faculty of social sciences, arts and humanities
ktu 1922

47/2025
Research Journal
Studies about Languages
pp. 19-36
ISSN 1648-2824 (print)
ISSN 2029-7203 (online)
DOI 10.5755/j01.sal.1.47.42127

LINGUISTICS / KALBOTYRA

Creating terms in the cybersecurity domain:
Proposals by different user groups

Received 07/2025 | Accepted 11/2025

HOW TO CITE: Rackevičienė, S. (2025). Creating terms in the cybersecurity domain: Proposals by different user groups. *Studies about Languages / Kalbų studijos*, 47, 19–36. https://doi.org/10.5755/j01.sal.1.47.42127

Creating terms in the cybersecurity domain: Proposals by different user groups

Terminų kūrimas kibernetinio saugumo srityje: skirtingų vartotojų grupių pasiūlymai

SIGITA RACKEVIČIENĖ, Mykolas Romeris University, Lithuania

Abstract

This paper continues the presentation of findings from the sociolinguistic terminological study, based on a survey on Lithuanian synonymous cybersecurity terms, the first part of which was reported in Rackevičienė and Utka (2024). The survey, involving 593 respondents from various age groups, professional fields and levels of expertise, asked participants to identify the most suitable terms for ten cybersecurity concepts. Respondents could either select terms from the pre-selected synonymous term lists or propose their own terms in open-entry slots, providing justifications for their choices. While the previous article analysed categorical data from pre-selected lists, the current article focuses on the textual data from open-entry slots where participants provided their own proposals. The analysis involves multiple stages: first, a quantitative descriptive analysis of the distribution of proposals across respondent groups and concepts; second, classification of proposals into formation patterns based on linguistic nomination principles, followed by quantitative analysis of their proportions and distributions across respondent groups; and third, a qualitative interpretive analysis of formation tendencies within each pattern. The findings reveal formation patterns and sociolinguistic differences in term-creation processes, highlight the creative potential of Lithuanian language users, and underscore the importance of incorporating their input into the development of Lithuanian terminology, particularly in rapidly evolving domains such as cybersecurity.

KEYWORDS: sociolinguistic terminological study, cybersecurity terms, terminology survey, neologisms, metaphorical terms, descriptive terms, borrowed terms.

Introduction

Lithuanian cybersecurity terminology is relatively young – it still shows considerable variation and inconsistency, and is predominantly composed of original English terms, particularly in informal contexts. Developing our own Lithuanian terminology fosters effective communication beyond the specialist community and broadens the reach of specialised knowledge, enhancing public comprehension of cybersecurity threats and raising cyber awareness. It also supports the creation of a national terminology, essential for use in national legislation, documentation of executive bodies, educational resources, and more, forming an important part of the national culture.

Terminology is primarily created by domain experts. However, involving broader groups of language users in the development of national terminology not only raises awareness of the terminology but also provides valuable insights into the needs of various user groups, fosters creativity and generates ideas for further refinement and standardisation of national terminology.

An effort to engage different Lithuanian language users in discussions about Lithuanian cybersecurity terminology was undertaken by inviting participants from various sociodemographic groups to take part in a terminology survey on Lithuanian synonymous cybersecurity terms. The survey gathered responses from 593 participants representing diverse age groups and areas of expertise. Respondents were asked to select the most suitable Lithuanian terms for 10 cybersecurity concepts. They could either select terms from pre-prepared lists of synonymous terms or propose their own terms in open-entry slots, providing explanations for their choices (the survey questionnaire and dataset are available in the CLARIN-LT repository[1]).

The results of the analysis of the categorical data, specifically data from the provided lists of pre-prepared synonymous terms, were published in Rackevičienė and Utka (2024). The current article continues the presentation of the survey results, focusing on the analysis of the textual data, which includes responses from open-entry slots where participants provided their own term proposals.

The aim of this article is to examine how the quantitative and qualitative characteristics of the proposed terminological designations vary across different respondent groups, and to identify the linguistic tendencies underlying each of the identified formation patterns of the proposals.

