The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Received: *October 8, 2025* | **Revisions Requested:** - | **Revision Received:** -
Accepted: *December 1, 2025* | **Published Online:** *April 10, 2026*

Licensed (C) by Creative Commons Attribution International License 4.0 (CC BY-NC-SA)

DOI: 10.62524/msj.2026.4.1.7

Methodological Approach to Creating a Cyber Defence Terminology System

Svitlana Zvarych
PhD of Technical Sciences, Senior Researcher
Leading Research Fellow
The Central Research Institute of the Armed Forces of Ukraine
03049, Povitrianykh Syl Avenue, 28 B, Kyiv, Ukraine
e-mail: zvarych.ss@gmail.com
ORCID: 0000-0002-0636-250X

Olexandr Trokhymenko
Senior Research Fellow
The Central Research Institute of the Armed Forces of Ukraine
03049, Povitrianykh Syl Avenue, 28 B, Kyiv, Ukraine
e-mail: tvo1978@ukr.net
ORCID: 0009-0008-8574-3757

Andrii Vorobyov
Senior Research Fellow
The Central Research Institute of the Armed Forces of Ukraine
03049, Povitrianykh Syl Avenue, 28 B, Kyiv, Ukraine
e-mail: atmssw@gmail.com
ORCID: 0000-0002-1689-3128

Tetiana Poberezhets
Senior Research Fellow
Military Institute of Telecommunications and Informatization
named after Heroes of Kruty
e-mail: tetiana.poberezhets@viti.edu.ua
ORCID: 0000-0001-8007-8614

Yuliia Kotiukh
Senior Research Fellow
Military Institute of Telecommunications and Informatization
named after Heroes of Kruty
e-mail: jul365@ukr.net
ORCID: 0009-0002-4511-9905

Abstract. The relevance of the study is determined by the recognised problem of heterogeneity and fragmentation of the cyber defence terminology in Ukraine. The lack of a unified, systematic terminology hinders effective interagency communication, the development of organizational and regulatory documentation, and operational coordination in countering cyber threats. The

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

interdisciplinary nature of cyber defence, which encompasses national security, technology, law, and other fields, reinforces the need to unify the conceptual apparatus. Until now, this area has been studied selectively, without considering terminology as a coherent system. The purpose of this article is to highlight a methodological approach to creating a cyber defense terminology system. The methodological basis of the work is the theoretical foundations of terminology, in particular the distinction between the concepts of "terminology" (as a spontaneously formed set of terms) and "terminology system" (as a consciously ordered, coherent, and structured system of concepts based on a specific concept). An analysis of the current state of cyber defence in Ukraine shows that, in parallel with the development of the cyber defence system itself, cyber defence terminology is in the process of active formation and is undergoing stages of coordination and consolidation in scientific publications and legislative acts. A methodological approach is proposed, which consists in systematising and structuring the existing terminological fund to give it the characteristics of a coherent terminology system. Following this approach, key components have been identified that form the basis of the terminology system structure. The proposed model consists of six main subsystems (groups of terms): fundamental terms and concepts, cyber defence objects, cyber threats and vulnerabilities, the functioning of the cyber defence system and its components, cyber defence entities, as well as the legal and regulatory environment. It is noted that the cyber defence terminology system is synthetic in nature, integrating concepts in the fields of information technology, politics, economics, law, and defence. The proposed methodological approach has made it possible to create a comprehensive and structured terminology system that allows for the unambiguous classification of any term related to cyber defence. It is emphasised that this system is not static and will evolve along with changes in technologies and forms of cyber warfare. The practical value of the research results lies in the development of methodological recommendations for the further formation and improvement of terms based on the principles of consistency and unambiguous interpretation, which will contribute to ensuring effective communication and cooperation between different sectors and their operational coordination in the field of cyber defence.

Keywords: term, terminology, terminological system, cyber defence.

