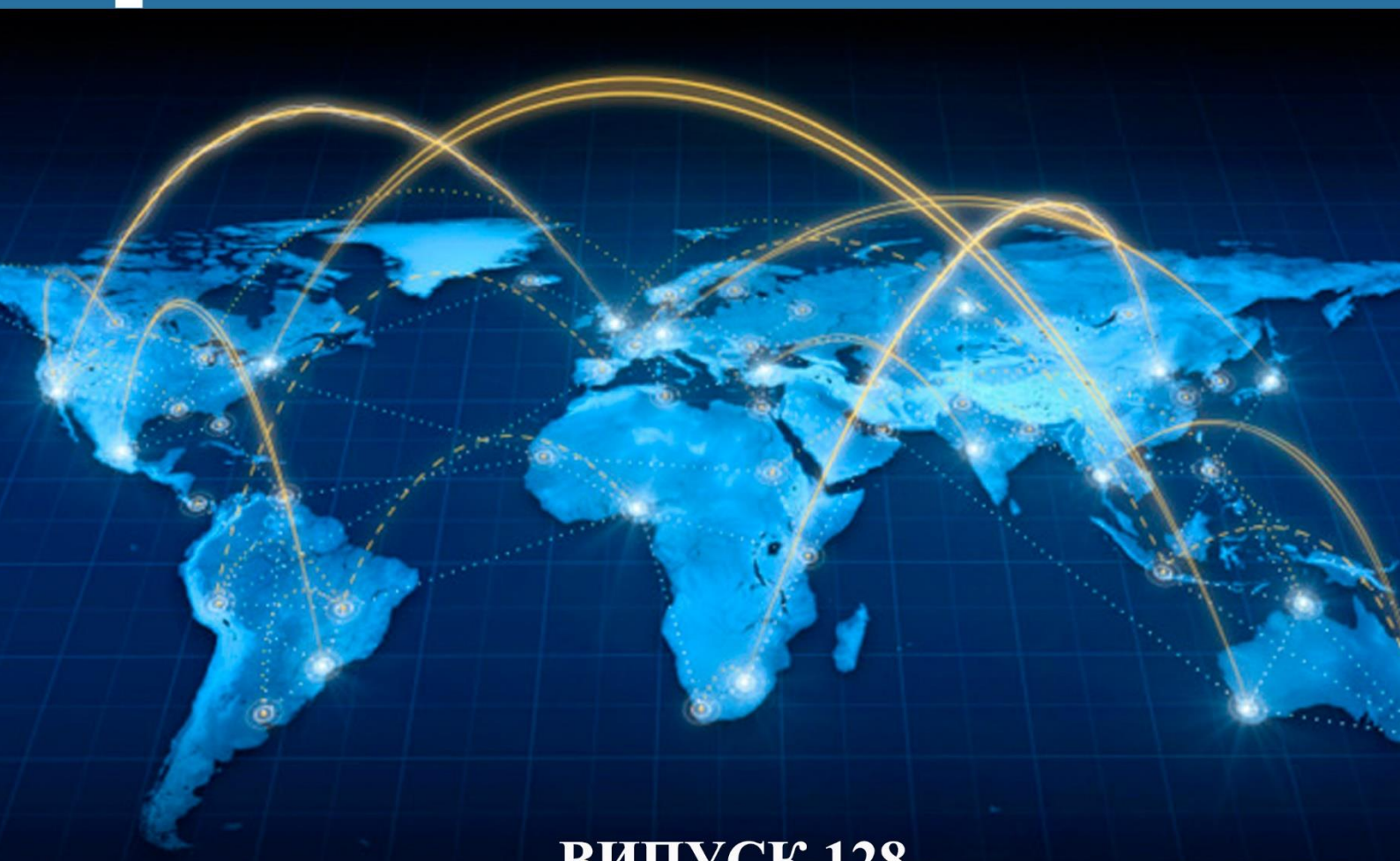
МІЖНАРОДНА НАУКОВО-ПРАКТИЧНА
ІНТЕРНЕТ-КОНФЕРЕНЦІЯ

«ТЕНДЕНЦІЇ ТА ПЕРСПЕКТИВИ РОЗВИТКУ НАУКИ І ОСВІТИ В УМОВАХ ГЛОБАЛІЗАЦІЇ»



ВИПУСК 128

30 квітня 2026 р.