The paper presents:

- the theoretical background of the research focusing on the core concepts in general and terminological neology, as well as on recent research on neologisms;
- the survey content and segmentation of respondents;
- survey results (1): quantitative findings on the distribution of proposed designations across different respondent groups and individual cybersecurity concepts;
- survey results (2): qualitative classification of proposed terminological designations according to their formation patterns, along with quantification of their overall proportions and distribution across different respondent groups;
- survey results (3): establishment of formation tendencies within each pattern through a detailed qualitative analysis.

The research methodology employs a mixed-method approach, implemented in three stages. First, a quantitative descriptive analysis examined the distribution of proposals across respondent groups and individual cybersecurity concepts, providing insights into which groups contributed more proposals and which concepts elicited the greatest number of suggestions. Second, all proposed designations were explored qualitatively and classified into four formation patterns (metaphorical, descriptive, borrowed, and combined) based on linguistic nomination principles; then the proportions of each pattern as well as their distribution across respondent groups were quantified. Third, a qualitative interpretive analysis explored the specific formation aspects within each pattern, highlighting the formation tendencies and the creativity displayed by respondents. This mixed-method approach allowed a comprehensive understanding of both the quantitative distribution and the qualitative nature of the terminological proposals provided by the survey respondents.

[1] Survey Data on Preferences of Lithuanian Cybersecurity Terminology, CLARIN-LT digital library in the Republic of Lithuania, http://hdl.handle.net/20.500.11821/59.

Research Background

The research examines sociolinguistic processes reflected in the proposals for Lithuanian designations of cybersecurity concepts submitted by respondents belonging to different professional fields and possessing varying levels of expertise. Given this diversity, it is first necessary to determine whether the proposals should be treated as instances of lexical innovation, terminological innovation, or as situated at the intersection of both; this issue is addressed in the first subsection of the research background. The second subsection positions the study within recent neologism research in Europe. For this purpose, recent studies are broadly grouped into corpus-based and survey-based methodological approaches with comparisons drawn regarding their analytical focus, research aims, and the sociolinguistic aspects they address.

Defining Processes of Lexical and Terminological Innovation

Lexical innovation processes arise from the interaction of two opposing forces: a tendency toward stability driven by the need to ensure effective communication and a tendency toward change motivated by the need to adapt to evolving realities, enhance communication, as well as attract attention (Guilbert, 1975 as cited in Cabré, 2023, p. 347).

Through lexical innovation processes, newly formed or newly perceived lexical units – neologisms – emerge in discourse. They are inherently multifaceted: unstable by nature, as their newness is temporary and relative, since what appears new to one group of speakers may already be familiar to another. Moreover, neologisms are not only elements of the linguistic system but also reflections of a particular area of reality, being "the result of a categorisation process biased by the culture of a sociocultural group" (Cabré, 2023, p. 340). The spread of neologisms within a language can vary. Some neologisms remain confined to the individual lexicon of their creator, while others become part of the broader social lexicon (Cabré, 2023, p. 354). They vary also in their formation patterns as well as in authorship and the circumstances of their creation (cf. Miliūnaitė, 2020). Consequently, neologism analysis must integrate both linguistic and extralinguistic perspectives.

Neologisms that emerge in general discourse (referred to as general neologisms) are distinguished from those that arise in specialised domains, known as terminological neologisms (also called neoterms or neonyms), which are deliberately created by domain experts (ISO 1087:2019; Druță, 2013; Miliūnaitė, 2020; Mikelionienė, 2025).

Terminological neologisms result from terminological innovation processes closely linked to developments in science and technology. They emerge within specialised knowledge domains, driven by the necessity and deliberate efforts of experts to designate newly arisen concepts. Terminological innovations are indispensable for specialised knowledge: it is neither possible to construct specialised knowledge, nor to communicate new scientific or technological developments without creating new terms (Cabré Castellví et al., 2012).