Introduction

In the scientific and legal environment of the global community, debates have long persisted regarding the explanation of the phenomenon of cyberspace, its incorporation into the framework of international law, and the establishment of mechanisms for controlling its development and protection against negative manifestations. A key challenge remains the absence of a universally accepted terminological framework in the field of cyberspace, which should eliminate the possibility of "grey areas" in the forms and methods of employing its actors and means. Over recent decades, certain definitions of terms and concepts have already been formed and stabilised within the information space; however, their interpretation and understanding require harmonisation in accordance with unified standards.

The inconsistency of cybersecurity and cyber defence terminology is a recognised problem [1]. The lack of a unified terminology in the cyber domain hinders effective communication, the development of organisational and regulatory documentation, and operational coordination, which may potentially lead to ambiguity and misunderstandings, resulting in inadequate or ineffective response strategies. The interdisciplinary nature of cyber defence, encompassing national security (including cybersecurity), technology, law, and other domains, also necessitates the establishment of a unified terminological system.

At present, the terminological framework of cyber defence in Ukraine has been studied only fragmentarily. Certain aspects have been addressed by linguists [1]–[4] as well as by specialists in relevant fields [5]–[9]. At the same time, issues and theoretical foundations related to the development

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

of the terminological framework as an integrated system have not been comprehensively examined. Therefore, in our view, the study of the terminological system of cyber defence constitutes a relevant scientific task.

The aim of this article is to present a methodological approach to the development of a terminological system for cyber defence.

Methodological Framework

For a better understanding of the subsequent material, it is appropriate to provide an overview of terminology studies, which examine terms, terminologies, and terminological systems. These categories will be analysed specifically in the context of cyber defence.

The concept of "terminology" is understood as the entire set of terms that has developed "spontaneously" within a particular field of scientific knowledge [2]. Terminologies emerge simultaneously with the establishment of a field of knowledge or activity and evolve (expand) in parallel with it. At a certain stage of development, after the accumulation of a sufficient level of experience and/or knowledge, a period of stabilisation occurs. At the same time, the process of quantitative accumulation of terms ceases and transitions into a qualitative phase namely, their generalisation and organisation into a terminological system.

A terminological system is defined as a system of terms within a particular field (or subfield) of knowledge that serves a scientific theory or conceptual framework [2].

Terminological systems originate from terminologies. However, unlike terminology, a terminological system is formed discretely, as a result of the completion and achievements of a particular stage in the development of a theory or theories within a given field. At the same time, a terminological system does not necessarily have to be based strictly on a scientific theory; in some cases, a concept or a generalised idea may be sufficient [2,3]. Thus, it can be concluded that a terminological system is formed at a certain stage in the development of a field of scientific knowledge, when a scientific theory has been established and the objects and relationships between them have been defined.

Terminological systems are characterised by the presence of the following typical features [2]:

- integrity;
- correspondence between the sum of parts and the whole;
- a certain degree of stability;
- a structured nature.

Taken together, these features allow a terminological system to be considered complete.

Results

At present, the cyber defence system of Ukraine is only partially formed. Alongside its further development, its terminology is also evolving. It is being tested in practice, discussed in academic publications [6]–[9], and agreed terms and their definitions are formalised through legislative acts at various levels [10]–[12]. However, even at this stage, the existing terminological system provides opportunities for the systematisation and refinement of current terms, as well as for the creation of new ones.

In order to capture the current state of development of the cyber defence terminological system, it is proposed, at this stage, to utilise the existing terminology, classify it into groups according to specific characteristics, and subsequently integrate these groups to ensure the structured nature and integrity of the system being developed. This approach will ensure that the emerging system complies with the fundamental characteristics of a terminological system. New terms that arise in the future will be assigned to the relevant group or will form new ones. In this way, the cyber defence terminological system will be closely linked to the cyber defence system itself and will serve to describe it.

