**Література:**

1. Карпік М., Труцуненко І. Прецедентний характер конекторів у сучасній німецькій мовію *Наукові праці Міжрегіональної академії управління персоналом. Філологія.* Київ, 2022. 2(4). С. 130–135.
2. Приходько Л. А. Художній час і художній простір у поезії : автореф. дис. … канд. філол. наук. Кіровоград, 2004. 19 с.
3. Ремарк Е. М. Чорний обеліск. Історія запізнілої юності. Київ, 1962. 399 с.
4. Шупта-В'язовська О. Проблеми вивчення художнього часу і простору в контексті літературознавчої термінології. *Історично-літературний журнал.* Київ, 2007. № 13. С. 4–54.
5. Hapkemeyer A., Ingeborg Bachmann. Entwicklungslinien in Werk und Leben. Wien : Verl. d. österreich. Akad. d. Wiss., 1990. 169 s.
6. Hendrix H. Ingeborg Bachmanns «Todesarten»-Zyklus. Eine Abrechnung mit der Zeit. Würzburg : Königshausen & Neumann, 2005. 238 s.
7. Remarque E. M. Der schwarze Obelisk. Geschichte einer verspäteten Jugend. Berlin, Weimar : Aufbau-Verlag Berlin und Weimar, 1965. 462 s.

DOI https://doi.org/10.30525/978-9934-26-548-8-26

## ORDINARY WORDS AS CYBERSECURITY TERMS OF ART: MISINTERPRETATION RISKS IN TRANSLATION

## ЗВИЧАЙНІ СЛОВА ЯК ГАЛУЗЕВІ ТЕРМІНИ КІБЕРБЕЗПЕКИ: РИЗИКИ НЕПРАВИЛЬНОГО ТЛУМАЧЕННЯ В ПЕРЕКЛАДІ

**Oliinyk O. S.**
*Candidate of Philological Sciences, Associate Professor, Associate Professor at the Department of Translation, Applied and General Linguistics Volodymyr Vynnychenko Central Ukrainian State University Kropyvnytskyi, Ukraine*

**Олійник О. С.**
*кандидат філологічних наук, доцент, доцент кафедри перекладу, прикладної та загальної лінгвістики Центральноукраїнський державний університет імені Володимира Винниченка м. Кропивницький, Україна*

Cybersecurity is "preservation of confidentiality, integrity and availability of information in the cyberspace" [1, p. 41]. For the first time, the need to protect cyberspace was legally recognized in the U.S. military doctrine **Concept Force XXI** in 1996 [3, p. 21]. In Ukraine, the term

"cybersecurity" was first used in 2007 [op. cit.], and the Law of Ukraine "On the Basic Principles of Ensuring Cybersecurity of Ukraine" dates back to 2017**.** Being a relatively new field of information technology, cybersecurity and data protection are rapidly evolving [2, p. 4]: the changes in the basic terminological framework of the U.S. Department of Defense in the field of cybersecurity over the past three years amount to 25–30% [3, p. 21]. Thus, the professional language of cybersecurity and its translatability into Ukrainian is a topical research issue.

The present study focuses on ordinary English words as cybersecurity terms of art and the misinterpretation risks while translating them into Ukrainian. *Words* (*terms) of art* are typically defined as terms that have specialized meaning in a particular field or profession. Among cybersecurity terms, English ordinary words (e.g. *bug, handshake, salt, sandbox, root,* etc.) used as words of art are of particular interest for translation purposes because their specialized meanings may not directly correspond to equivalent terms in Ukrainian as the target language. Such semantic shifts and possible specialization of ordinary words in professional contexts should be in the focus of translators' cognitive and linguistic processing of the original text.

Clear understanding and translation consistency of ordinary words as cybersecurity terms of art require their categorization. A possible common taxonomy that aligns cybersecurity definitions and terminologies to enable the categorization of existing institutions and expertise across Europe – *The JRC Cybersecurity Taxonomy* [1], presents the list of the following 15 domains: "1) Assurance, Audit and Certification; 2) Cryptology (Cryptography and Cryptanalysis); 3) Data Security and Privacy; 4) Education and Training; 5) Human Aspects; 6) Identity Management; 7) Incident Handling and Digital Forensics; 8) Legal Aspects; 9) Network and Distributed Systems; 10) Security Management and Governance; 11) Security Measurements; 12) Software and Hardware Security Engineering; 13) Steganography, Steganalysis and Watermarking; 14) Theoretical Foundations; 15) Trust Management and Accountability". Though the taxonomy above can serve as a crucial reference point for cybersecurity activities and the alignment of cybersecurity definitions and terminology, a more user-friendly framework for translation practices would incorporate two key parameters: 1) the cybersecurity domain and 2) the translatability of terms of art.