Whereas general neologisms often arise spontaneously in response to specific communicative situations within general discourse, terminological neologisms are tied to systematic naming practices. They are deliberately coined to designate a concept and distinguish it from others within a defined conceptual system, ensuring minimal ambiguity, which is essential for effective specialised communication (Costa et al., 2022). Term formation typically follows established procedures and employs mechanisms that align new terminological designations with pre-existing patterns within the relevant domain (for typologies of term-formation patterns, see Druță, 2013; Mockienė, 2016; Humbley, 2018). As a result, terminological designations tend to be more stable than general neologisms, some of which arise spontaneously from individual creativity and may function in various forms of expression, including stylistically marked ones (Miliūnaitė, 2020).

The research presented in this paper draws on the theoretical framework outlined above and reflects the intersection of lexical and terminological innovation processes. As the survey involved respondents from different areas of expertise and varying levels of professional experience, their proposals can be considered part of the broader process of lexical innovation in the Lithuanian language. The suggestions are particularly valuable as instances of spontaneous lexical creativity, revealing which formation patterns are perceived as the most transparent and communicatively effective. At the same time, because the survey included domain experts, their proposals can also be seen as deliberate, informed attempts to name concepts within the cybersecurity domain, thus becoming part of the ongoing terminological innovation process. Although the proposed designations cannot yet be considered neologisms in the strict sense, as they have not entered actual usage in Lithuanian discourse, they may nonetheless be regarded as candidate neologisms, created by individual, albeit anonymous, authors for a specific occasion: a survey in which participants were invited to propose the most suitable Lithuanian designations for ten predefined cybersecurity concepts.

Recent Research on Neologisms

Research on neologisms often focuses on either general or terminological neologisms, though many studies address both types. Recent research has been largely driven by significant societal and technological developments, including crisis-related vocabulary (e.g., economic downturns, pandemics, military events) and the rapid evolution of digital communication over the last decade. Neologism research methodologies display substantial variation, reflecting a wide range of methods that can broadly be grouped into corpus-based approaches and survey-based approaches involving user participation.

Corpus-based approaches involve the analysis of neologisms used in written texts and are employed for multiple purposes: tracing the long-term viability of neologisms and evaluating their suitability for inclusion in general-language dictionaries (Afentoulidou & Christofidou, 2021; Bueno & Freixa, 2022); examining communicative functions of neologisms, their degree of neologicity, and gender-based sociolinguistic aspects of usage in mass media texts (Llopart-Saumell & Cañete-González, 2023); exploring the sociolinguistic dynamics of neologism diffusion across different communities on a social media platform by integrating corpus and social network analysis (Würschinger, 2021); investigating communicative motivations behind neologism use in social media environments and their sociolinguistic functions (particularly in constructing and negotiating online identity and community belonging) (Szymańska, 2025; Chyrvonyi, 2025) and analysing their communicative deployment as instruments of information warfare (Styshov, 2022), among others.

Survey-based studies, though less common than corpus-based ones, offer valuable insights into speakers' cognitive processes in neologism acceptance, awareness, and creation. They typically adopt a top-down approach, presenting participants with lists of neologisms, or a bottom-up approach, in which participants generate neologisms themselves. Examples of the top-down approach include Wolfer and Klosa-Kückelhaus' study (2023), which tested German speakers' acceptance of native versus borrowed neologisms using a mouse-tracking paradigm to measure decision uncertainty, and the work of Skubis et al. (2023), which examined students' awareness, comprehension, and attitudes towards neologisms related to sexual technologies. In contrast, a bottom-up study by Sánchez Ibáñez and Pérez Sobrino (2024) investigated formal and semantic neological procedures in the creation of names for COVID-19-related objects, eliciting participants' spontaneous naming through the use of pictures. These studies also explored sociolinguistic variation, considering factors such as age or gender in relation to the investigated aspects of neologisms.

The present research contributes to the latter group of studies by employing a bottom-up approach to the investigation of neologisms. Unlike the previously described bottom-up study, which used pictures as stimuli, respondents in this research were asked to propose designations for cybersecurity concepts based on definitions provided in Lithuanian and their English equivalents. This research also examines designation formation patterns and sociolinguistic variation, focusing on respondents' areas and levels of expertise rather than age. To the author's knowledge, no comparable sociolinguistic research has previously been conducted on neological processes within a specialised domain in Lithuanian.