м. Переяслав

УНІВЕРСИТЕТ ГРИГОРІЯ СКОВОРОДИ
В ПЕРЕЯСЛАВІ
РАДА МОЛОДИХ УЧЕНИХ УНІВЕРСИТЕТУ
ГО «ІНСТИТУТ СУСПІЛЬНОГО РОЗВИТКУ
І НАУКОВИХ ДОСЛІДЖЕНЬ»

Матеріали
Міжнародної науково-практичної інтернет-конференції

«ТЕНДЕНЦІЇ ТА ПЕРСПЕКТИВИ РОЗВИТКУ НАУКИ І ОСВІТИ В УМОВАХ ГЛОБАЛІЗАЦІЇ»

30 квітня 2026 року
Вип. 128

Збірник наукових праць

Переяслав – 2026

УДК 001+37(100)
ББК 72.4+74(0)
Т 33

Матеріали Міжнародної науково-практичної інтернет-конференції «Тенденції та перспективи розвитку науки і освіти в умовах глобалізації»: зб. наук. праць. Переяслав, 2026. Вип. 128. 210 с.

ГОЛОВНИЙ РЕДАКТОР:
Кикоть С. М. – кандидат історичних наук, заступник голови ГО «Інститут суспільного розвитку і наукових досліджень»

РЕДАКЦІЙНА КОЛЕГІЯ:
Воловик Л. М. – кандидат географічних наук, доцент
Гузун А. В. – кандидат біологічних наук, доцент
Євтушенко Н. М. – кандидат економічних наук, доцент
Носаченко В. М. – кандидат педагогічних наук, доцент
Руденко О. В. – кандидат психологічних наук, доцент
Садиков А. А. – кандидат фізико-математичних наук, доцент (Казахстан)
Скляренко О. Б. – кандидат філологічних наук, доцент
Халматова Ш. С. – кандидат медичних наук, доцент (Узбекистан)
Юхименко Н. Ф. – кандидат філософських наук, доцент

Збірник матеріалів конференції вміщує результати наукових досліджень наукових співробітників, викладачів вищих навчальних закладів, докторантів, аспірантів, студентів з актуальних проблем гуманітарних, природничих і технічних наук

Відповідальність за грамотність, автентичність цитат, достовірність фактів і посилань несуть автори публікацій

© Університет Григорія Сковороди в Переяславі
© Рада молодих учених університету
© ГО «Інститут суспільного розвитку і наукових досліджень»

ДЖЕРЕЛА ТА ЛІТЕРАТУРА

1. Автономова Н. Інформаційні технології в практиці інформаційно-аналітичної діяльності наукових бібліотек. *Наукові праці Національної бібліотеки України ім. В. І. Вернадського*. 2011. Вип. 30. С. 161–175. URL: http://nbuv.gov.ua/UJRN/npnbuimviv_2011_30_15 (дата звернення 25.04.2026).
2. Бабінська С. Електронний документообіг у процесі ведення бухгалтерського обліку у сучасних умовах. *Наукові записки Національного університету «Острозька академія». Серія: Економіка*. 2023. № 30(58). С. 70–74. DOI: 10.25264/2311-5149-2023-30(58)-70-74 (дата звернення 25.04.2026).
3. Домашенко С. В. Інформаційні технології в управлінні підприємством: електронний документообіг. *Збірник наукових праць ТДАТУ (економічні науки)*. 2013. № 2(3). С. 103–112. URL: http://ear.tsatu.edu.ua/hande/123456789/1849 (дата звернення 25.04.2026).
4. Жежнич П. І. Аналіз сучасних засобів автоматизації роботи з електронною документацією. *Вісник Національного університету «Львівська політехніка»: Комп'ютерні науки та інформаційні технології*. 2012. № 732. С. 395–398. URL: https://science.lpnu.ua/ sites/default/files/journal-paper/2024/feb/33740/vis732komp-nauky-395-398.pdf (дата звернення 25.04.2026).
5. Овсієнко А. С., Дубовчук М. В. Впровадження електронного документообігу в системі управління підприємством. *Економіка. Менеджмент. Бізнес*. 2024. № 1(44). С. 87–93. DOI: 10.31673/2415-8089.2024.010013 (дата звернення 05.04.2026).
6. Орлик О. В. Сучасні тенденції та напрями використання підприємствами інформаційно-комунікаційних технологій. *Вісник соціально-економічних досліджень* (ОНЕУ). 2021. № 2(77). С. 98–110. DOI: 10.33987/vsed.2(77).2021.98-110 (дата звернення 25.04.2026).
7. Система електронного документообігу «M.E.Doc» звітність: посіб. користувача. URL: https://duikt.edu.ua/uploads/l_2061_92994856.pdf (дата звернення 26.04.2026).

