UDC 811.111:81'276.6:35
DOI https://doi.org/10.32782/tps2663-4880/2025.42.1.19

VOCABULARY OF CYBERSECURITY IN THE CONTEXT OF ENSURING NATIONAL SECURITY

ЛЕКСИКА КІБЕРБЕЗПЕКИ В КОНТЕКСТІ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Zaiats L.I.,
orcid.org/0000-0003-1751-1301
Candidate of Pedagogical Sciences,
Associate Professor at the Department of Romance and Germanic Languages
National Academy of Security Service of Ukraine

In the digital age, evolving cyber threats demand precise communication, yet inconsistent cybersecurity vocabulary across disciplines and documents hinders effective coordination and public understanding. This paper analyzes the linguistic features of cybersecurity vocabulary and its role in national security communication. The aim of this study is to analyze the vocabulary of cybersecurity within the context of national security, focusing on its semantic typology, word-building patterns, etymological origins, and functioning as international vocabulary.

It was revealed that cybersecurity is currently one of the key elements of national security, as it protects critical societal and governmental interests in the digital realm. It includes diverse practices aimed at defending networks, information, and infrastructure from cyber threats and unauthorized access. Defined by both national legislation and international bodies, cybersecurity comprises technologies, regulations, and coordinated actions to prevent and respond to cyberattacks, thus contributing to global stability and the advancement of the information society.

An examination of cybersecurity vocabulary reveals the main semantic groups that include "security concepts and principles," "threats and attack types," "cryptography and data protection," "tools, technologies, and defenses," "incidents and responses," "policy, compliance, and governance," and "infrastructure and environment". Such vocabulary organization reflects the multifaceted nature of cybersecurity vocabulary and its significance for both technical and regulatory fields of national security. In terms of word formation, cybersecurity vocabulary follows common patterns of specialized vocabulary: many units derive from Latin and Greek roots, lending them scientific precision and international recognition; others are created through compounding, blending, abbreviations, initialisms, and semantic shifts, with some originating from personal or geographical names. A significant share of the vocabulary comprises internationalisms – lexical units adopted with minimal or no change across different languages – including both direct and partial internationalisms, depending on the linguistic context. Conversely, some culturally specific or informal expressions remain localized, often either being translated or keeping their English form in the texts in other languages. As such, cybersecurity vocabulary forms a dynamic and globally significant part of national security vocabulary, characterized by conceptual consistency, lexical productivity, and growing international integration, which supports efficient communication and cooperation in combating cyber threats.

Key words: national security, cybersecurity, cybersecurity vocabulary, semantic groups, word formation, internationalisms, information society.

У сучасну цифрову епоху постійний розвиток кіберзагроз вимагає точної комунікації, проте неузгоджена система лексики сфери кібербезпеки в різних дисциплінах та документах перешкоджає ефективній координації та суспільному розумінню. У цій статті аналізуються лінгвістичні особливості лексики кібербезпеки та її роль у комунікації з питань національної безпеки. Метою цього дослідження є аналіз лексики кібербезпеки в контексті національної безпеки, що зосереджується на її семантичній типології, моделях словотворення, етимології та функціонуванні в якості інтернаціональної лексики.

Виявлено, що кібербезпека наразі є одним із ключових елементів національної безпеки, оскільки вона захищає критично важливі суспільні та урядові інтереси в цифровій сфері. Вона включає різноманітні практики, спрямовані на захист мереж, інформації та інфраструктури від кіберзагроз та несанкціонованого доступу. За визначенням як національного законодавства, так і міжнародних організацій, кібербезпека охоплює технології, нормативні акти та скоординовані дії для запобігання кібератакам та реагування на них, тим самим сприяючи глобальній стабільності та розвитку інформаційного суспільства.