Survey Content and Segmentation of Respondents

Concepts Selected for the Terminology Survey

The selection of concepts for the terminology survey was based on research conducted in the project 'Bilingual Automatic Terminology Extraction' (DVITAS)[2]. Data from the English-Lithuanian parallel and comparable cybersecurity corpora, along with the bilingual cybersecurity termbase compiled during the

[2] DVITAS (Dvikalbis automatinis terminų atpažinimas / Bilingual Automatic Terminology Extraction) https://sitti.vdu.lt/dvitas/en.

project, allowed identifying cybersecurity concepts whose Lithuanian designations remain highly diverse and inconsistent, and are often replaced by original English terms. Based on these insights, 10 concepts were selected for the survey to determine the preferred terminological designations across different user groups (see **Table 1**).

Table 1 Concepts selected for the terminology survey

Concept 1	‘cyberattack’	Concept 6	‘phishing’
Concept 2	‘spam’	Concept 7	‘botnet’
Concept 3	‘denial-of-service attack’	Concept 8	‘hacker’
Concept 4	‘man-in-the-middle attack’	Concept 9	‘honeypot method’
Concept 5	‘brute force attack’	Concept 10	‘zero-day vulnerability’

Concept 1 is a generic superordinate concept that represents the entire class of cyberattacks. Concepts 2–6 refer to different forms of cyber threats. Concept 2, ‘spam’, refers to unsolicited electronic messages sent widely for advertising, phishing, malware distribution, or other malicious purposes. Concepts 3–6 represent different types of cyberattacks:

- Denial-of-service attack: blocking authorised access to systems or disrupting time-critical operations.
- Man-in-the-middle attack: inserting oneself between two communicating parties and impersonating one or both of them to access sensitive and confidential data.
- Brute force attack: automatically entering numerous combinations of values, typically to discover passwords and gain unauthorised access.
- Phishing: sending fraudulent emails pretending to be legitimate to trick users into surrendering private information.

Concept 7, ‘botnet’, refers to a network of infected computers controlled without the owners' knowledge. Concept 8, ‘hacker’, refers to a person who breaks into computer systems without authorisation, typically for malicious purposes.

The remaining concepts are related to cybersecurity mechanisms. Concept 9, ‘honeypot method’, refers to a network-attached system set up as a decoy to lure cyberattackers, allowing the detection, deflection, and/or study of hacking attempts. Concept 10, ‘zero-day vulnerability’, represents a vulnerability in a system or device that has been disclosed but is not yet patched (definitions of the concepts are based on IATE (European Union, 2025) and the Glossary of the National Institute of Standards and Technology, US (National Institute of Standards and Technology, n.d.)).

Thus, the concepts represent a wide range of cyber realities. Some, such as ‘cyberattack’, ‘spam’, and ‘hacker’, are familiar to a wide range of Internet users, while others are more specific and require specialised knowledge to fully understand them.

Structure of the Survey

The first part of the survey concentrated on collecting sociodemographic data from the respondents, while the second (main) part gathered data on the selected or proposed Lithuanian terminological designations of the provided cybersecurity concepts, along with the reasons for their selections or proposals.

The main part of the survey was divided into ten sections, each dedicated to a specific concept. Each section included the following elements: Concept Definition in Lithuanian; Common English Designation; Question 1 “Which term do you think is the most suitable to represent this concept?”, accompanied by a list of synonymous terms and an open-entry slot for respondents’ own terms; and Question 2 “Why did you choose this term or propose your own version?", accompanied by a list of predefined reasons and an open-entry slot for additional explanations.

As mentioned in the Introduction, this paper focuses on analysing the textual data collected from open-entry slots in Question 1.

Segmentation of Respondents

The survey was distributed to various educational institutions, state bodies, and private companies in Lithuania to reach respondents from diverse age groups and professional backgrounds, including those studying or working within IT and cybersecurity, as well as those outside these fields.

