the bank's public position should remain the responsibility of designated professionals.

The European integration context further enhances the practical relevance of the findings. Requirements concerning digital operational resilience and ICT risk management associated with European approaches and DORA [4] demonstrate the increasing convergence of technological reliability, cybersecurity, and the reputational responsibility of financial institutions. For Ukrainian banks, adaptation to these approaches can be regarded not only as a regulatory task but also as a factor contributing to stronger trust among customers and other stakeholders.

Nevertheless, the study has certain limitations. The proposed IDRS is conceptual in nature and has not yet been tested on an empirical sample of banks, while the weighting coefficients assigned to its components require statistical and expert validation. The system of quantitative indicators for each component also requires further refinement, together with an assessment of their availability and comparability across banks. Furthermore, the specific operating conditions of the Ukrainian banking sector during the full-scale war limit the direct transferability of the proposed framework to banking systems operating in more stable security environments.

Future research should primarily focus on the empirical testing of the IDRS using a sample of Ukrainian banks, determining statistically substantiated weights for its components, and examining changes in the index before, during, and after crisis events. It would also be appropriate to investigate the relationship between IDRS values and indicators of customer behavior, including levels of trust, willingness to recommend the bank, use of digital services, and intentions to switch banks. Another promising research direction is the quantitative assessment of the impact of generative AI, deepfakes, and algorithmic content dissemination on the speed and scale of digital reputational crises.

Conclusions. The study made it possible to substantiate a comprehensive approach to crisis management of bank brand reputation in the digital environment. It was established that a bank's reputational resilience is shaped not only by the quality of its communications but also by the interaction of operational, cyber, informational, communication, regulatory, and AI-related risks. For Ukrainian banks, this approach is particularly relevant in the context of the full-scale war, when cyberattacks, disruptions to the continuity of digital services, information attacks, and fraudulent campaigns directly affect customer trust and perceptions of a banking institution's reliability.

The scientific novelty of the findings lies in developing a comprehensive approach to assessing and managing a bank's digital reputational resilience by integrating its communication, behavioral, managerial, and technological dimensions. The Index of Digital Reputation Resilience (IDRS) is proposed, integrating five components: quality of digital communications (Communication), digital trust (Trust), effectiveness of crisis response (Response), digital and cyber

resilience (Security), and adaptability (Adaptability). The IDRS can be used as a methodological tool for the comprehensive assessment and monitoring of changes in a bank's reputational resilience before, during, and after a crisis, while the analysis of its individual components makes it possible to identify priority areas for managerial intervention. This diagnostic logic constitutes a core feature of the proposed index.

A cyclical model of bank brand reputation crisis management, PRE-CRISIS → CRISIS → POST-CRISIS → RESILIENCE, has been developed, enabling a shift from reactive responses to an already emerging reputational crisis toward continuous management of its entire life cycle. A key element of the model is the RESILIENCE stage, during which lessons learned from crisis experience are used to adjust monitoring procedures, response scenarios, communication protocols, and other components of the management system, thereby providing a basis for enhancing the bank's preparedness for future crises. This function of the RESILIENCE stage is consistent with the logic of the model presented in the main body of the article.

The practical significance of the findings lies in the potential application of the proposed approach by banking institutions to monitor the digital reputational environment, detect potential threats at an early stage, assess preparedness for crisis response, identify weaknesses in individual components of reputational resilience, and improve procedures for restoring trust following crisis events. Of particular importance is the integration of reputation management with digital operational resilience, ICT risk management, cybersecurity, and customer protection in accordance with the European integration trajectory of Ukraine's financial sector.

The development of generative AI further reinforces the need for such an integrated approach. Artificial intelligence simultaneously creates new sources of reputational threats associated with deepfakes, synthetic content, automated disinformation, and bot networks, while expanding opportunities for the early detection of crisis signals and monitoring of the digital environment. Therefore, the use of AI in crisis reputation management should be combined with professional judgment, information verification, and established crisis decision-making procedures.