Аналіз лексики кібербезпеки дозволив виявити основні семантичні групи, які включають «концепції та принципи безпеки», «типи загроз та атак», «криптографію та захист даних», «інструменти, технології та засоби захисту», «інциденти та реагування», «політику, відповідність та управління» й «інфраструктуру та середовище». Така організація лексичної системи відображає багатогранний характер лексики кібербезпеки та її значення як для технічної, так і для регуляторної сфер національної безпеки. З точки зору творення одиниць лексика кібербезпеки дотримується загальних моделей творення спеціалізованої лексики: багато лексичних одиниць походять від латинського та грецького коріння, що надає їм наукової точності та міжнародного визнання; інші створені шляхом слововкладання, контамінації, ініціалізації, абревіації та семантичних зрушень, причому деякі лексичні одиниці походять від власних імен або географічних назв. Значну частку цієї лексики запасу складають інтернаціоналізми – лексичні одиниці, що застосовуються з мінімальними змінами або без змін у різних мовах, включаючи як прямі, так і часткові інтернаціоналізми, залежно від лінгвістичного контексту. І навпаки, деякі культурно специфічні або неформальні вирази залишаються локалізованими, часто зазнаючи перекладу або зберігаючи свою англійську форму в документах

іншими мовами. Таким чином, лексика сфери кібербезпеки утворює динамічну та глобально значущу частину лексики національної безпеки, характеризується концептуальною узгодженістю, лексичною продуктивністю та зростаючою міжнародною інтеграцією, що підтримує ефективну комунікацію та співпрацю у боротьбі з кіберзагрозами.

Ключові слова: національна безпека, кібербезпека, лексика кібербезпеки, семантичні групи, словотвір, інтернаціоналізми, інформаційне суспільство.

Problem statement. In the digital age, the rapid development of information and communication technologies has led to the emergence of new threats to national security, particularly in the cyberspace domain. Governments and institutions worldwide increasingly rely on precise communication to coordinate cybersecurity efforts, legislate protections, and respond to cyber incidents. Cybersecurity intersects with multiple disciplines, including information technology, law, defense, and linguistics. However, despite growing interest in cybersecurity, linguistic analysis of the domain-specific vocabulary used in national security contexts remains limited. This leads to inconsistencies in vocabulary usage across official documents, legal frameworks, and expert discourse. As a result, communication between security agencies, policymakers, and the public may become unclear or ambiguous, reducing the effectiveness of cybersecurity strategies. This linguistic instability undermines the effectiveness of national cybersecurity frameworks and complicates the dissemination of information to non-specialist audiences. This paper aims to analyze the linguistic characteristics of cybersecurity vocabulary and its functional role in national security communication.

Analysis of recent research and publications. The vocabulary of cybersecurity is an integral component of national security vocabulary which was the object of the researches by such scholars as L. I. Zaiats [1], D. Blagojević [2], S. Mijalković [2]. Securing computer systems and applications is the goal of cybersecurity as a new interdisciplinary field of knowledge, which requires a special versatile study of its vocabulary. This task is caused by the need of the time, since the development of this field has rapid pace. Due to its social significance, the field of cybersecurity has become one of the priority objects of the governments' activity and the object of linguistic scientific research [3, p. 79]. The previous researches on the issue concerned the definition of cybersecurity [4; 5], specifics of cybersecurity as an activity [5; 8], structural peculiarities of English cybersecurity terms [3]. However, these is a need to determine the specifics of cybersecurity vocabulary within national security one.

The aim of this study is to analyze the vocabulary of cybersecurity within the context of national security, focusing on its semantic classification, word-building patterns, etymological origins, and functioning as internationalisms. The study highlights how cybersecurity vocabulary form a shared global vocabulary that supports international cooperation and effective communication in the domain of national security.

Presentation of the main material. The sphere of national security encompasses the protection of society (regardless of the ethnic, ethical, racial or ideological affiliation of its members) and the state, as well as their participation in international and global security. It includes ensuring protection of their essential interests and values through coordinated efforts of both the military and civilian sectors, as well as state and non-state structures in the national security system. This system also relies on numerous international (both governmental and non-governmental) organizations to facilitate various aspects of international security cooperation. All the levels of security – individuals, societies, states and the world community – are involved in the protection of national security [2, p. 52]. Special vocabulary of the national security sphere is understood as words or phrases that denote the concepts of the sphere of special knowledge in the field of society security and state security, their participation in international and global security, are intelligible for specialists in the field of national security, stable, reproducible elements in this system, occupying certain classification places in it [1, p. 243].