Data were collected from 593 respondents, who were segmented based on two key variables: education level and area of expertise. According to education level, respondents were grouped into university/college students (58.9%) and university/college graduates (41.1%). Based on area of expertise, they were categorised into experts (41%) and the general public (59%). The expert group comprised students and professionals in IT, cybersecurity, and electronic communications. The general public group included students and professionals from a range of fields, such as language and translation; social sciences (including law, political science, public administration, business management, economics, psychology, social work, education, and communication); natural sciences (life sciences, physical sciences, medicine, and agricultural sciences); and formal sciences (such as mathematics, civil engineering, and financial technologies). Thus, two segmentations were applied to explore the collected data (see **Fig. 1**; for a detailed presentation of the respondents' sociodemographic data, see Rackevičienė & Utka, 2024).

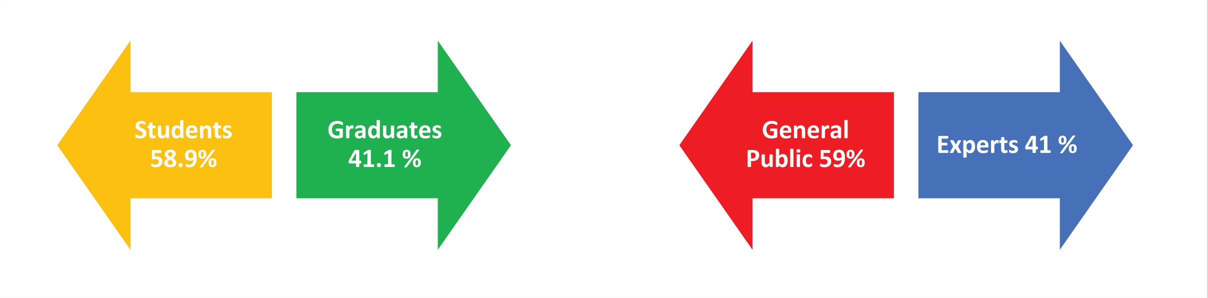

Fig. 1 Data segmentations and segment proportions

Survey Results (1)

Distribution of Proposals across Respondent Groups

As explained earlier, respondents had two options: they could either select the term they considered most suitable from pre-prepared synonymous term lists or suggest their own terms in an open-entry slot labelled "Other". This latter option was used 151 times, of which 126 responses contained term proposals, while the remainder provided comments only, without any terminological suggestions. Some responses included the same proposal (e.g., the designation *šlamštas* for the concept 'spam' was suggested by 12 respondents), while other responses contained multiple proposals (e.g., one respondent suggested four designations for the concept 'botnet'). Thus, the number of responses with term proposals did not equal the total number of term proposals.

The number of responses with term proposals varied across respondent groups. In the Students vs. Graduates segmentation, graduates submitted considerably more responses with term proposals than students (35% of all responses with term proposals came from students, and 65% from graduates). In the General Public vs. Experts segmentation, experts contributed more than the general public (38% of all responses with term proposals came from the general public, and 62% from experts) (see **Fig. 2**).