The limitations of the study are primarily related to the conceptual and methodological nature of the proposed IDRS and the absence, at this stage, of its empirical testing on a sample of banks. The weighting coefficients of the index components and the system of quantitative indicators require further statistical and expert validation. Accordingly, future research should focus on testing the IDRS on a sample of Ukrainian banks, determining empirically substantiated weights for its components, and examining changes in the index before, during, and after crisis events. Another promising research direction is the quantitative assessment of the impact of generative AI, deepfakes, and algorithmic information dissemination on the speed of emergence and scale of reputational crises in the Ukrainian banking sector.

References

1. Apatskyi, V. V. (2026). Ukrainian banks under conditions of war risks, cyber threats and uncertainty. *Journal of Strategic Economic Research*, 2(31), 8–20. DOI: https://doi.org/10.30857/2786-5398.2026.2.1 [in Ukrainian]
2. Beldad, A. D., van Laar, E., & Hegner, S. M. (2018). Should the shady steal thunder? The effects of crisis communication timing, pre-crisis reputation valence, and crisis type on post-crisis organizational trust and purchase intention. *Journal of Contingencies and Crisis Management*, 26, 150–163. DOI: https://doi.org/10.1111/1468-5973.12172
3. Temchenko, Ye. (2025). Artificial intelligence in banking: A comprehensive mapping of applications, challenges, and strategic implications. *Socio-Economic Relations in the Digital Society*, 3(57), 5–18. DOI: https://doi.org/10.55643/ser.3.57.2025.622 [in Ukrainian]
4. Kurii, Y., Susukailo, V., Yerofeieva, A., & Nesteriuk, M. (2025). Analysis of the impact of Digital Operational Resilience Act (DORA) requirements on the process of secure software development. *Cybersecurity: Education, Science, Technique*, 4(28), 400–412. DOI: https://doi.org/10.28925/2663-4023.2025.28.852 [in Ukrainian]
5. Fedevych, L., & Blavt, A. (2022). Implementation of marketing policy of commercial banks using modern social network technologies. *Economy and Society*, (43). DOI: https://doi.org/10.32782/2524-0072/2022-43-23 [in Ukrainian]
6. Xu, S., Huang, W., & Weng, L. (2020). Responding to a health crisis on Facebook: The effects of response timing and message appeal. *Public Relations Review*, 46(3), Article 101909. DOI: https://doi.org/10.1016/j.pubrev.2020.101909
7. Siano, A., Vollero, A., & Bertolini, A. (2022). From brand control to brand co-creation: An integrated framework of brand paradigms and emerging brand perspectives. *Journal of Business Research*, 152, 372–386. DOI: https://doi.org/10.1016/j.jbusres.2022.08.001