With the increasing number of attacks, cybersecurity is becoming essential component of global stability requiring international cooperation, strategic investments and collective efforts to combat these threats [4, p. 251]. Hence, cybersecurity is one of the rapidly evolving policy areas of global data governance, and the international community is increasingly realizing that cyberspace goes far beyond the technical aspects of network and data security, and includes national and economic security [7, p. 62].

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) defines cybersecurity as protecting networks, devices, and data from unauthorized access and ensuring the confidentiality, integrity, and availability of information, which includes technologies, practices, and policies aimed at preventing cyberattacks and protecting computer systems, applications, data, financial assets, and people from threats such as ransomware, malware, phishing, and data theft [5]. In the Law "On the Basic Principles of Ensuring

Cybersecurity of Ukraine", the term "cybersecurity" is used in the following meaning: "the protection of the vital interests of a person and a citizen, society and the state when using cyberspace, which ensures the sustainable development of the information society and the digital communication environment, timely detection, prevention and neutralization of real and potential threats to the national security of Ukraine in cyberspace" [8].

Cybersecurity has many international and transnational elements and is not easily divided into "domestic", "national" or "in-state" on either side of the Atlantic, however over time cybercrime has become less important on both sides of the Atlantic as the external or international dimensions of cyberspace have become increasingly important, for example, the use of cyberwarfare in Ukraine and Chinese surveillance and disinformation [6, p. 1090].

Thus, the vocabulary of cybersecurity occupies a crucial and rapidly expanding place within the broader framework of national security vocabulary. As digital technologies increasingly underpin critical infrastructure, defense systems, and governmental operations, cybersecurity has become an integral component of national security discourse. The specialized vocabulary associated with cybersecurity – encompassing lexical units related to threats, vulnerabilities, protocols, and response mechanisms – not only reflects technical realities but also shapes policy, legislation, and inter-agency communication. Its integration into national security vocabulary ensures precise articulation of cyber-related risks and strategies, enabling more effective coordination between security sectors.

Respectively, cybersecurity vocabulary encompasses the concept related to several spheres also relevant for national security. In particular, the analysis of short "Cybersecurity glossary" [9] allows distinguishing the following semantic groups of cybersecurity lexical units:

1) security concepts and principles, such as *access control mechanism* "security measures designed to detect and deny unauthorised access and permit authorised access to an information system or a physical facility" [9, p. 2]; *data integrity* "data that is complete, intact, and trusted and has not been modified or destroyed in an unauthorised or accidental manner" [9, p. 3];

2) threats and attack types, in particular, *adversary* "an individual, group, organisation, or government that conducts (or intends to conduct) detrimental activities" [9, p. 2]; *man-in-the-middle (MITM) attack* "when a hacker intercepts communication between two (or more) parties and relays the information to both sides" [9, p. 5];

3) cryptography and data protection, such as *cryptanalysis* "the operations performed in defeating or circumventing cryptographic protection of information by applying mathematical techniques" [9, p. 2]; *symmetric key* "a cryptographic key that is used to perform both the cryptographic operation and its inverse, for example to encrypt plaintext and decrypt ciphertext, or create a message authentication code and to verify the code" [9, p. 7];

4) tools, technologies, and defenses, for example, *keylogger* "software or hardware that tracks keystrokes and keyboard events to monitor actions by the user of an information system" [9, p. 5]; *whitelist* "a list of entities that are considered trustworthy and are granted access or privileges" [9, p. 8];

5) incidents and responses, such as *incident response plan* "a set of predetermined and documented procedures to detect and respond to a cyber incident" [9, p. 4]; *recovery* "the activities after an incident or event to restore essential services and operations in the short and medium term, and fully restore all capabilities in the longer term" [p. 6];

6) policy, compliance, and governance, for example, *information security policy* "regulations, rules, and practices that prescribe how an organization manages, protects, and distributes information" [9, p. 4]; *risk assessment* "the product or process that collects information and assigns values to risks for informing priorities, developing or comparing courses of action, and informing decision making" [9, p. 6];

7) infrastructure and environment including *cyber ecosystem* "the interconnected information infrastructure of interactions among persons, processes, data, and information and communications technologies, along with the environment and conditions that influence those interactions" [9, p. 2]; *network resilience* "the ability of a network to: provide continuous operation (i.e., highly resistant to disruption and able to operate in a degraded mode if damaged); recover effectively if failure does occur; and scale to meet rapid or unpredictable demands" [9, p. 5].