Науковий керівник: кандидат історичних наук, доцент Петрович В. В.

УДК 004.056

Pavlo Mushta, Maryna Vyshnevska
(Kyiv, Ukraine)

SECURITY AND USER ADOPTION OF DIGITAL PAYMENT SYSTEMS AND MOBILE WALLETS WITH CONSUMER BEHAVIOR ANALYSIS

This article explores digital payment systems from an information security perspective, focusing on how security mechanisms, perceived risks, and user trust influence adoption behavior. It highlights the role of authentication technologies, privacy protection methods, and human factors in shaping secure usage. The study also discusses emerging threats and future security trends in mobile payment ecosystems.

Keywords: *digital payments, mobile wallets, cybersecurity, information security, data privacy, fraud prevention, perceived risk, mobile payment systems.*

У цій статті досліджуються цифрові платіжні системи з точки зору інформаційної безпеки, зосереджуючись на тому, як механізми безпеки, сприйняті ризики та довіра користувачів впливають на поведінку користувачів. У ній висвітлюється роль технологій автентифікації, методів захисту конфіденційності та людського фактору у формуванні безпечного використання. У дослідженні також обговорюються нові загрози та майбутні тенденції безпеки в екосистемах мобільних платежів.

Ключові слова: *цифрові платежі, мобільні гаманці, кібербезпека, інформаційна безпека, конфіденційність даних, запобігання шахрайству, сприйнятий ризик, мобільні платіжні системи.*

Digital payment systems have become a core part of modern digital infrastructure, replacing many traditional cash-based transactions. Their rapid expansion was especially visible during the COVID-19 pandemic, when contactless and remote payment methods became necessary for safety and convenience. Mobile wallets, QR-code systems, and contactless cards are now widely used across both developed and developing economies, making digital payments a standard component of everyday financial activity.

From an information security perspective, this transformation is not only about convenience but also about the increasing exposure of sensitive financial and personal data. Every digital transaction involves the exchange, storage, and processing of data that can be targeted by cybercriminals. As a result, security and trust have become central factors influencing both system design and user adoption.

Digital payment systems rely on several technologies that aim to protect user data and ensure secure transactions. Mobile wallets typically use encryption, tokenization (replacing sensitive card details with single-use cryptographic tokens), and secure elements within mobile devices to protect payment credentials. QR-code systems, while simple and accessible, introduce risks related to malicious code substitution and phishing attacks if not properly validated. Contactless cards use NFC communication with embedded security protocols, but they are still vulnerable to interception in poorly secured environments. At the more advanced level, biometric authentication methods such as fingerprint and facial recognition are increasingly used to strengthen identity verification and reduce fraud risks.

However, despite these technical protections, security vulnerabilities remain a major concern in mobile payment ecosystems. Attack vectors such as malware on mobile devices, man-in-the-middle attacks, SIM-swapping, and social engineering continue to evolve. According to recent security-focused research, mobile payment platforms remain attractive targets due to the high value of financial data and the increasing dependence on mobile devices for transactions [1]. These threats highlight that technical encryption alone is not sufficient; the entire ecosystem, including user behavior, must be considered in security design.