Categorizing terms based on the specific cybersecurity domain they belong to will yield the following groups: 1.1) **Attacks and Threats**, e.g. *backdoor* (a secret method of bypassing security to access a system; *бекдор / метод обходу стандартних процедур автентифікації*); *eavesdropping* (intercepting communications to steal sensitive data; *прослуховування*); *flood* (overloading a system with excessive requests;

*флуд / надсилання великої кількості запитів*); 1.2) **Vulnerabilities and Exploits**, e.g. *crack* (bypassing security protections, such as breaking passwords or software licenses; *зламування*); *hook* (a technique used in malware to intercept system functions; *гук* / *перехоплення*, яке може бути використане шкідливим кодом); *bug* (a fault in the system of instructions that operates a computer; *баг / помилка в програмі*); 1.3) **Authentication and Access Control**, e.g. *gate* (a security control that regulates access to a system; *шлюз*); *handshake* (process of establishing communication; *процедура узгодження*); key (a security mechanism preventing unauthorized access; *ключ* / *захисний механізм, який допомагає запобігти несанкціонованому доступу*); 1.4) **Defensive Measures and Security Mechanisms**, e.g. *firewall* (system that filters traffic**;** *фаєрвол / брандмауер*); *honeypot* (decoy system to attract attackers; *пастка для хакерів*); *sandbox* (isolated environment for testing; *пісочниця / ізольоване середовище*).

Several factors can cause potential misinterpretations, ambiguous or misleading translations of ordinary terms of art. One of them is a failure to convey their specialized meaning in cybersecurity, e.g. it will be incorrect/misleading to translate *exploit* (code used to attack vulnerabilities) as *експлуатація*; its Ukrainian equivalent term of art is *експлойт / використання вразливості*. The term of art *brute force* (password cracking method) cannot be literally translated as *груба сила* (physical violence); its correct Ukr. counterpart is *метод перебору*.

Another cause of potential translation misinterpretation is words with multiple meanings: e.g. *root* can have the following meanings depending on the context: the part of a plant that grows underground and absorbs water and nutrients (*корінь*); a source or origin of something (*джерело або причина чогось*); the base or core of a word from which other words are derived (*корінь слова*); a solution to an equation (*корінь рівняння*); heritage or origin of a person or group *(коріння, походження),* etc. In cybersecurity, *root* means "the highest level of access in a computer system", therefore this term of art has the Ukr. equivalent "*найвищий рівень доступу в комп'ютерній системі".*

Some words can function as translator's false friends, e.g. *blacklist* and *чорний список* look similar, but in cybersecurity, its specialized meaning is "list of blocked entities" that is equivalent to Ukr. *список блокування*. The term *zero-day* has a Ukrainian calque *нульовий день*, but its specialized equivalent is *вразливість, невідома постачальнику ПО* (a vulnerability unknown to the vendor). The word *threat* (which generally means *загроза*) has acquired a specialized meaning in cybersecurity, referring to a *potential cybersecurity risk*. The term *worm* typically denotes a crawling creature, but in cybersecurity, it relates to self-replicating malware that spreads across

networks. In this context, it can be translated as *хробак* or *черв'як* (шкідливе програмне забезпечення).

In conclusion, relevant translation strategies to avoid misinterpretation of ordinary words as cybersecurity terms of art include: 1) using direct borrowings for some terms (*рут-доступ* instead of *корінь доступу*); 2) providing contextual clarification (*salt* in cryptography is *випадкові дані для хешування*); 3) avoiding word-for-word translations (the equivalent for *handshake* is *процедура узгодження***,** but not *рукостискання***).** In every case, it is worthwhile cross-checking with Ukrainian Cybersecurity and IT Standards.

**Bibliography:**

1. European Commission: Joint Research Centre, Nai Fovino, I., Neisse, R., Hernandez Ramos, J., Polemi, N., Ruzzante, G., Figwer, M., & Lazari, A. *A proposal for a European cybersecurity taxonomy*. European Commission, Joint Research Centre. Publications Office, 2019. URL: https://data.europa.eu/doi/10.2760/106002

2. Kalogeraki, E. M.; Polemi, N. A taxonomy for cybersecurity standards. *Journal of Surveillance, Security and Safety*. 2024. No. 5. P. 95–115. http://dx.doi.org/10.20517/jsss.2023.50

3. Vdovenko S., Danik Y., Faraon S. Definitive problems of the Terms of the Sphere of Cyber security and Cyber Defense and the Ways of their Solution. *Computer Science and Cybersecurity*. 2019. № 1. С. 18–30. DOI: https://doi.org/10.26565/2519-2310-2019-1-02