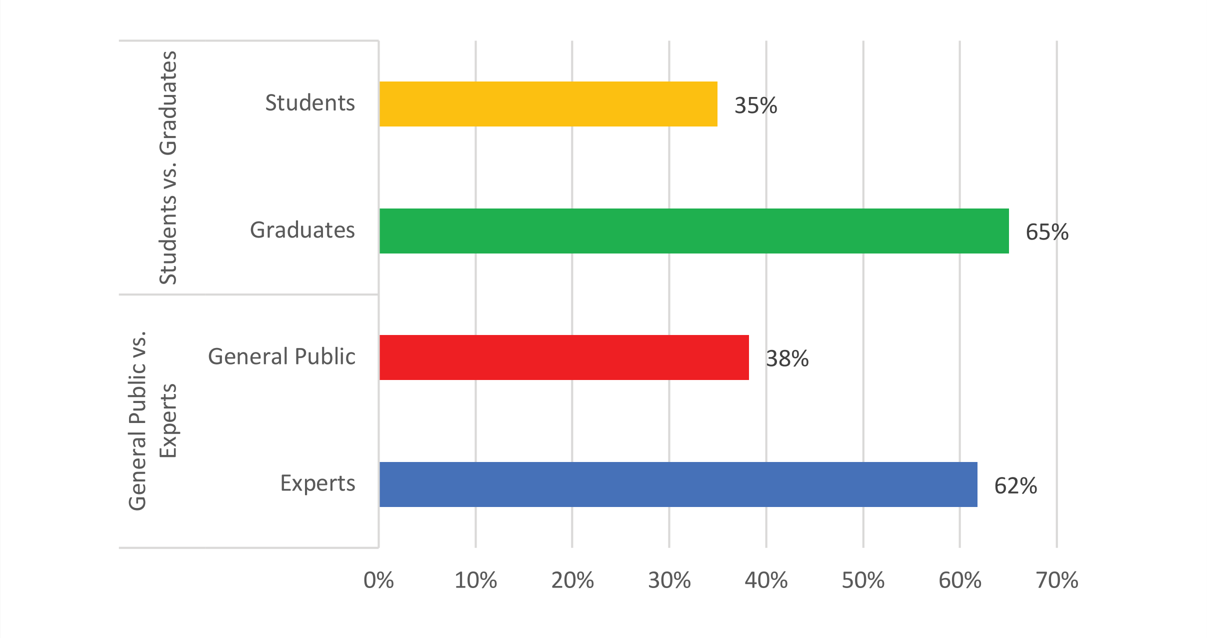

Fig. 2 Proportions of responses with term proposals across respondent groups

Distribution of Proposals across Individual Concepts

In total, the respondents proposed 119 terminological designations in their responses. The number of designations per concept varied from 1 to 22, indicating that some concepts elicited more term proposals than others. **Fig. 3** presents the counts of designations provided for each concept.