User adoption of digital payment systems is strongly influenced by perceived security and trustworthiness. Even when systems are technically secure, users may avoid them if they believe they are vulnerable to fraud or data leakage. Research shows that perceived security risk is one of the strongest negative predictors of mobile payment adoption, often outweighing convenience and usability factors [2]. This means that user perception is as important as actual system security.

Beyond technical measures, several behavioral and demographic factors shape adoption. Age plays a critical role: users over 55 years old consistently report higher perceived vulnerability compared to younger cohorts (18–35), often limiting their use to low-value transactions or avoiding mobile wallets entirely. Gender differences also emerge: some studies indicate that female users exhibit stronger privacy concerns and are more likely to abandon a payment app after a single reported security incident. Additionally, financial literacy is positively correlated with secure usage behavior – users who understand basic cryptographic principles (e.g., what end-to-end encryption means) are significantly less likely to fall for phishing scams.

Another powerful driver is social proof. If a user's immediate social circle or local news reports fraud cases involving a specific mobile wallet, trust in that platform drops sharply – often by 50–60% – regardless of whether the platform has already patched the vulnerability. This explains why payment providers increasingly invest in transparent incident communication and bug bounty programs: restoring reputation is harder than building it initially.

Authentication mechanisms play a critical role in reducing these concerns. Multi-factor authentication (MFA), biometric verification, and device-based authentication are widely

implemented to improve security assurance. However, usability challenges sometimes limit their effectiveness, as users may prefer faster but less secure methods (e.g., PIN codes shorter than 6 digits or disabling fingerprint prompts). This creates a trade-off between security strength and user experience, which is a key issue in information security design for mobile financial systems.

Privacy protection is another major aspect of digital payment security. Mobile wallets collect large amounts of sensitive data, including transaction history, location information, and behavioral patterns. If this data is improperly stored or transmitted, it can lead to serious privacy violations. Studies in information systems security emphasize that data minimization, encryption at rest and in transit, and strict access control mechanisms are essential to reduce privacy risks [3].

In addition to technical risks, human factors remain one of the weakest points in security systems. Users often fall victim to phishing attacks, fake payment applications, or social engineering schemes. Even strong encryption cannot prevent attacks if users unknowingly disclose credentials or approve fraudulent transactions. This is why modern security frameworks increasingly focus on user awareness and behavioral security training. Some wallets now include real-time risk warnings - for example, flagging unusually large transactions or suspicious merchant domains before the user confirms payment.

The impact of digital payment security issues on consumer behavior is significant. When users perceive high security risks, they are less likely to adopt mobile wallets or may limit their usage to low-value transactions. Conversely, strong security assurance increases trust and encourages broader adoption. This relationship between perceived security and behavioral intention is widely confirmed in information systems security research [4]. Moreover, actual negative experiences – such as unauthorized transactions or account lockouts – reduce adoption rates for up to 12 months, even after the issue is resolved.

Regulatory frameworks also shape security outcomes. The European PSD2 directive, which mandates Strong Customer Authentication (SCA), has reduced unauthorized transaction fraud by approximately 35–40% across the EU. In contrast, jurisdictions with delayed or fragmented regulations (parts of Southeast Asia and Africa) see higher rates of merchant gateway spoofing and SIM-swap attacks. Thus, legal enforcement of security standards is as important as technical design.

Despite these challenges, the security architecture of digital payment systems continues to evolve. Zero-trust security models, real-time fraud detection using machine learning, and behavioral biometric authentication (e.g., analyzing typing speed, device tilt, or touch pressure) are emerging trends that aim to strengthen protection against advanced cyber threats. These technologies analyze user behavior patterns to detect anomalies and prevent unauthorized access before transactions are completed.