The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Thus, in accordance with the Law of Ukraine "On the Basic Principles of Ensuring Cybersecurity of Ukraine" [11], cyber defence is defined as a set of political, economic, social, military, scientific, scientific-technical, informational, legal, organisational, and other measures implemented in cyberspace and aimed at ensuring the protection of state sovereignty and defence capability, preventing the outbreak of armed conflict, and repelling armed aggression.

An analysis of this definition indicates the presence of threats in/through cyberspace, the sources of such threats, the tools of cyber influence and cyber protection, the objects requiring cyber protection, and the actors responsible for providing it, as well as the possibility of their functioning in both peacetime and wartime conditions. Furthermore, this definition reflects the composition of the elements of the cyber defence system and the level of its functioning.

Based on the results of this analysis, within the framework of the proposed terminological system, key subsystems (or domains), which themselves are likely to represent systems, can be identified: **threats; actors of influence and protection; objects of protection; the tools employed; and the capabilities (functional capacities) of system components.** At the same time, the terminological system should describe both the internal interconnections between elements and the external regulatory relationships namely, the regulatory and legal environment. For completeness of the structure, it is also advisable to include a subsystem of basic (fundamental) terms that are common to all cyber domain systems.

It is evident that the cyber defence terminological system is synthetic in nature, as the system of concepts it encompasses integrates multiple domains, including information technology, communications, politics, economics, law, defence, as well as society and its relations.

Accordingly, in order to define the main subsystems of the cyber defence terminological system, an approach "from content to form" is applied, allowing for the identification of the principal groups of terminology.

Based on these conclusions, the proposed structure of the cyber defence terminological system may be represented as follows (Figure 1):

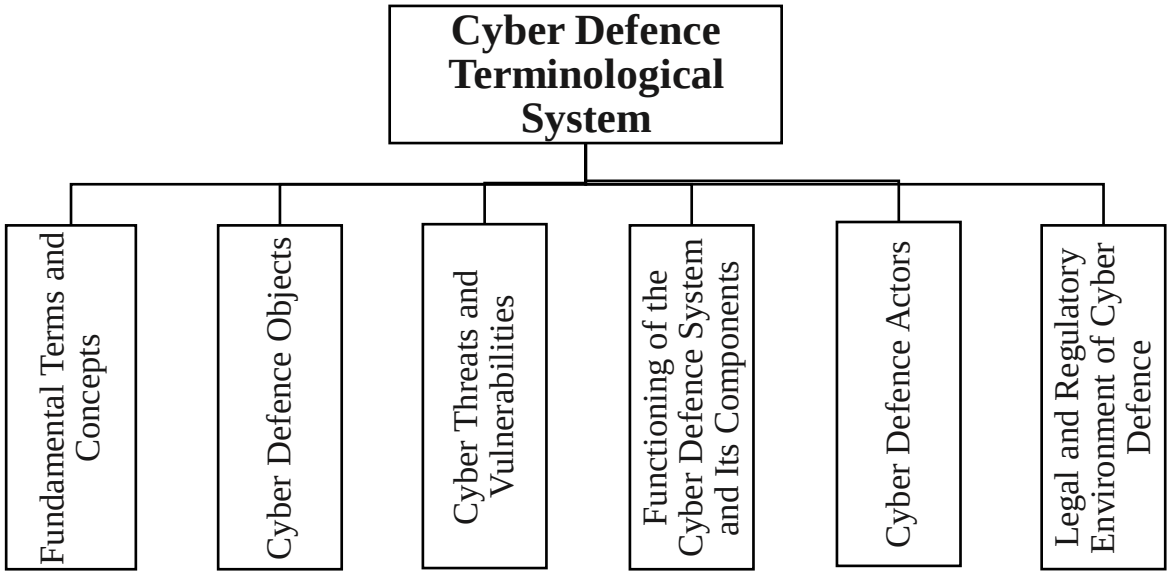


Figure 1. Generalised Scheme of the Cyber Defence Terminology System

Let us examine each of the subsystems in more detail

The fundamental terms and concepts subsystem includes the key general terms that describe cyberspace, cyber defence as a whole, and terms that cannot be assigned to more narrowly focused subsystems. These include, for example, cyberspace, cybersecurity, cyber resilience, cyber

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

protection, cyber defence, cyber operations, and others.

