

# Comparative Semantic And Terminological Analysis Of Cybersecurity Terms In English And Uzbek As Semantic Fields

**Umarova Feruza Muhiddin qizi**

Teacher at General Secondary School No. 32, Karshi City

E-mail: [feruzaumarova790@gmail.com](mailto:feruzaumarova790@gmail.com)

ORCID: 0009-0008-3502-4527

**ANNOTATION.** This article examines the semantic features of cybersecurity terminology in English and Uzbek. Particular attention is paid to semantic fields, synonymy, polysemy, metaphorical transfer, borrowing, calquing, and semantic adaptation. The analysis demonstrates that English cybersecurity terminology is highly dynamic and internationally oriented, while Uzbek terminology develops through borrowing, transliteration, descriptive translation, and the creation of functional equivalents.

**Keywords:** cybersecurity, terminology, semantic field, semantic features, borrowing, calquing, metaphorization, semantic adaptation, English, Uzbek.

## INTRODUCTION

The rapid development of information and communication technologies has significantly changed modern society and created new areas of professional communication. One of the most important and rapidly developing areas is cybersecurity. The widespread use of digital technologies, online services, cloud computing, artificial intelligence, mobile applications, social networks, and interconnected information systems has resulted in the emergence of numerous concepts and specialized terms related to information protection. Cybersecurity terminology represents an important part of modern technical vocabulary. It includes terms referring to cyber threats, attacks, vulnerabilities, protection mechanisms, authentication, encryption, malicious software, data protection, network security, and incident response. Since many technological innovations initially emerge in English-speaking scientific and professional environments, English has become one of the principal sources of international cybersecurity terminology. The development of cybersecurity terminology is not limited to the creation of new words. It also involves significant semantic processes. Existing lexical units may acquire specialized meanings, ordinary words may become technical terms, and metaphorical expressions may be transferred from everyday language into the digital sphere. For example, terms such as virus, worm, firewall, phishing, backdoor, and honeypot demonstrate the influence of metaphorical conceptualization on cybersecurity. [1; 2; 4]

For the Uzbek language, the rapid development of digital technologies presents a particular terminological challenge. A considerable number of cybersecurity concepts enter Uzbek through English. These concepts can be expressed through direct borrowing, transliteration, calquing, descriptive translation, or the creation of Uzbek equivalents. Consequently, the same concept may sometimes have several linguistic forms. The semantic study of cybersecurity terminology is therefore important for both theoretical linguistics and practical translation. A translator cannot always achieve an adequate equivalent through literal translation because the semantic structure of a technical term may differ between languages. The translator must understand the underlying concept, its semantic components, and its function in a particular professional context. The purpose of this article is to examine the semantic features of cybersecurity terms in English and Uzbek and to identify the major similarities and differences between the two terminological systems. The research employs descriptive, comparative-semantic, componential, and contextual methods. The analysis is based on cybersecurity terminology used in professional glossaries, standards, academic publications, and technical communication. [6; 8; 9]

Cybersecurity terminology should not be considered merely as a collection of separate lexical units. It represents a structured conceptual system in which individual terms are interconnected through semantic and conceptual relationships. The cybersecurity domain includes several major semantic fields. These include: [1; 3]

| Semantic field | English examples | Uzbek equivalents/forms |
|----------------|------------------|-------------------------|
|----------------|------------------|-------------------------|

|                           |                                           |                                                     |
|---------------------------|-------------------------------------------|-----------------------------------------------------|
|                           |                                           |                                                     |
| Threats and attacks       | cyberattack, phishing, spoofing           | kiberhujum, soxtalashtirish fishing,                |
| Vulnerabilities and risks | vulnerability, exploit, risk              | zaiflik, eksploit, xavf                             |
| Protection                | firewall, encryption, antivirus           | xavfsizlik devori, shifrlash, antivirus             |
| Access and identity       | authentication, authorization, credential | autentifikatsiya, avtorizatsiya, hisob ma'lumotlari |
| Malicious software        | malware, ransomware, spyware              | zararli dastur, tovlamachi dastur, josus dastur     |
| Incident response         | incident, detection, recovery             | hodisa, aniqlash, tiklash                           |

The semantic organization of these terms reflects the conceptual structure of cybersecurity itself. For example, a vulnerability can be exploited by an attacker, an attack may result in a security incident, and security controls can be implemented to reduce the associated risk. Therefore, the meaning of an individual term is partly determined by its relationship with other terms within the same semantic field. [1; 3]