8. Foroudi, P., Nazarian, A., Ziyadin, S., Kitchen, P., Hafeez, K., Priporas, C., & Pantano, E. (2020). Co-creating brand image and reputation through stakeholder's social network. *Journal of Business Research*, 114, 42–59. DOI: https://doi.org/10.1016/j.jbusres.2020.03.035
9. Sorokivska, Z. K. (2018). The impact of bank reputational risk on retail banking business. *Uzhorod National University Herald. International Economic Relations and World Economy*, 21(2), 89–93. Retrieved from: http://nbuv.gov.ua/UJRN/Nvuumevcg_2018_21(2)__20 [in Ukrainian]
10. Adeabah, D., Andoh, C., Asongu, S., & Gemegah, A. (2023). Reputational risks in banks: A review of research themes, frameworks, methods, and future research directions. *Journal of Economic Surveys*, 37(2), 321–350. DOI: https://doi.org/10.1111/joes.12506
11. Khrystin, A. I. (2017). Reputational risks of modern Ukrainian banks. *Proceedings of Scientific Works of Cherkasy State Technological University. Series: Economic Sciences*, (47), 98–104. DOI: https://doi.org/10.24025/2306-4420.0.47.2017.119907 [in Ukrainian]
12. Brady, W. J., McLoughlin, K., Doan, T. N., & Crockett, M. J. (2021). How social learning amplifies moral outrage expression in online social networks. *Science Advances*, 7(33), Article eabe5641. DOI: https://doi.org/10.1126/sciadv.abe5641
13. Yakovlev, M., & Liubchak, V. (2025). Artificial intelligence capabilities in detecting and preventing phishing and cyberattacks. *Cybersecurity: Education, Science, Technique*, 1(29), 298–309. DOI: https://doi.org/10.28925/2663-4023.2025.29.840 [in Ukrainian]
14. Avanesova, N. E., & Bakalo, I. V. (2025). Financial stability of the banking system of Ukraine under martial law: Challenges and ways to strengthen it. *Economy and Society*, (73). DOI: https://doi.org/10.32782/2524-0072/2025-73-78 [in Ukrainian]
15. Hrudzevych, U. Ya., Sidelnyk, O. P., & Nahorniuk, O. V. (2023). Problems and directions of development of the banking system of Ukraine under martial law. *Financial Space*, 4(52). DOI: https://doi.org/10.30970/fp.4(52).2023.829394 [in Ukrainian]
16. National Bank of Ukraine. (2025). *Strategy for the development of the financial sector of Ukraine*. Retrieved from: https://bank.gov.ua/ua/about/develop-strategy [in Ukrainian]
17. Hodlevskyi, M. O., & Morozova, N. L. (2025). Features of banking branding in the digital environment. *Business Inform*, (7), 433–440. DOI: https://doi.org/10.32983/2222-4459-2025-7-433-440 [in Ukrainian]
18. Kim, Y., & Sung, Y. (2018). Exploring the relationship between corporate reputation and the public's crisis communication on social media. *Public Relations Review*, 44(1), 56–64. DOI: https://doi.org/10.1016/j.pubrev.2017.12.006
19. Coombs, W. T., & Laufer, D. (2018). Global crisis management – Current research and future directions. *Journal of International Management*, 24(3), 199–203. DOI: https://doi.org/10.1016/j.intman.2017.12.00

Received: 02.04.2026 *Accepted: 13.09.2026*
Received after review: 08.08.2026 *Published: 05.10.2026*

Authors Contribution: *All authors have contributed equally to this work*
Conflict of Interest: *The authors declare no conflict of interest*

Declaration on the use of artificial intelligence

During the preparation of this article, the artificial intelligence tool Grammarly was used to check for grammatical and spelling errors. The concept, content, scientific novelty, and research results belong to the authors. The final version of the article was reviewed, revised, and edited by the authors.

Бабенко Максим
доктор філософії, доцент кафедри менеджменту, обліку та бізнес-комунікацій,
Харківський національний університет імені В.Н. Каразіна,
майдан Свободи, 4, Харків, 61022, Україна
e-mail: babenkomv2011@gmail.com
ORCID ID: 0000-0001-6792-3465
Бітнер Ірина
к.е.н., доцент, доцент кафедри банківського бізнесу та фінансових технологій,
Харківський національний університет імені В. Н. Каразіна,
майдан Свободи, 4, Харків, 61022, Україна
e-mail: irinabitner@karazin.ua
ORCID ID: 0000-0003-0269-5670
Пивавар Ірина
к.е.н., доцент, доцент кафедри державного управління,
публічного адміністрування та економічної політики,
Харківський національний економічний університет імені Семена Кузнеця,
проспект Науки, 9А, Харків, 61166, Україна
e-mail: pivavariv@ukr.net
ORCID ID: 0000-0002-6115-0200
Литвиненко Андрій
к.е.н., доцент, доцент кафедри державного управління,
публічного адміністрування та економічної політики,
Харківський національний економічний університет імені Семена Кузнеця,
проспект Науки, 9А, Харків, 61166, Україна
e-mail: in4.andrey@gmail.com
ORCID ID: 0000-0001-5973-5173

