

LINGUISTIC PRINCIPLES OF CYBERSECURITY
TERMINOLOGY STANDARDIZATION AND ISSUES OF
TERMINOLOGICAL EQUIVALENCE IN ENGLISH AND UZBEK

Umarova Feruza Muhiddin qizi

Teacher at General Secondary School No. 32, Karshi City

ORCID 0009-0008-3502-4527

Annotation. *This article provides a comparative analysis of the linguistic foundations of cybersecurity terminology standardization in English and Uzbek and the problems of cross-language equivalence. It proposes approaches to term selection based on conceptual precision, systematicity, semantic transparency, formal consistency, and international harmonization. The discussion establishes the need to distinguish threat, vulnerability, and risk, as well as authentication and authorization. A bilingual terminographic model is proposed in which borrowed and descriptive equivalents are recorded together with definitions, contexts, and domains of use.*

Keywords: *cybersecurity, term, standardization, equivalence, calquing, borrowing, terminography, English, Uzbek.*

Introduction

In digital communication, the accurate interpretation of technical instructions depends on terminological precision. Reproducing the form of an English term in Uzbek does not always ensure conceptual correspondence. The use of several designations for one concept, or a single word for different concepts, can create ambiguity in translation and education. The primary task of standardization is therefore to ensure consistency between concepts, definitions, and designations rather than simply to restrict borrowing.

The definition of core domain concepts in the Law of the Republic of Uzbekistan “On Cybersecurity” provides a foundation for national terminology work [1]. However, the terms contained in legislation do not cover every software tool or emerging attack technique. This article aims to identify criteria for selecting Uzbek equivalents of English terms and to develop linguistic recommendations for their use.

Materials and Methods

The study adopts a qualitative approach. Its materials comprise national legislation, the publicly available description of ISO 704:2022, and selected entries from NIST terminology resources [1–3]. The ISO description identifies the relationships between objects, concepts, definitions, and designations as fundamental to terminology work [2]. The NIST glossary aggregates definitions from different documents; consequently, a definition should be interpreted with reference to its source document and context [3].

Comparative semantic analysis was used to examine the boundaries of meaning in English terms and their Uzbek equivalents. Componential analysis identified distinguishing conceptual features, while contextual analysis assessed the suitability of translation choices in professional situations. Examples were selected purposively and do not represent the frequency of usage across Uzbek sources. The recommendations below should be understood as scholarly proposals for dictionary compilation and text editing, rather than as an officially approved list of terms.

Results and Discussion

Conceptual precision. Selecting a term first requires establishing the object or process it designates. For example, threat corresponds to *tahdid* and denotes a circumstance or event capable of causing adverse effects, whereas vulnerability corresponds to *zaiflik* and denotes a weakness that a threat source can exploit [4; 5]. Risk involves an assessment associated with the likelihood

and consequences of harm [6]. Translating all three concepts through the general Uzbek word *xavf* can therefore obscure their conceptual boundaries.

For risk, this article proposes choosing either *kiberxavf* or the borrowed form *risk* accompanied by an explanation, depending on context. A simple password, for instance, is a vulnerability; an attempt to access an account unlawfully is an attack; and the likelihood of resulting data loss and the expected damage are relevant components of risk assessment. These terms designate distinct but related concepts rather than synonyms. Translation should preserve these relationships.

Systematicity. The suitability of an individual term also depends on its capacity to function within a family of related terms. The Uzbek base *shifrlash* supports combinations such as *shifrlash kaliti* (encryption key), *shifrlangan ma'lumot* (encrypted data), and *shifrlash algoritmi* (encryption algorithm). *Tahdid* similarly retains its conceptual core in *tahdid manbai* (threat source) and *tahdidlarni aniqlash* (threat detection). If the same document uses *shifrlash* in one passage and *kodlash* in another for encryption, clarification is required: encoding does not necessarily denote a cryptographic operation that provides confidentiality.

Semantic transparency. An equivalent should, where possible, make the concept's central feature understandable. For example, *zararli dasturiy ta'minot* expresses the meaning of malware. For ransomware, *to'vlamachi zararli dastur* may be proposed as a descriptive equivalent. Calling it only *shifrllovchi virus* ("encrypting virus") narrows the concept: such software is not necessarily a virus, and extortion does not always rely exclusively on encrypting data. A designation's convenience must therefore be evaluated alongside its correspondence with the definition.