The **objects of cyber defence** subsystem describes all entities whose protection is the focus of cyber defence measures. This ranges from the sovereignty of the state and its governance systems to individual computers and their software products. Terms in this subsystem may include: critical information infrastructure and its components, government bodies, infrastructure objects, critical infrastructure, the National Bank of Ukraine (banking sector entity), institutions (organisations), target audiences, and individual citizens, among others.

The **cyber threats and vulnerabilities** subsystem encompasses terms that describe potential threats that the cyber defence system must counter. It is logical to divide this subsystem into two corresponding groups: threats and vulnerabilities.

Terms in the **cyber threats** group include concepts and/or names describing cyber impacts: DoS (Denial of Service) and DDoS (Distributed Denial of Service), Man-in-the-Middle, malware, social engineering, and many others.

The vulnerabilities group is primarily defined by the terminology of software and hardware tools, as well as factors associated with human error, external influence, and similar risks.

The functioning of the cyber defence system and its components subsystem, in turn, consists of lower-level subsystems containing terms related to organisational, technical, and practical measures implemented during the operation of the system.

Organisational measures terms – Cyber Defence Plan, cyber protection policy, incident response plan, disaster recovery plan, cybersecurity standards, etc.

Technical measures terms – firewall, antivirus software, encryption, multi-factor authentication (MFA), digital signature, etc.

Practical measures terms – all forms and methods of deploying cyber forces and their types, including cyber intelligence, OSINT, cyber reconnaissance, cyber counterintelligence, forensics, penetration testing, cyber training, cyber ranges, and more.

The **subjects of cyber defence** subsystem includes international, state, quasi-state, private entities, institutions, organisations, formations, and independent actors who may be directly or indirectly involved in the operation of the cyber defence system. Terms in this group include cyber forces, cybersecurity specialists, cybercriminals, cyberterrorists (groups), hacker groups, hackers, activists, and others.

The **legal and regulatory environment** subsystem, by topic, could technically be considered a component of the functioning subsystem. However, due to its unique nature and distinction from other components, it is advisable to highlight it as a separate direction. This group includes legislation, strategies, standards, departmental and interdepartmental regulatory documents, international agreements, and similar instruments.

The further development of cyber technologies is expected to alter the level of cyber threats, the degree of vulnerabilities, the scale, forms, and methods of cyber force deployment. This will necessitate new or updated terms to describe them, which, in turn, will require adjustments to the terminology system itself – including the introduction of new terms and subsystems or refinement of existing ones.

Discussions

Most of the key terms of the proposed cyber defence terminology system have already been described within other terminology systems [13]–[14]. For instance, in VST 01.114.001, definitions are provided for cyber attack, cyber operations, cyber influence, cyber threat, cyber protection, cyber weapon, cyber incident, cyber operation, and cyberspace. In VST 01.004.004, terms include cybernetic space (cyberspace), cybernetic attack, cyber strike, cybernetic threat, cybernetic security (cybersecurity), cybernetic protection, and cybernetic weapon. These terms were defined in earlier periods and reflected the level of cyber technology development at the time. However, they never became universally accepted or final. Since their definitions vary across different sources and sometimes even refer to repealed regulatory documents, they do not fully meet the requirements for

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

systematicity and coherence within the proposed terminology system. Consequently, they require revision and updating of their formulations.

Conclusion

In conclusion, the proposed methodological approach has enabled the creation of a coherent and structured cyber defence terminology system, which allows any term related to cyber defence to be unambiguously assigned to one of its subsystems. The described terminology system is not yet fully fixed. As the cyber defence system and its terminology continue to develop, the terminology system will also evolve and undergo corresponding changes.