Looking forward, the integration of digital payments with broader cyber-physical systems, such as Internet of Things (IoT) devices and smart environments, will further increase the importance of robust security frameworks. As payment systems become more embedded in daily life, the attack surface expands, requiring continuous adaptation of security mechanisms. Central Bank Digital Currencies (CBDCs) will also introduce new security challenges, particularly in terms of scalability, identity management, and systemic risk protection [5].

In conclusion, digital payment systems represent not only a financial innovation but also a complex information security challenge. While they offer significant benefits in terms of convenience and efficiency, their widespread adoption depends heavily on the ability to ensure data security, privacy protection, and fraud resistance. Strengthening technical safeguards, improving authentication systems, addressing demographic and social factors, and increasing user awareness are all essential steps toward building secure and trustworthy digital payment ecosystems.

REFERENCES

1. Tian Y., Chan T. J. Predictors of mobile payment adoption: Trust, perceived usefulness, and behavioral intention. *SAGE Open.* 2024. Vol. 14, No. 3. Article 21582440241292525. DOI: 10.1177/21582440241292525.
2. Alamleh H., AlQahtani A. A. S., Al Smadi B. Secure mobile payment architecture enabling multi-factor authentication. *arXiv preprint.* 2023. Article arXiv:2304.09468. DOI: 10.48550/arXiv.2304.09468.
3. Changchit C., Klaus T., Lonkani R., Sampet J. Determinants of mobile payment adoption: Evidence from perceived risk factors. *Journal of Risk and Financial Management.* 2024. Vol. 17, No.8. Article 315. DOI: 10.3390/jrfm17080315.
4. Shaikh A., Glavee-Geo R., Karjaluoto H., Hinson R. Mobile money as a driver of digital financial inclusion. *Technological Forecasting and Social Change.* 2023. Vol. 186. Article 122158. DOI: 10.1016/j.techfore.2022.122158.
5. Bojjagani S., Sastry V. N., Chen C.-M., Kumari S., Khan M. Systematic survey of mobile payments, protocols, and security infrastructure. *Journal of Ambient Intelligence and Humanized Computing.* 2021. P. 1–27. DOI: 10.1007/s12652-021-03134-0.

УДК 004.8:004.382:004.891

Anastasiia Serytsan
(Kyiv, Ukraine)

LARGE LANGUAGE MODEL HALUCINATION DETECTION METHOD BASED ON ANOMALY ANALYSIS OF HIDDEN STATES IN GEOSPATIAL SEARCH TASK

With the rapid development of large language models, it has become clear that they all share a critical vulnerability known as hallucinations. Therefore, the development of methods for hallucination detection is of great importance. This article presents a method for hallucination detection based on the analysis of a model's hidden states. It explores the use of the Mahalanobis distance as a tool for anomaly detection in hidden states and a Gaussian Mixture Model for threshold selection in unsupervised scenarios. The proposed method is evaluated on a language model specifically trained for a geospatial search task.

Key words: *hallucinations, language models, hidden states, Mahalanobis distance, Gaussian Mixture Model, anomaly detection.*

Зі стрімким розвитком великих мовних моделей стало очевидно, що всі вони мають критичну вразливість, відому як галюцинації. Тому розробка методів виявлення галюцинацій є надзвичайно важливою. У цій статті представлено метод виявлення галюцинацій, що ґрунтується на аналізі прихованих станів моделі. Розглядається використання відстані Махаланобіса як інструменту для виявлення аномалій у прихованих станах, а також Гаусівської Сумішевої Моделі для визначення порогу в сценаріях без міток. Запропонований метод оцінюється на мовній моделі, спеціально навченій для задачі геопросторового пошуку.

Ключові слова: *галюцинації, мовні моделі, приховані стани, відстань Махаланобіса, Гаусівська Сумішева Модель, виявлення аномалій.*

Large language models (LLMs) have demonstrated strong performance across a wide range of natural language processing tasks. However, hallucinations, that is factually incorrect yet plausible outputs, remain a major challenge [1]. This issue becomes particularly critical in geospatial applications, where even small numerical errors can lead to substantial real-world deviations.