Антикризове управління репутацією бренду банку в епоху цифрових комунікацій

Анотація. Повномасштабна війна, цифровізація та зростання кіберзагроз посилили значення репутаційної стійкості банківського бренду. У дослідженні систематизовано репутаційні ризики, запропоновано індекс цифрової репутаційної стійкості та комплексну модель антикризового управління, орієнтовану на попередження криз, оперативне реагування й відновлення довіри клієнтів. Обґрунтовано комплексний підхід, що поєднує цифровий моніторинг, кризову комунікацію, кіберстійкість, технології штучного інтелекту та адаптацію до європейських вимог.

Постановка проблеми. Попри активну цифровізацію банківських послуг, антикризове управління репутацією банківського бренду залишається недостатньо системним в умовах зростання воєнних, кібернетичних та інформаційних загроз. Традиційні підходи до управління репутацією не повною мірою враховують швидкість поширення інформації в цифровому середовищі, розвиток генеративного штучного інтелекту, необхідність оперативного відновлення довіри клієнтів та посилення вимог до цифрової операційної стійкості в умовах євроінтеграції України.

Нерозв'язані аспекти. Незважаючи на значну кількість досліджень у сфері банківської репутації, кризових комунікацій та цифрової стійкості, недостатньо розробленими залишаються комплексні підходи до антикризового управління репутацією банківського бренду в цифровому середовищі. Подальшого дослідження потребують взаємозв'язки між цифровими та репутаційними ризиками, швидкістю кризового реагування, використанням штучного інтелекту, здатністю банку відновлювати довіру клієнтів та формуванням його репутаційної стійкості.

Мета статті. Метою статті є обґрунтування комплексного підходу до антикризового управління репутацією банківського бренду та підвищення його репутаційної стійкості в умовах цифровізації, воєнних ризиків, розвитку штучного інтелекту та євроінтеграції України.

Основний матеріал. Дослідження ґрунтується на системному, процесному та ризик-орієнтованому підходах до антикризового управління репутацією банківського бренду в цифровому середовищі. У статті досліджено еволюцію банківської репутації в умовах цифровізації, систематизовано основні групи репутаційних ризиків, проаналізовано вплив воєнних загроз, цифрових комунікацій, кіберризиків, генеративного штучного інтелекту та євроінтеграційних процесів на формування довіри клієнтів. Запропоновано авторський Індекс цифрової репутаційної стійкості банку (IDRS), що поєднує якість цифрових комунікацій, рівень довіри, ефективність кризового реагування, цифрову та кіберстійкість і адаптивність банку. Розроблено циклічну модель антикризового управління репутацією, яка охоплює етапи PRE-CRISIS, CRISIS, POST-CRISIS та RESILIENCE, а також сформовано практичні рекомендації щодо підвищення репутаційної стійкості українських банків з урахуванням воєнних викликів, розвитку AI та європейських вимог до цифрової операційної стійкості.

Висновки. Антикризове управління репутацією банківського бренду в цифровому середовищі потребує інтеграції репутаційних, комунікаційних, технологічних і безпекових складових у єдину систему управління. Запропонований Індекс цифрової репутаційної стійкості банку (IDRS) та розроблена модель дають змогу комплексно оцінювати здатність банку протидіяти репутаційним загрозам, підтримувати довіру клієнтів і використовувати кризовий досвід для посилення подальшої стійкості. Для українських банків особливого значення набуває поєднання цифрової надійності, ефективної кризової комунікації, можливостей AI та європейських підходів до цифрової операційної стійкості.

Ключові слова: *антикризове управління, репутація банку, банківський бренд, репутаційна стійкість, цифрові комунікації, репутаційний ризик, цифрова стійкість, штучний інтелект, кіберризики, довіра клієнтів.*

Формули: 1, рис.: 1, табл.: 5, бібл.: 20.