Recommendations

Considering the described cyber defence terminology system and the requirements for terminology systems [3], the main rules for synthesising (creating and improving) new terms and their definitions can be defined as follows:

1. According to the rules of term formation [3], a term should be short and precise. Therefore, when creating a new term for the cyber defence system, it is advisable to use a word with the term-element “cyber-” rather than a multi-word phrase. For example, “cyber operation” is preferable to “cybernetic operation.”

2. Terminologies are not characterised by synonymy, so the principle of unambiguity must be observed: one object (subject, phenomenon, or event) – one term. If an established term already exists for an object or process in a related field, there is no need to create a new one. It is also inadvisable to rewrite the definition of an established term from a related field to describe another object of a different nature, as this may lead to ambiguity in understanding.

3. Following the principle of systematicity, similar concepts (processes, phenomena) that differ in terms of the level of involved subjects and objects, scale, intensity, etc., should be described according to the same rules, so that both their similarity and their fundamental differences are apparent from the definition.

For example, in the definitions of the terms cyber action, cyber strike, cyber attack, and cyber operation, it is advisable to indicate the purpose (goal), the object of influence, the acting subject, and the time.

Conflict of Interest

The authors declare that they have no competing interests regarding the subject matter of this article.

References

1. Nikolic, I. (2023). Nomination of cybersecurity terms in modern Ukrainian literary language. *Philological Journal*, *2* (22), 31–39.
2. Vashenko, L. A., Dubichynskyi, V. V., & Krymets, O. M. (2008). *Professional Ukrainian Language.* Center for Educational Literature.
3. Dyakov, A. S., Kiyak, T. R., & Kudelko, Z. B. (2000). *Fundamentals of Terminology: Semantic and Sociolinguistic Aspects*. KM Academia.
4. Kochan, I. (2016). Words with the Component “Cyber-” in Modern Ukrainian. *Bulletin of Lviv University*. *Series: Philological*, *63*, 277–285.
5. Kamchatnyi, M. V. Main features of the concept of “cyberwar” in modern international law. *Almanac of International Law*, *15*, 12–22.
6. Melnik, S. V. (2016). Conceptual and categorical apparatus in the system of professional training of future cybersecurity specialists. *Information technologies and teaching aids, 55* (5), 187–197.
7. Vdovenko, S. G., Danik, Yu. G., & Faraon, S. I. (2019). Definitive problems of the terms of the sphere of cyber security and cyber defense and the ways of their solution. *Computer Science*

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

and Cybersecurity, 1 (13), 17–29. https://doi.org/10.26565/2519-2310-2019-1-02.
8. Horhulenko, V. A. (2024). Military-theoretical justification of recommendations for the development of terminological apparatus in the sphere of cyber warfare. *Modern information technologies in the field of security and defense, 3* (51), 41–50. https://doi.org/10.33099/2311-7249/2024-51-3-41-50.
9. Mashtalir, V. V., & Gusak, Yu. A. (2025). Development of conceptual apparatus on cyber defense issues and approaches to creating cyber forces in Ukraine. *Science and Defense*, *1*, 36–46.
10. President of Ukraine. *Cybersecurity Strategy of Ukraine (96/2016).* (2016, 15 бер.). https://zakon.rada.gov.ua/laws/ show/96/2016/ed20160315#Text
11. *On the basic principles of ensuring cybersecurity in Ukraine*. Law of Ukraine No. 2163-VIII (2017, Oct. 5): as of April 20, 2025. https://zakon.rada.gov.ua/laws/show/2163-19.
12. *On the defense of Ukraine*. Law of Ukraine No. 1932-XII (1991, 6 груд.). https://zakon.rada.gov. ua/laws/show /1932-12#Text.
13. Military Standard 01.114.001 (Edit. 1). *Electromagnetic and cyber warfare. Glossary of terms and definitions. VST 01.114.001. 2023 (01).*
14. Military Standard 01.004.004 (Edit. 1). *Military Policy, Security, and Strategic Planning. State Information Security in the Military Sphere. Terms and Definitions. VST 01.004.004 – 2014 (01).*