The lexical units of the cybersecurity sector are formed according to the patterns typical for specialized vocabulary in general. In particular, cybersecurity vocabulary includes numerous units of Latin origin, such as *authentication* (Latin *authenticus* "genuine, authoritative, real" [10]), *confidentiality* (Latin *confidentia* "trust, confidence, faith" [10]), *integrity* (Latin *integritas* "wholeness, purity, uprightness, honesty" [10]), *privacy* (Latin *privatus* "personal, not public, restricted" [10]), *signature* (Latin *signum* "a mark or sign of approval" [10]).

Also, cybersecurity vocabulary includes numerous units of Greek origin, such as *cryptography* (Greek *kryptos* "hidden" + *graphein* "to write"

[10]), *cryptology* (Greek *kryptos* "hidden" + *logos* "study" [10]), *cryptanalysis* (Greek *kryptos* "hidden" + *analyein* "to loosen" [10]), *symmetric* (Greek *symmetros* "commensurate" [10]); *asymmetric* (*a-* + Greek *symmetros* "commensurate" [10]).

A large group of cybersecurity vocabulary units is represented by scientific / technical coinages and modern neologisms such as:

1) compound words, two or more words combined to form a new lexical unit: *firewall = fire + wall; plaintext = plain + text; ciphertext = cipher + text; keylogger = key + logger; whitelist / blacklist = white/black + list;*

2) blends (portmanteau words), parts of two words fused into one new lexical unit: *malware = malicious + software; ransomware = ransom + software; spyware = spy + software; botnet = bot (short for robot) + net (network)*;

3) initialisms, such as *pen test – penetration test* (abbreviated clipping of the first part);

4) abbreviations: *DDoS – distributed denial of service; SQL – structured query language; MITM – man-in-the-middle; IT – information technology; IAM – identity and access management*;

5) lexical units formed by semantic shift (words given new meanings in a cybersecurity context): *firewall* – from physical fire barrier to network defense; *phishing* – metaphorical extension of *fishing* (luring a victim); spoofing – from *spoof* (a hoax, parody) to deceptive imitation in cybersecurity.

Cybersecurity vocabulary also includes words derived from personal or geographic names, such as *algorithm* (from name *al-Khwarizmi*, Persian mathematician), *Trojan Horse* (from Greek mythology (metaphorical usage)).

In the modern digital era, cybersecurity has become a globally significant domain, and with it, the vocabulary of cybersecurity has rapidly expanded and internationalized. Many vocabulary units used in cybersecurity originate from English but are widely adopted across multiple languages with minimal adaptation, forming what linguists refer to as internationalisms. These are words that retain a similar form, pronunciation, and meaning across various languages due to their technical, scientific, or universal nature. These are:

1) direct internationalisms being vocabulary units that appear unchanged or only slightly adapted in languages such as French, Spanish, Ukrainan, etc.: *antivirus – антивірус* (Ukrainian), *antivirus* (French, Spanish); *authentication – authentification* (French), *autenticación* (Spanish), *аутентифікація* (Ukrainian); *cryptography – cryptographie* (French), *criptografía* (Shanish), *криптографія* (Ukrainian); *botnet – botnet* (French, Spanish), *ботнет* (Ukrainian);

2) partial internationalisms are recognizable but with more adaptation or variation: *penetration test (pen test)* – present in technical usage, but often translated (e.g. *тест на проникнення* in Ukrainian, although *пентест* is also used in informal communication); *keylogger – кейлоггер* (Ukrainian), *enregistreur de frappes* (French); *spyware* – common but sometimes translated: *logiciel espion* (French), *software espía* (Spanish);

3) non-internationalisms, language units with slang roots or culturally-specific development, such as *Man-In-The-Middle (MITM)* – often remains in English or translated literally (e.g., *«людина посередині»* (Ukrainian)).