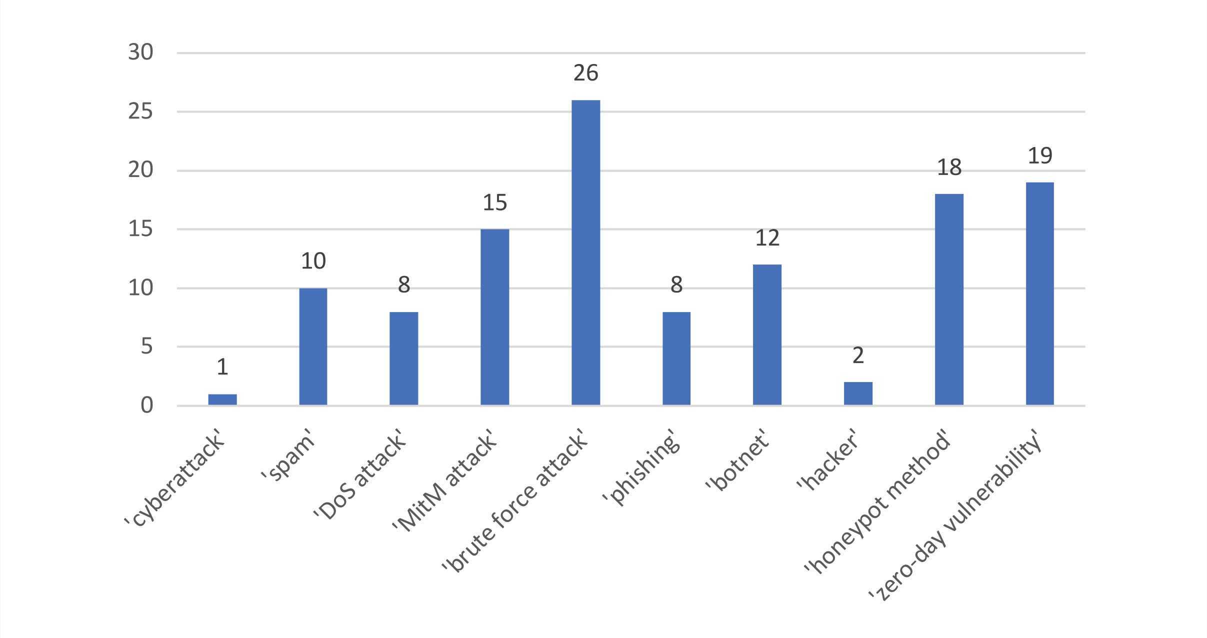

Fig. 3 Counts of proposed terminological designations for each concept

Fig. 3 reveals that Concept 5 ‘brute force attack’ received the highest number of proposals (26), followed by Concept 10 ‘zero-day vulnerability’ (19 proposals), and Concept 9 ‘honeypot method’ (18 proposals). In contrast, Concept 1 ‘cyberattack’ and Concept 8 ‘hacker’ received only 1 and 2 proposals, respectively. It is important to note that each concept was accompanied by a pre-prepared list of synonymous terms ranging from 4 to 10, meaning all the proposals mentioned here represent additional designations beyond those provided in the lists.

Survey Results (2)

Formation Patterns of Proposed Designations and their Overall Proportions

As mentioned earlier, respondents proposed a total of 119 terminological designations. Their analysis allowed the identification of four main formation patterns, presented in **Fig. 4** alongside their overall proportions in the dataset: metaphorical, descriptive, borrowed, and combined (a combination of descriptive and borrowed elements). The classification of the observed patterns was based on nomination principles: metaphorical, involving figurative designation through semantic mechanisms; descriptive, relying on literal naming realised through morphological and syntactic means; and borrowing, where existing foreign terms were adopted with varying degrees of localisation. This classification thus reflects two intersecting oppositions: figurative versus literal lexical nomination (metaphorical vs. descriptive), and direct borrowing versus varying degrees of modification or attempts at original formation (borrowed vs. metaphorical and descriptive). In addition to these three patterns, 16 designations were categorised as inaccurate due to conceptual inconsistencies.