JEL Classification: G21, M31, M15, O33.

Для цитування: Babenko Maksym, Bitner Iryna, Pyvavar Iryna, Lytvynenko Andrii. Crisis management of bank brand reputation in the era of digital communications. Фінансово-кредитні системи: перспективи розвитку. №3(22) 2026. С. 9-30. https://doi.org/10.26565/2786-4995-2026-3-01

Список літератури

1. Апацький В. Українські банки в умовах воєнних ризиків, кіберзагроз та невизначеності // *Журнал стратегічних економічних досліджень*. 2026. № 2 (31). С. 8-20. DOI: https://doi.org/10.30857/2786-5398.2026.2.1.
2. Beldad, A. D., van Laar, E., Hegner, S. M. (2018). Should the shady steal thunder? The effects of crisis communication timing, pre-crisis reputation valence, and crisis type on post-crisis organizational trust and purchase intention. *Journal of Contingencies and Crisis Management*, 26, 150–163. DOI: https://doi.org/10.1111/1468-5973.12172.
3. Темченко Є. Штучний інтелект у банківській справі: комплексне картографування застосувань, викликів і стратегічних наслідків // *Socio-Economic Relations in the Digital Society*. 2025. № 3(57). С. 5–18. DOI: https://doi.org/10.55643/ser.3.57.2025.622.
4. Курій, Є., Сусукайло, В., Єрофеєва, А., & Нестерюк, М. (2025). Аналіз впливу вимог Digital Operational Resilience Act (DORA) на процес безпечної розробки програмного забезпечення. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, *4*(28), 400–412. . DOI: https://doi.org/10.28925/2663-4023.2025.28.852. URL: https://www.csecurity.kubg.edu.ua/index.php/journal/article/view/852/676.
5. Федевич, Л., & Блавт, А. (2022). Реалізація маркетингової політики комерційних банків сучасними технологіями соціальних мереж. *Економіка та суспільство*, 2022. (43). DOI: https://doi.org/10.32782/2524-0072/2022-43-23.
6. Xu S., Huang W., Weng L. (2020). Responding to a health crisis on Facebook: The effects of response timing and message appeal. *Public Relations Review*. Vol. 46, No. 3. Article 101909. DOI: https://doi.org/10.1016/j.pubrev.2020.101909.
7. Siano A., Vollero A., Bertolini A. (2022). From brand control to brand co-creation: An integrated framework of brand paradigms and emerging brand perspectives. *Journal of Business Research*. Vol. 152. P. 372–386. DOI: https://doi.org/10.1016/j.jbusres.2022.08.001.
8. Yuanfang Jiang, Xujun Zheng. Digital media communication, FinTech, and corporate reputation. *Finance Research Letters*. 2026. Vol. 88. Article 109266. DOI: https://doi.org/10.1016/j.frl.2025.109266.
9. Foroudi P., Nazarian A., Ziyadin S., Kitchen P., Hafeez K., Priporas C., Pantano E. (2020). Co-creating brand image and reputation through stakeholder's social network. *Journal of Business Research*. Vol. 114. P. 42–59. DOI: https://doi.org/10.1016/j.jbusres.2020.03.035.
10. Сороківська З. К. (2018). Вплив репутаційного ризику банку на роздрібний банківський бізнес. Науковий вісник Ужгородського національного університету. Серія: Міжнародні економічні відносини та світове господарство. Вип. 21 (2). С. 89–93. URL: http://nbuv.gov.ua/UJRN/Nvuumevcg_2018_21(2)__20.
11. Adeabah D., Andoh C., Asongu S., Gemegah A. (2023). Reputational risks in banks: A review of research themes, frameworks, methods, and future research directions. *Journal of Economic Surveys*. Vol. 37, No. 2. P. 321–350. DOI: https://doi.org/10.1111/joes.12506.
12. Христін А. І. (2017). Репутаційні ризики сучасних банків України. Збірник наукових праць Черкаського державного технологічного університету. Серія: Економічні науки. № 47. С. 98–104. DOI: https://doi.org/10.24025/2306-4420.0.47.2017.119907.
13. Brady W. J., McLoughlin K., Doan T. N., Crockett M. J. (2021). How social learning amplifies moral outrage expression in online social networks. *Science Advances*. Vol. 7, No. 33. Article eabe5641. DOI: https://doi.org/10.1126/sciadv.abe5641.
14. Яковлев М., Любчак В. (2025). Можливості штучного інтелекту у виявленні та запобіганні фішингу й кібератакам. *Кібербезпека: освіта, наука, техніка*. Т. 1, № 29. С. 298–309. DOI: https://doi.org/10.28925/2663-4023.2025.29.840.
15. Аванесова Н. Е., Бакало І. В. (2025). Фінансова стабільність банківської системи України в умовах воєнного стану: виклики та шляхи зміцнення. *Економіка та суспільство*. Вип. 73. DOI: https://doi.org/10.32782/2524-0072/2025-73-78.
16. Грудзевич У. Я., Сідельник О. П., Нагорнюк О. В. (2023). Проблеми та напрями розвитку банківської системи України в умовах воєнного стану. *Фінансовий простір*. № 4 (52). DOI: https://doi.org/10.30970/fp.4(52).2023.829394.
17. Національний банк України. Стратегія розвитку фінансового сектору України. Київ: НБУ. URL: https://bank.gov.ua/ua/about/develop-strategy?utm_source=chatgpt.com.
18. Годлевський М. О., Морозова Н. Л. (2025). Особливості банківського брендингу в цифровому середовищі. *Бізнес Інформ*. № 7. С. 433–440. DOI: https://doi.org/10.32983/2222-4459-2025-7-433-440.
19. Kim Y., Sung Y. (2018). Exploring the relationship between corporate reputation and the public's crisis communication on social media. *Public Relations Review*. Vol. 44, No. 1. P. 56–64. DOI: https://doi.org/10.1016/j.pubrev.2017.12.006.