This observation is particularly important for bilingual terminology. A direct lexical equivalent may exist at the word level, but the conceptual relationship between the terms must also be preserved. For instance, vulnerability is not simply a synonym of risk. A vulnerability refers to a weakness or deficiency that can be exploited, whereas risk involves the possibility of an adverse consequence. Translating both concepts using the same Uzbek lexical unit would therefore lead to semantic imprecision. [7; 8]

Another interesting example is the word exploit. In general English, exploit can mean to use something for one's own benefit, sometimes unfairly. In cybersecurity, exploit can function as a technical noun referring to a method, technique, or piece of code that takes advantage of a vulnerability. [1; 5]

This process can be described as semantic specialization. Semantic specialization occurs when a general lexical item develops a narrower meaning in a particular professional field. Cybersecurity terminology contains many examples of such specialization. The Uzbek language also demonstrates semantic adaptation of borrowed technical terms. For example, the term eksploit may be used by specialists in a specialized technical sense that differs from the general meanings associated with the English verb exploit. Therefore, terminology transfer involves not only the borrowing of lexical form but also the adaptation of semantic content. [9; 10]

Metaphor plays a significant role in the development of cybersecurity terminology. New technological concepts often require names that can be understood through familiar concepts from everyday life, biology, physical space, or social activity. [10]

One of the clearest examples is firewall. The term firewall originates from the concept of a physical wall designed to prevent the spread of fire. In cybersecurity, a firewall is a security mechanism that monitors and controls network traffic according to established security rules. The term virus was transferred from biology into computing because malicious software can reproduce, spread between systems, and cause damage to its host environment. Similarly, worm refers to a type of malicious software capable of spreading through networks, while backdoor metaphorically represents a hidden method of gaining access to a system. The term phishing is another example of semantic creativity. Its form is associated with fishing, suggesting the idea of attracting or "catching" unsuspecting users through deceptive messages or websites. [1; 10]

The metaphorical character of such terms demonstrates that terminology formation is not always purely technical or mechanical. Human conceptualization and familiar cultural images also participate in the creation of specialized vocabulary. For translation into Uzbek, metaphorical terminology may create several difficulties. A literal translation may preserve the original image but may not correspond to established professional usage. Consequently, the translator needs to determine whether the metaphor itself is conventionally used in Uzbek cybersecurity discourse or whether an explanatory equivalent is more appropriate. [7; 10]

Borrowing is one of the most productive mechanisms in the formation of Uzbek cybersecurity terminology. Some borrowed terms are adapted orthographically or phonetically, while others remain close to their original English forms. [6; 8; 9]

Borrowing provides an efficient method of naming new concepts, especially when the corresponding concept does not previously exist in the target language. However, uncontrolled borrowing may create terminological inconsistency. For example, a specialist may use an English form in one context, a transliterated form in another, and a descriptive Uzbek equivalent in a third context. This situation demonstrates that Uzbek cybersecurity terminology is still developing and undergoing processes of standardization. [6; 9]

The comparison of English and Uzbek cybersecurity terminology demonstrates that semantic equivalence cannot always be achieved through direct lexical substitution. An Uzbek term may correspond only to part of the semantic content of the English term. This type of equivalence is particularly problematic because a superficially similar word may create conceptual ambiguity. Consequently, semantic equivalence should be established at the conceptual rather than purely lexical level. [7; 8]

### **LITERATURE REVIEW AND THEORETICAL BASIS**

Modern cybersecurity terminology is formed at the intersection of computer science, information security, law, management and professional communication. For this reason, its semantic organization cannot be described adequately through general-language definitions alone. Authoritative terminological sources such as the NIST Cybersecurity and Privacy Glossary and ISO/IEC 27000 establish concept-oriented definitions in which a term is connected with a network of related notions, operational procedures and risk-management practices [1; 3]. The NIST Cybersecurity Framework 2.0 also demonstrates that contemporary cybersecurity vocabulary is organized around functions such as governance, identification, protection, detection, response and recovery, which means that terminological meaning is closely linked to functional relations inside the domain [2].