Thus, cybersecurity vocabulary effectively transcends language barriers, contributing to a shared global vocabulary that supports international cooperation, education, and technical development in the field.

Conclusions. Cybersecurity today is an integral component of national security, as it ensures the protection of vital societal and state interests in the digital sphere. It encompasses a broad range of practices aimed at safeguarding networks, data, and infrastructure from unauthorized access and cyber threats. Defined both by national laws and international agencies, cybersecurity includes technologies, policies, and coordinated efforts to prevent cyberattacks and mitigate their consequences, thus playing a key role in preserving global stability and the sustainable development of the information society.

The analysis of the cybersecurity vocabulary reveals a semantic system that reflects the conceptual scope of the field. The identified semantic groups include such semantic groups as "security concepts and principles", "threats and attack types", "cryptography and data protection", "tools, technologies, and defenses", "incidents and responses", "policy, compliance, and governance", as well as "infrastructure and environment". This classification illustrates the complexity of cybersecurity vocabulary and its relevance for both technical and policy-oriented domains. From the perspective of word formation, cybersecurity vocabulary follows typical patterns of specialized vocabulary. Many units are of Latin and Greek origin, contributing to their scientific and internationally recognizable character. Others are coined through compounding, blending, initialisms and abbreviations, or semantic shift. The vocabulary also includes lexical units derived from personal or geographic names. A considerable portion of the cybersecurity vocabulary consists of internationalisms – lexical units that are adopted across multiple languages with little or no modification. These include direct internationalisms, as well as partial internationalisms which may be translated or adapted depending

on linguistic context. In contrast, some culturally specific or slang-based expressions remain less universal and often retain their original English form. Thus, cybersecurity vocabulary represents a dynamic and internationally relevant subset of national security vocabulary. It is conceptually coherent, lexically productive, and increasingly globalized, facilitating effective communication, international cooperation, and shared understanding in addressing modern cyber threats.

The prospects for further research include, in particular, international nature of cybersecurity vocabulary including the specifics of borrowing such units into other languages, their translation into national languages, and the development of national cybersecurity vocabulary systems.

REFERENCES:

1. Заяць Л. І. Лексика сфери національної безпеки: до визначення поняття. *Science and innovation of modern world. Proceedings of the 12th International scientific and practical conference*. London: Cognum Publishing House, 2023. С. 241–244.

2. Mijalković S., Blagojević D. The basis of national security in international law. *Žurnal za kriminalistiku i parvo*. 2014. Vol. 1. P. 49–68.

3. Жовтяк В. А. Структурні особливості англомовних термінів кібербезпеки. *Закарпатські філологічні студії*. 2024. № 34. Т. 1. С. 79–84.

4. Карвацька С. Б., Маник А. З., Строїч М. І. Кібербезпека: сучасні виклики та міжнародно-правові рамки щодо захисту даних. *Науковий вісник Ужгородського Національного Університету. Серія: Право*. 2025. № 87. Ч. 4. С. 251–256.

5. Jonker A., Lindemulder G., Kosinski M. What Is Cybersecurity? *IBM*. URL: https://www.ibm.com/think/topics/cybersecurity (Accessed on Jul 25, 2025).

6. Brown S. A. W. Beyond the Great Firewall: EU and US Responses to the China Challenge in the Global Digital Economy. *Journal of European Integration*. 2024. No. 46 (7). P. 1089–1110.

7. Mishra N. International Trade Law and Global Data Governance: Aligning Perspectives and Practices – An Overview. URL: https://ssrn.com/abstract=4741678 (Accessed on Jul 25, 2025).

8. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (Accessed on Jul 25, 2025).

9. Cybersecurity glossary. URL: https://www.optus.com.au/content/dam/optus/documents/enterprise/pdf/Cybersecurity-Glossary_FINAL.pdf (Accessed on Jul 25, 2025).

10. Online Etymology Dictionary. URL: https://www.etymonline.com/ (Accessed on Jul 25, 2025).

Дата першого надходження рукопису до видання: 08.09.2025
Дата прийнятого до друку рукопису після рецензування: 23.09.2025
Дата публікації: 28.11.2025