SEMANTIC EQUIVALENCE IN UZBEK INTERPRETATIONS OF CYBERSECURITY TERMINOLOGY

Khurshida Rasuljonova
Affiliation: —
E-mail: example@email.com
https://doi.org/10.5281/zenodo.18622005

ARTICLE INFO

Received: 10th February2026
Accepted: 11th February 2026
Online: 12th February 2026

KEYWORDS

semantic equivalence, cybersecurity terminology, interpretation, Uzbek language

ABSTRACT

This article examines the problem of semantic equivalence in the interpretation of cybersecurity terminology from English into the Uzbek language. Due to the rapid development of information technologies, cybersecurity terms are constantly entering Uzbek, often without standardized equivalents. The study analyzes selected cybersecurity terms and identifies cases of full equivalence, partial equivalence, and non-equivalence in interpretation. The research is based on comparative and semantic analysis of English terms and their Uzbek renderings. The results show that borrowing, descriptive translation, and explanation are the most frequently used strategies, while the lack of terminological standardization remains a key challenge. The article emphasizes the importance of semantic accuracy for effective professional communication..

Introduction

Cybersecurity has become one of the most critical areas within modern computer networks due to the increasing number of digital threats and cybercrimes. As international cooperation in information security grows, the demand for accurate interpretation of cybersecurity terminology also increases. English serves as the primary source language for most cybersecurity terms, while Uzbek interpreters are required to render these concepts accurately for academic, professional, and public communication.

Semantic equivalence is a core concept in translation and interpretation studies, referring to the degree to which meaning is preserved between the source and target languages. In the field of cybersecurity, achieving semantic equivalence is particularly challenging because many terms denote abstract, highly technical, and rapidly evolving concepts. This article aims to explore the types of semantic equivalence and non-equivalence that arise when interpreting cybersecurity terminology into Uzbek.

Review of Related Literature

The concept of semantic equivalence has been widely discussed in translation studies. Scholars such as Nida (1964) emphasize the importance of meaning-based equivalence rather than formal similarity. In terminology studies, Cabré (1999) highlights the necessity of precise conceptual correspondence in specialized domains.

Research on English–Uzbek technical translation indicates that borrowing is the most common strategy for rendering new terms. However, limited attention has been paid to semantic accuracy in oral interpretation, particularly in the cybersecurity domain. Existing studies mainly focus on general computer terminology, leaving cybersecurity terms underexplored. This article addresses this gap by providing a focused semantic analysis of cybersecurity interpretations.

Methodology

The study employs a qualitative research approach based on comparative and semantic analysis. A corpus of commonly used cybersecurity terms was selected from English-language security reports, online conferences, and educational materials. Their Uzbek interpretations were collected from media broadcasts, translated training materials, and interpreter performances. The terms were analyzed according to three categories: full semantic equivalence, partial equivalence, and non-equivalence.

Analysis and Discussion

Full Semantic Equivalence

Some cybersecurity terms demonstrate a relatively high degree of semantic equivalence in Uzbek interpretation. For example, the term virus is directly borrowed into Uzbek and widely understood by both specialists and the general public. Although originally metaphorical, its meaning has become conventionalized, allowing interpreters to use it without semantic loss.

Partial Semantic Equivalence

Many cybersecurity terms fall into the category of partial equivalence. The term malware, for instance, is often interpreted as zararli dastur. While this translation conveys the general idea of harmful software, it does not fully reflect the broad scope of the original term, which includes various types of malicious programs. Similarly, phishing is sometimes explained as aldov orqali ma'lumot o'g'irlash, which captures the function but lacks terminological conciseness.

Semantic Non-Equivalence

Semantic non-equivalence occurs when no direct or adequate Uzbek equivalent exists. Terms such as zero-day vulnerability and exploit present serious challenges for interpreters. These terms are frequently borrowed or briefly explained during interpretation, which may result in incomplete understanding. The abstract and technical nature of these concepts contributes to semantic gaps between the source and target languages.

Results

The analysis reveals that semantic equivalence in cybersecurity interpretation is influenced by several factors, including terminological novelty, level of abstraction, and interpreter expertise. Borrowing ensures terminological accuracy but may reduce accessibility for non-specialist audiences, while descriptive translations improve comprehension but risk semantic simplification. The lack of standardized Uzbek cybersecurity terminology remains a major obstacle to achieving consistent semantic equivalence.

Conclusion and Recommendations

Achieving semantic equivalence in the interpretation of cybersecurity terminology into Uzbek is a complex task that requires both linguistic competence and technical knowledge. This article has demonstrated that while some terms achieve full equivalence through borrowing, many others suffer from partial or non-equivalence due to conceptual and terminological gaps. To address these challenges, it is necessary to develop standardized cybersecurity glossaries, enhance interpreter training, and encourage collaboration between linguists and IT specialists. Further research may involve corpus-based studies and experimental analysis of interpreter performance in cybersecurity contexts.

References:

Nida, E. A. (1964). Toward a Science of Translating. Leiden: Brill.

Cabré, M. T. (1999). Terminology: Theory, Methods and Applications. Amsterdam: John Benjamins.

Crystal, D. (2001). Language and the Internet. Cambridge: Cambridge University Press.