Theoretical work on English and Uzbek technical terminology shows that language contact has become one of the major factors shaping the Uzbek terminological system. Studies by Tojiddinova, Norqobilova, Bozorova and Obloberdiyev indicate that English-derived forms coexist with translated, calqued and descriptively expressed variants in Uzbek professional discourse [6; 8; 9]. This coexistence is linguistically productive, but it also creates instability when several competing forms refer to the same concept. Consequently, terminology research must consider not only the lexical form of a term but also its conceptual scope, usage frequency, compatibility with related terms and degree of professional acceptance.

A particularly important issue is semantic equivalence. Rasuljonova emphasizes that the interpretation of cybersecurity terminology in Uzbek requires attention to the conceptual content of the source term rather than mechanical replacement at the word level [7]. This principle is essential because many cybersecurity terms have specialized meanings that differ from their general-language meanings. Terms such as threat, attack, exploit, credential, incident and control belong to ordinary English vocabulary, yet in information-security discourse they function as precisely delimited technical concepts. Their Uzbek equivalents must therefore reproduce the specialized meaning and the systemic relation to neighboring concepts.

Metaphorical nomination constitutes another important mechanism in the formation of cyber vocabulary. Usmanova notes the semantic and metaphorical productivity of computer and Internet terminology in English and Uzbek [10]. Terms such as virus, worm, firewall, backdoor and honeypot are especially illustrative because they transfer familiar images from biology, architecture, everyday life or physical space into the digital environment. Such metaphors are not merely decorative. They compress complex technological processes into cognitively accessible conceptual models. However, when transferred into Uzbek, the translator must decide whether to preserve the English form, reproduce the metaphor, or replace it with a more explicit technical equivalent. This decision directly affects semantic transparency and terminological consistency.

### **METHODOLOGY OF COMPARATIVE SEMANTIC ANALYSIS**

The research applies a multi-level comparative methodology. At the first stage, cybersecurity terms are grouped according to their conceptual field: threats and attacks, vulnerabilities and risks, protection mechanisms, access and identity, malicious software, and incident response. The classification is compared with the conceptual organization reflected in NIST and ISO terminology [1; 3]. At the second stage, the lexical-semantic structure of individual terms is examined through componential analysis. Core semantic features are identified and compared with the meanings of the corresponding Uzbek forms. At the third stage, translation mechanisms are classified as direct borrowing, transliteration, calquing, descriptive translation, semantic specialization or functional equivalence.

The contextual method is used because the meaning of a cybersecurity term may vary according to professional situation. For example, control may refer to a security safeguard rather than the everyday meaning of management or supervision; incident refers to an event that compromises or potentially compromises information security; and credential denotes information used to establish an identity or authorization status [1; 3]. Context therefore acts as an important disambiguating mechanism. A bilingual terminological equivalent can be considered adequate only when it preserves the relevant conceptual features in a real professional context.

The comparative procedure also distinguishes between formal equivalence and conceptual equivalence. Formal equivalence is present when an English term and an Uzbek form are structurally similar, especially in borrowed terminology such as autentifikatsiya, avtorizatsiya or antivirus. Conceptual equivalence is stronger: it requires that the target-language term activate approximately the same specialized concept, boundaries and relational structure. This distinction is important because a formally similar borrowing may still be semantically unstable if specialists use it inconsistently or if its definition has not been standardized [6; 7].

### EXTENDED COMPARATIVE ANALYSIS AND DISCUSSION

The semantic field of threats and attacks is especially dynamic. English terms such as cyberattack, phishing, spoofing, malware and ransomware are highly conventionalized in international discourse and are supported by institutional definitions [1; 2]. Uzbek professional communication uses several strategies simultaneously: kiberhujum is a transparent calque-hybrid formation; fishing is often a transliterated borrowing; spoofing may remain in English-derived form; and ransomware may be rendered descriptively as tovlamachi dastur. These examples show that Uzbek terminology balances international recognizability with semantic accessibility. Borrowing is efficient for specialists who work with global documentation, whereas descriptive translation may be more transparent for students and non-specialist readers.

The field of vulnerabilities and risks illustrates the importance of semantic boundaries. Vulnerability denotes a weakness that can be exploited, whereas risk concerns the possibility and consequences of harm. NIST and ISO terminology distinguish these concepts systematically [1; 3]. In Uzbek, zaiflik and xavf can provide workable equivalents, but translation practice must avoid collapsing the two notions into a single general concept of danger. The term exploit presents an additional difficulty because it can denote either the act of exploiting a weakness or a tool, technique or code designed to use that weakness. Its semantic specialization demonstrates why dictionary-level equivalence is insufficient and why context-based interpretation is necessary [1; 5].