Formal consistency and linguistic adaptation. The spelling, suffixation, and combinational patterns of borrowed terms should follow a consistent editorial policy. For example, the Uzbek spelling *fishing* can be confused with

the ordinary English word fishing. An initial explanation such as phishing — fishing, aldov orqali maxfiy ma'lumotni qo'lga kiritishga qaratilgan usul (“a deceptive method aimed at obtaining confidential information”) is therefore useful. This connects the international form with the Uzbek expression; the selected variant can then be used consistently in subsequent passages.

International harmonization. Specialists should be able to recognize a term in international documentation or a software interface. However, retaining an international form does not itself establish equivalence. Although autentifikatsiya and avtorizatsiya are formally similar, in access management the former concerns verifying a claimed identity, whereas the latter concerns determining permitted actions [7; 8]. Educational texts can explain them as “checking who someone is” and “determining what they are allowed to do.” These explanations do not replace the terms in every technical context.

Levels of Terminological Equivalence

This article proposes evaluating equivalence in three situations. The first is conceptual equivalence, in which definitions and distinguishing features correspond; encryption — shifrlash provides a working example. The second is partial equivalence requiring explanation. For credential, the expression hisob ma'lumotlari (“account information”) may be too broad in some contexts because it can include ordinary profile information. Where identity verification is involved, an explanation referring to “information or evidence used to substantiate identity” can be more precise.

The third situation involves constructing a contextual equivalent where a stable one-word designation has not been established through evidence. For example, exploit as a noun may designate code, a tool, or a technique that takes advantage of a vulnerability. Translating it invariably as foydalanish (“use” or “using”) creates grammatical and semantic ambiguity. Where a software object is intended, zaiflikdan foydalanuvchi kod (“code that exploits a vulnerability”) is appropriate; where a process is intended, zaiflikdan foydalanish (“exploiting

a vulnerability”) may be selected. Term selection must therefore account for grammatical category and referent.

A Practical Model for Standardization

A bilingual terminological entry should contain more than an English–Uzbek word pair. It should record the English term, recommended Uzbek designation, concise definition, domain label, context, variant status, and source. For authentication, for example, autentifikatsiya can serve as the principal designation, with “verification of a claimed identity” as an explanation within access management. Its distinction from authorization should be recorded separately. Identifying the source of a definition helps distinguish a compiler’s interpretation from an institutional definition.

Conceptual precision should be the primary criterion for evaluating variants, followed by comprehensibility, systematicity, linguistic compatibility, and international recognizability. Frequency should be treated as evidence only when corpus data are available. Specialist review can identify technical errors, while linguistic editing checks spelling and combinational patterns. Reader testing can assess whether explanations are understandable. These stages are recommendations for future standardization work, rather than experiments conducted as part of the present study.

Conclusion

Equivalence between English and Uzbek cybersecurity terms depends primarily on conceptual correspondence rather than formal similarity. The analysis demonstrates the need to preserve distinctions between threat, vulnerability, and risk, as well as authentication and authorization. Borrowing, calquing, and descriptive translation should be selected according to definitions and contexts of use rather than by treating any single method as universally preferable. The proposed terminographic model supports consistent documentation of variants. Its practical effectiveness requires subsequent evaluation through corpus analysis and assessment by domain specialists.

REFERENCES

1. Republic of Uzbekistan. On Cybersecurity. Law No. O'RQ-764 of 15 April 2022. <https://lex.uz/acts/-5960604>
2. ISO. ISO 704:2022. Terminology work — Principles and methods. Geneva, 2022. Public description. <https://www.iso.org/standard/79077.html>
3. NIST. Computer Security Resource Center Glossary. <https://csrc.nist.gov/glossary>
4. NIST. Threat. CSRC Glossary. <https://csrc.nist.gov/glossary/term/threat>
5. NIST. Vulnerability. CSRC Glossary. <https://csrc.nist.gov/glossary/term/vulnerability>
6. NIST. Risk. CSRC Glossary. <https://csrc.nist.gov/glossary/term/risk>
7. NIST. Authentication. CSRC Glossary. <https://csrc.nist.gov/glossary/term/authentication>
8. NIST. Authorization. CSRC Glossary. <https://csrc.nist.gov/glossary/term/authorization>