UDC 004.056.011

I.S. KOT

S.O. KOT

CYBERSECURITY: A NEW DIMENSION OF NATIONAL INDEPENDENCE

Vinnytsia National Technical University

Анотація

У статті розкрито роль кібербезпеки як фундаментального складника сучасного державного суверенітету. Проаналізовано вплив цифрової стійкості на захист критичної інфраструктури, інформаційну цілісність та економічну самостійність країни. Обґрунтовано, що в умовах гібридних загроз здатність держави ефективно протидіяти кібератакам є вирішальним чинником збереження її політичної незалежності та національної безпеки.

Ключові слова: кібербезпека, державний суверенітет, національна безпека, критична інфраструктура, цифрова стійкість, інформаційна війна, гібридні загрози, незалежність держави.

Abstract

This article explores the role of cybersecurity as a fundamental component of modern state sovereignty. It analyzes the impact of digital resilience on the protection of critical infrastructure, information integrity, and a country's economic independence. It is argued that, in the context of hybrid threats, a state's ability to effectively counter cyberattacks is a decisive factor in preserving its political independence and national security.

Keywords: cybersecurity, state sovereignty, national security, critical infrastructure, digital resilience, information warfare, hybrid threats, state independence.

Introduction

Historically, a state's independence was defined by its ability to defend its land, sea, and air borders. However, in the 21st century, a fourth domain of conflict has emerged: cyberspace. Today, national sovereignty is impossible without digital resilience. Cybersecurity is no longer a narrowly specialized IT topic but has become one of the key factors in the survival and autonomy of any modern country.

The Digital State — Digital Risks

Ukraine and the world are rapidly becoming digitized. Government services, the financial sector, the energy industry, and healthcare are moving to the cloud. This makes life more convenient for citizens, but at the same time creates new vulnerabilities. When all critical infrastructure is controlled by software, a successful cyberattack can be more devastating than a physical attack [1].

Imagine a situation where a hostile state gains control over a country's power grid or water supply. Without firing a single shot, they could shut down factories, leave cities without power, and sow chaos. In such a scenario, political independence becomes a mere formality, as real control over the nation's lifeline passes to the aggressor. Therefore, creating a reliable "cyber shield" is not just a matter of technology; it is a matter of preserving the people's right to make their own decisions.

Information Warfare and Manipulation of Public Opinion

A nation's independence is founded on social unity and trust in state institutions. Cybersecurity involves not only protecting code but also countering disinformation and cognitive attacks. Social media has become a battleground for influence operations, where malicious actors use algorithms to fuel internal conflicts.

If a state is unable to protect its information space from manipulation, it loses its intellectual independence. Citizens whose opinions are shaped by hostile bot farms may unconsciously act against their own country's interests [2]. Thus, digital hygiene and data security become tools for protecting democratic choice and national identity.

The Economic Dimension of Sovereignty

Economic self-sufficiency is another pillar of independence. In a world where intellectual property is more valuable than raw materials, cyber espionage poses a massive threat. The theft of military technology, classified research, or banking data can set a country's development back by decades [5].

Moreover, cybersecurity is key to investment attractiveness. No investor will put money into the economy of a country where the banking system is vulnerable to hacks and corporate data is unprotected. By building a robust cybersecurity sector, the state creates a secure environment for innovation, which is the foundation of true economic independence.

Cyber Resilience as an Element of Defense

Modern warfare is hybrid warfare. Every military operation today is accompanied by cyberattacks on communication systems, troop command and control, and logistics. A state without its own "cyber front line" becomes "blind" and "deaf" on the battlefield.

Experience in recent years shows that the ability to quickly repel digital attacks and restore system operations is key to maintaining defense capabilities [6]. Cybersecurity allows a state to maintain control during the most critical moments, which is a critical factor in the struggle for territorial integrity.

The Path to Digital Independence

For cybersecurity to truly become a guarantor of independence, the state must implement several strategic steps:

1. Domestic technological infrastructure: Reducing dependence on foreign (especially potentially hostile) software and hardware.

2. Education and Human Resources: Investing in the training of specialists capable not only of using off-the-shelf solutions but also of creating new security algorithms.

3. International cooperation: Cyberspace has no borders, so collective security with allies is vital.

4. Public-private partnership: Combining the efforts of government agencies and the IT industry to create the most effective monitoring and response systems.

Conclusions

In summary, cybersecurity is the invisible yet fundamental framework upon which the structure of the modern state rests. In a world where data has become the "new oil" and algorithms have become weapons, independence can no longer be defended with tanks and missiles alone. It is defended through cryptography, intrusion detection systems, and a high level of digital literacy among the population.

Only a state that controls its own digital space can consider itself truly free and sovereign. Cybersecurity is an investment in the future, where freedom of choice is guaranteed not only by laws but also by the resilience of digital systems.

REFERENCES

1. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 23.03.2026).

2. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26.08.2021 р. № 447/2021. URL: https://www.president.gov.ua/documents/4472021-39745 (дата звернення: 23.03.2026).

3. Гнатюк С. О., Юдін О. К., Корченко О. О. Захист критичної інформаційної інфраструктури : підручник. Київ : НАУ, 2022. 340 с.

4. Дубов Д. В. Кіберпростір як новий об'єкт державної політики національної безпеки : монографія. Київ : НІСД, 2010. 190 с.

5. Кириченко О. А. Роль кібербезпеки у забезпеченні національного суверенітету в умовах гібридної війни. *Юридичний часопис*. 2023. № 2. С. 45–52.

6. Національна стійкість у цифровому світі: виклики та рішення для України : аналітична доповідь / за ред. О. М. Суходолі. Київ : НІСД, 2024. 88 с.

7. Global Cybersecurity Index 2024. International Telecommunication Union (ITU). URL: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx (дата звернення: 23.03.2026).

8. Шевченко В. П. Інформаційна безпека держави в епоху цифровізації: правовий аспект. *Наукові записки НаУКМА. Юридичні науки*. 2025. Т. 12. С. 110–118.

Кот Іларія Сергіївна – студентка групи 1ЕХКБ-25б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e–mail: ilaria_cat@icloud.com.

Кот Сергій Олександрович – к.філ.н., доцент кафедри Іноземних мов, Вінницький національний технічний університет, м. Вінниця, e-mail: kot.sergii@vntu.edu.ua

Ilariia S. Kot – 1EHC-25b group student, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: ilaria_cat@icloud.com.

Sergii O. Kot – *PhD,* Associate Professor in the Department of Foreign Languages at Vinnytsia National Technical University, Vinnytsia, e-mail: kot.sergii@vntu.edu.ua