The protection field includes firewall, encryption, antivirus, access control and security control. Some of these terms have relatively stable Uzbek equivalents: encryption is commonly represented by shifrlash, while antivirus is internationally transparent. Firewall is more complex. The literal image of a physical fire-resistant wall is historically important to the term, but Uzbek professional discourse may use either the borrowing firewall or the calqued expression xavfsizlik devori. From a terminological perspective, both forms can function, but their distribution should be standardized according to audience, genre and institutional practice. The metaphorical motivation of firewall also illustrates how technical language makes abstract digital processes cognitively understandable [10].

The access-and-identity field demonstrates the interaction of borrowing and semantic precision. Authentication and authorization are often transliterated as autentifikatsiya and avtorizatsiya. Although the forms are similar and sometimes confused in non-specialist discourse, the concepts are different: authentication verifies identity, whereas authorization determines permitted actions or access rights. International standards maintain this distinction, and Uzbek terminology should preserve it consistently [1; 3]. Credential is another problematic term. The phrase hisob ma'lumotlari may be understandable in some contexts, but it can be too broad when credential refers specifically to evidence or data used to establish identity or authorization. A standardized bilingual glossary should therefore include definitions, contextual examples and usage notes rather than a single isolated equivalent.

Malicious-software terminology is characterized by metaphor, abbreviation and rapid lexical renewal. Malware is itself a compressed form of malicious software, while virus and worm are metaphorical terms based on biological concepts. Ransomware encodes the notion of ransom within a software label, and spyware combines the semantic components of spying and software. Uzbek equivalents such as zararli dastur,

tovlamachi dastur and josus dastur make the conceptual meaning more transparent, but they can differ in stylistic and professional conventionality. The choice between borrowing and descriptive translation should therefore depend on terminological stability and communicative function rather than on a general preference for either foreign or native forms [6; 8; 10].

The incident-response field further demonstrates that cybersecurity terminology forms a relational semantic system. Detection, incident, response, recovery and mitigation describe different stages or actions within security-event management. The NIST Cybersecurity Framework 2.0 strengthens this functional organization by structuring cybersecurity practice around interrelated functions and outcomes [2]. In Uzbek, aniqlash, hodisa, javob choralari and tiklash can provide semantically transparent equivalents, but their technical interpretation must be distinguished from broad everyday meanings. Thus, the professional semantic field narrows and systematizes common lexical units.

A major finding of the comparative analysis is that terminological variation in Uzbek is not simply a sign of linguistic deficiency. It reflects an active stage of conceptual adaptation. New cyber concepts enter professional discourse faster than full standardization can occur. As a result, an English term, a transliterated form, a calque and a descriptive Uzbek expression may coexist for a period of time. This variation can be useful during the early diffusion of a concept, but prolonged coexistence without normative guidance can generate ambiguity. Previous contrastive studies likewise point to the need for coordinated terminology management and consistent bilingual resources [6; 8; 9].

From a semantic-field perspective, standardization should proceed through concept systems rather than isolated word lists. A glossary of cybersecurity terms should show hierarchical and associative relations: malware is related to virus, worm, ransomware and spyware; vulnerability is linked to exploit and risk; authentication is connected with identity and credential; incident is linked with detection, response and recovery. Such a model would help translators select equivalents on the basis of conceptual relations and would reduce accidental synonymy. It would also support teaching, lexicography and the development of Uzbek-language technical documentation.

The analysis also demonstrates that metaphorical transparency varies across languages. An English metaphor may be instantly recognizable to specialists because it has become conventionalized internationally, whereas its literal Uzbek rendering may sound unusual or overly explanatory. Conversely, a descriptive Uzbek equivalent may communicate the technical function more clearly than the borrowed English form. Therefore, equivalence should be evaluated according to several criteria: conceptual accuracy, professional usage, linguistic economy, derivational potential, comprehensibility and consistency with related terms. No single criterion is sufficient in all contexts.