20. Coombs W. T., Laufer D. (2018). Global Crisis Management – Current Research and Future Directions. *Journal of International Management*. Vol. 24, No. 3. P. 199–203. DOI: https://doi.org/10.1016/j.intman.2017.12.00.

Стаття надійшла до редакції 02.04.2026 *Статтю рекомендовано до друку 13.09.2026*
Стаття надійшла після рецензування 08.08.2026 *Статтю опубліковано 05.10.2026*

Внесок авторів: *всі автори зробили рівний внесок у цю роботу*
Конфлікт інтересів: *автори повідомляють про відсутність конфлікту інтересів*

Декларація про використання штучного інтелекту

Під час підготовки цієї статті було використано інструменти штучного інтелекту Grammarly для перевірки граматичних та орфографічних помилок. Задум, зміст, наукова новизна та результати дослідження належать авторам. Остаточний текст статті був перевірений, опрацьований та відредагований авторами.

Наукове видання

ФІНАНСОВО-КРЕДИТНІ СИСТЕМИ: ПЕРСПЕКТИВИ РОЗВИТКУ

Збірник наукових праць

Випуск 3(22)2026

Українською та англійською мовами

Підписано до друку 05.10.2026. Формат 60x84/8.
Обл.-вид. арк. 37,54. Ум. друк. арк. 30,04. Наклад 100 пр.
Замовлення № 30/26.

Видавець і виготовлювач
Харківський національний університет імені В. Н. Каразіна.
61022, Харків, майдан Свободи, 4, **www.karazin.ua**
Свідоцтво суб'єкта видавничої справи ДК № 3367 від 13.01.09

Видавництво Харківського національного університету імені В. Н. Каразіна