Методичний підхід до створення термінологічної системи кібероборони

Світлана Зварич
кандидат технічних наук, старший дослідник
провідний науковий співробітник
Центральний науково-дослідний інститут Збройних Сил України
03049, проспект Повітряних Сил України, 28 Б, Київ, Україна
e-mail: zvarych.ss@gmail.com
ORCID: 0000-0002-0636-250X

Олександр Трохименко
старший науковий співробітник
Центральний науково-дослідний інститут Збройних Сил України
03049, проспект Повітряних Сил України, 28 Б, Київ, Україна
e-mail: tvo1978@ukr.net
ORCID: 0009-0008-8574-3757

Андрій Воробйов
старший науковий співробітник
Центральний науково-дослідний інститут Збройних Сил України
03049, проспект Повітряних Сил України, 28 Б, Київ, Україна
e-mail: atmssw@gmail.com
ORCID: 0000-0002-1689-3128

Тетяна Побережець
старший науковий співробітник
Військовий інститут телекомунікацій та інформатизації
імені Героїв Крут
e-mail: tetiana.poberezhets@viti.edu.ua
ORCID: 0000-0001-8007-8614

The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Юлія Котюх
старший науковий співробітник
Військовий інститут телекомунікацій та інформатизації імені Героїв Крут
e-mail: jul365@ukr.net
ORCID: 0009-0002-4511-9905

Анотація. Актуальність дослідження зумовлена визнаною проблемою неоднорідності та фрагментарності термінологічного апарату кібероборони в Україні. Відсутність єдиної, систематизованої термінології перешкоджає ефективній міжвідомчій комунікації, розробці організаційної та нормативно-правової документації та оперативній координації з протидії кіберзагрозам. Міждисциплінарний характер кібероборони, що охоплює національну безпеку, технології, право та інші галузі, посилює потребу в уніфікації понятійного апарату. Досі ця сфера досліджувалася вибірково, без розгляду термінології як цілісної системи. Метою статті є висвітлення методичного підходу до створення термінологічної системи кібероборони. Методологічною основою роботи стали теоретичні засади термінознавства, зокрема розмежування понять «термінологія» (як стихійно сформована сукупність термінів) та «терміносистема» (як свідомо впорядкована, цілісна та структурована система понять, що базується на певній концепції). Аналіз сучасного стану кібероборони в Україні показує, що, паралельно з розвитком самої системи кібероборони, термінологія кібероборони перебуває на стадії активного формування та проходить етапи узгодження та закріплення у наукових публікаціях і законодавчих актах. Запропоновано методичний підхід, що полягає у систематизації та структуруванні вже існуючого термінологічного фонду для надання йому ознак цілісної терміносистеми. Слідуючи цьому підходу виділено ключові компоненти, які лягли в основу структури терміносистеми. Запропонована модель складається з шести основних підсистем (груп термінів): фундаментальні терміни та поняття, об’єкти кібероборони, кіберзагрози та вразливості, функціонування системи кібероборони та її складових, суб’єкти кібероборони, а також правове і регуляторне середовище. Зазначено, що терміносистема кібероборони має синтетичний характер, інтегруючи поняття у сферах інформаційних технологій, політики, економіки, юриспруденції, оборони .

Запропонований методичний підхід дозволив створити цілісну та структуровану терміносистему, яка дає можливість однозначно класифікувати будь-який термін, що належить до сфери кібероборони. Підкреслено, що ця система не є сталою і буде розвиватися разом зі змінами у технологіях та формах ведення кіберборотьби. Практична цінність результатів дослідження полягає у розробленні методичних рекомендацій для подальшого формування і удосконалення термінів, що базуються на принципах системності та однозначності трактування, що сприятиме забезпеченню ефективної комунікації та співпраці між різними секторами та їх оперативній координації у сфері кібероборони.

Ключові слова: термін, термінологія, термінологічна система, кібероборона.