УДК 004.056.5

V. M. Horkovliuk
V. V. Chopliak

PERSONAL DATA PROTECTION IN THE DIGITAL AGE: CHALLENGES AND SOLUTIONS

Vinnytsia National Technical University

Анотація

У роботі розглянуто сучасні загрози захисту персональних даних в умовах цифрової трансформації. Проаналізовано нормативно-правові механізми регулювання у сфері захисту даних. Запропоновано комплексний підхід до підвищення рівня кібербезпеки на технічному, правовому та освітньому рівнях.

Ключові слова: персональні дані, кібербезпека, витік даних, GDPR, шифрування, цифрова грамотність.

Abstract

The paper examines contemporary threats to personal data protection in the context of digital transformation. Legal and regulatory mechanisms for data protection are analyzed. A comprehensive approach to improving cybersecurity at the technical, legislative, and educational levels is proposed.

Keywords: personal data, cybersecurity, data breach, GDPR, encryption, digital literacy.

Introduction

The rapid expansion of digital technologies has fundamentally transformed how personal information is collected, stored, and processed. Social media platforms, e-commerce services, healthcare systems, and financial institutions handle vast volumes of sensitive user data on a daily basis. As a result, personal data has become one of the most valuable assets in the modern economy, and simultaneously, one of the most targeted resources in cyberspace. According to IBM's Cost of a Data Breach Report 2023, the global average cost of a single data breach reached $4.45 million, the highest figure ever recorded [1]. This alarming trend underscores the urgent need for robust and comprehensive personal data protection strategies.

Main part

Personal data breaches occur as a result of various attack vectors, including phishing, ransomware, credential stuffing, and insider threats. Phishing remains the leading cause of data compromise globally: the Anti-Phishing Working Group (APWG) reported over 4.7 million phishing attacks in 2022 alone, representing a 150% increase compared to 2020 [2]. These attacks exploit human vulnerability rather than technical flaws, which highlights a critical weakness in the current security landscape – the human factor.

On the legislative front, the General Data Protection Regulation (GDPR), enforced by the European Union since 2018, represents the most comprehensive framework for personal data protection to date. It establishes strict requirements for data collection, processing, and storage, mandates informed user consent, and introduces significant financial penalties for non-compliance – up to €20 million or 4% of annual global turnover [3]. However, the enforcement of GDPR across different jurisdictions remains inconsistent, and many countries still lack equivalent national legislation, leaving millions of users inadequately protected.

From a technical perspective, several proven solutions exist to safeguard personal data. End-to-end encryption using standards such as AES-256 ensures that data remains unreadable to unauthorized parties during transmission and storage. Multi-factor authentication (MFA) significantly reduces the risk of account compromise by requiring users to verify their identity through multiple channels. The Zero Trust security model, formalized by the National Institute of Standards and Technology (NIST) in Special Publication 800-207, proposes that no entity – internal or external – should be automatically trusted, and that access must be continuously verified and granted on a least-privilege basis [4]. These technologies, when implemented together, substantially reduce the attack surface for malicious actors.

Despite the availability of technical and legal tools, studies consistently identify human behavior as the weakest link in data security. Research published by Stanford University found that approximately 88% of all data breaches are caused, at least in part, by employee error [5]. This finding emphasizes that cybersecurity awareness and digital literacy programs are not supplementary measures – they are essential components of any effective data protection strategy. Organizations must invest in regular security training, simulated phishing exercises, and clear internal data-handling policies.

Conclusions

Personal data protection in the digital age is a multidimensional challenge that cannot be addressed by a single solution. Effective defence requires the convergence of three equally important pillars: strong legislative frameworks such as GDPR that establish clear accountability; advanced technical measures including encryption, MFA, and Zero Trust architecture; and continuous investment in human-centered cybersecurity education. Future research should focus on the application of artificial intelligence for real-time anomaly detection in data flows, as well as the development of globally harmonized data protection standards.

REFERENCES

1. IBM Security. Cost of a Data Breach Report 2023. IBM Corporation, 2023. 64 p.
2. Anti-Phishing Working Group (APWG). Phishing Activity Trends Report, Annual Report 2022. APWG, 2023. 20 p.
3. European Parliament and of the Council. Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data (GDPR). Official Journal of the European Union, 2016.
4. NIST Special Publication 800-207. Zero Trust Architecture. National Institute of Standards and Technology, 2020. 50 p.
5. Tessian Research. The Psychology of Human Error. Stanford University – Tessian, 2022. 30 p.
6. Nykyporets, S. S., & Hadaichuk, N. M. (2025). Foreign language media literacy as a protective factor against AI-generated disinformation and psychological stress in technical higher education in Ukraine. In *Transformational vectors of public administration, law, and humanities in the development of the modern educational system: Scientific monograph* (pp. 305-330). Baltija Publishing. https://doi.org/10.30525/978-9934-26-647-8-14.
7. Nykyporets, S. S., Herasymenko, N. V., & Chopliak, V. V. (2025). Developing digital language competence as a factor of competitiveness of future master's degree holders in power engineering in the digital economy. In O. H. Cherep (Ed.), *Artificial intelligence as a tool to protect the economy disinformation: Innovative solutions and international practices: Collective monograph* (pp. 140-193). Baltija Publishing. DOI: https://doi.org/10.30525/978-9934-26-586-0.
8. Nykyporets, S. S., & Kukharchuk, H. V. (2025). Intercultural communication in information security: Risks, conflicts, and educational opportunities for English language teachers. In *International security studies: Managerial, technical, legal, environmental, informative and psychological aspects* (Vol. II, pp. 398-420). ISAP, Research and Education. DOI: https://doi.org/10.5281/zenodo.15356424.
9. Ibrahimova, L. V., & Nykyporets, S. S. (2025). Information security in the global context: Linguistic perspectives and the role of English. In *International security studies: Managerial, technical, legal, environmental, informative and psychological aspects* (Vol. II, pp. 321-345). ISAP, Research and Education. DOI: https://doi.org/10.5281/zenodo.15356365.

Горковлюк Вадим Миколайович, студент групи 1БС-24б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, м. Вінниця; e-mail: vadikcoin94@gmail.com.

Науковий керівник: **Чопляк Вікторія Володимирівна** викладач англійської мови, кафедра іноземних мов, Вінницький національтий технічний університет, м. Вінниця, e-mail: nikavnuchkova@gmail.com.

Horkovliuk Vadym Mykolaiovych, student of group 1SS-24b, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University,. Vinnytsia; e-mail: vadikcoin94@gmail.com.

Academic supervisor: **Viktoriya V. Chopliak**, English teacher of the Department of Foreign Languages, Vinnytsia National Technical University,. Vinnytsia, e-mail: nikavnuchkova@gmail.com.