Finally, cybersecurity terminology is highly sensitive to technological change. New attack methods, defensive mechanisms and governance practices regularly generate new terms or modify existing ones. Institutional glossaries and standards must therefore be treated as living reference systems rather than static dictionaries [1; 2; 4]. For Uzbek terminology, continuous corpus observation is particularly important. A specialized corpus could show which variants are actually preferred by cybersecurity specialists, translators, educators and official institutions. Frequency data, collocational patterns and genre distribution would provide empirical evidence for selecting standardized equivalents and documenting semantic change over time.

## CONCLUSION

The analysis demonstrates that cybersecurity terminology in English and Uzbek represents a complex and dynamically developing semantic system. The terminology includes interconnected semantic fields covering threats, attacks, vulnerabilities, protection mechanisms, access control, malicious software, data protection, and incident response. The major semantic characteristics of cybersecurity terminology include semantic specialization, polysemy, metaphorization, synonymy, borrowing, calquing, descriptive translation, and semantic adaptation. English plays a particularly important role in the international development of cybersecurity terminology. Many new concepts are first named in English and subsequently enter other languages, including Uzbek. As a result, Uzbek cybersecurity vocabulary is developing through a combination of direct borrowing, transliteration, calquing, descriptive translation, and the creation of functional equivalents.

The comparative analysis shows that lexical similarity does not always guarantee semantic equivalence. A technically accurate translation requires an understanding of the conceptual structure of the source term and its relationship to other terms within the cybersecurity system. Metaphorical terms such as firewall, virus, worm, and backdoor demonstrate that technical terminology can develop through conceptual transfer from everyday, physical, and biological domains. At the same time, terms such as threat, attack, and exploit demonstrate semantic specialization, whereby general lexical units acquire specific professional meanings. For Uzbek terminology development, semantic accuracy, consistency, and professional acceptability should be considered essential criteria. Borrowed terms may provide effective solutions for newly emerging concepts, but they should be systematically defined and standardized. Therefore, further research should focus on the creation of a comprehensive English–Uzbek cybersecurity terminology database containing definitions, semantic fields, equivalents, synonyms, contextual examples, and standardized forms. Corpus-based research involving authentic cybersecurity texts would also make it possible to determine the frequency and contextual distribution of competing terms.

In conclusion, the semantic comparison of English and Uzbek cybersecurity terminology is important not only for theoretical linguistics but also for translation studies, terminology management, professional communication, and the development of modern Uzbek scientific and technical vocabulary.

### REFERENCES

1. National Institute of Standards and Technology. NIST Cybersecurity and Privacy Glossary– Gaithersburg, MD: National Institute of Standards and Technology, 2026. – URL: <https://csrc.nist.gov/glossary> .
2. National Institute of Standards and Technology. Cybersecurity Framework (CSF) 2.0. – Gaithersburg, MD: NIST, 2024. – 71 p.
3. International Organization for Standardization; International Electrotechnical Commission. ISO/IEC 27000:2018. Information technology – Security techniques – Information security management systems – Overview and vocabulary. – Geneva: ISO, 2018.
4. International Organization for Standardization; International Electrotechnical Commission. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements. – Geneva: ISO, 2022.
5. Roback E. Glossary of Computer Security Terminology. NISTIR 4659. – Gaithersburg, MD: National Institute of Standards and Technology, 1991.
6. Tojiddinova D. The Formation and Structural-Semantic Features of Cybersecurity Terminological Units in English and Uzbek // Хорижий лингвистика ва лингводидактика. – 2026. – Vol. 4, No. 6/S. – P. 248–254. – DOI: 10.47689/2181-3701-vol4-iss6/s-pp248-254.
7. Rasuljonova K. Semantic Equivalence in Uzbek Interpretations of Cybersecurity Terminology // International Conference on Linguistics & Translation. – 2026. – Vol. 2, No. 2. – P. 56–58. – DOI: 10.5281/zenodo.18622005.
8. Norqobilova F. A. Contrastive Analyses of English and Uzbek IT Terminology // Educational Research in Universal Sciences. – 2023. – Vol. 2, No. 5. – P. 276–279.
9. Bozorova V. M., Obloberdiyev Sh. O. A Lexico-Semantic Analysis of Computer Terminology in English and Uzbek // Conference of Modern Science & Pedagogy. – 2025. – Vol. 1, No. 1.
10. Usmanova L. Some Comments on Semantic and Metaphorical Features of Computer and Internet Terms in English and Uzbek Languages // European Scholar Journal. – 2024. – Vol. 5, No. 2.