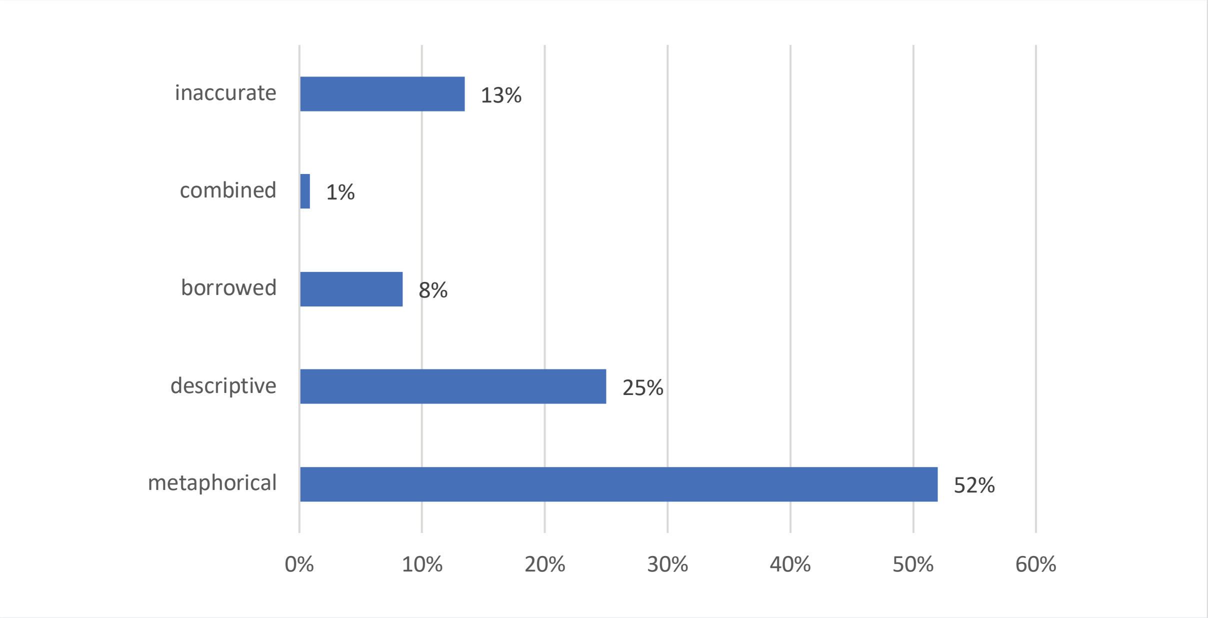

Fig. 4 Overall proportions of proposed designations by formation pattern

Metaphorical designations encompass lexical entities formed on the basis of conceptual mappings between the cybersecurity domain and other domains, allowing the expression of complex cybersecurity concepts through imagery drawn from everyday experience (e.g. *šlamštas* ‘rubbish’ for Concept 2 ‘spam’). As the chart indicates, metaphorical designations constitute the largest proportion of all proposals. Descriptive designations rank second, directly expressing concept characteristics by highlighting one or several aspects that the respondent considers particularly salient (e.g. *aptarnavimo trikdymo ataka* ‘service disruption attack’ for

Concept 3 ‘DoS attack’). Borrowed designations follow, comprising English terms with varying degrees of localisation (e.g. *honeypotas* for Concept 9 ‘honeypot method’). A combined designation is represented by a single proposal that combines a descriptive component with an unlocalised borrowing – *duomenų viliojimas „phishing“* ‘data seduction “phishing”’ for Concept 6 ‘phishing’. The remaining proposals are classified as inaccurate designations, as they do not reflect the intended concepts with sufficient precision.

Distribution of Formation Patterns across Respondent Groups

The analysis of formation patterns and their overall proportions prompted further investigation into which respondent groups predominantly employed each pattern. Therefore, the data were reprocessed based on the two segmentations (Students vs Graduates and General Public vs Experts), and quantitatively analysed. The results are presented in **Fig. 5** and **Fig. 6**.

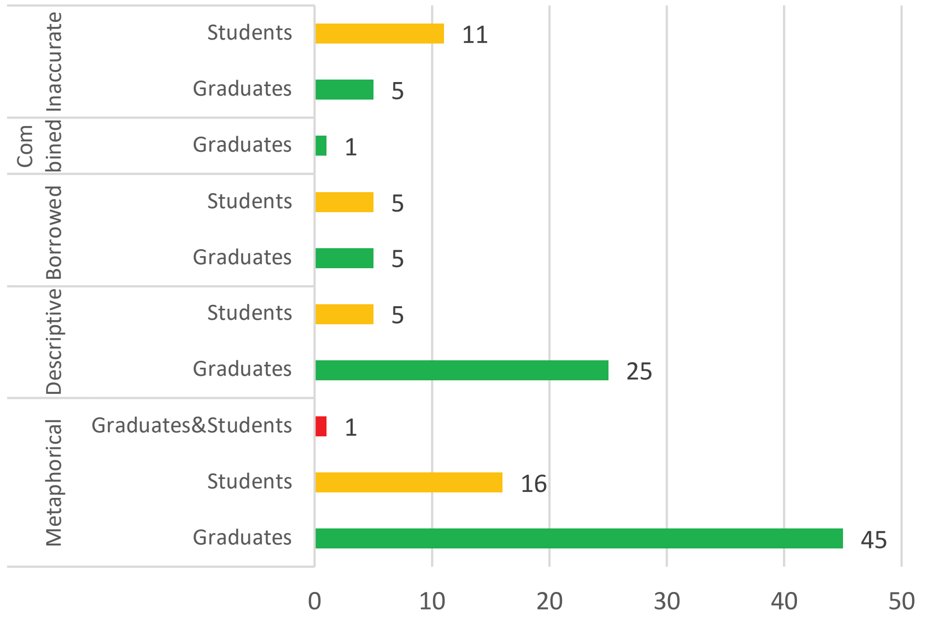

Fig. 5 Proposal counts by formation pattern in Students vs. Graduates segmentation

The results of the Students vs. Graduates segmentation reveal that the vast majority of metaphorical and descriptive designations were proposed by graduates, although students were also productive, particularly in suggesting metaphorical designations. Borrowed designations were relatively few in both groups and evenly distributed (five in each group).

The results of the General Public vs. Experts segmentation indicate particularly high productivity among experts in proposing metaphorical designations. Descriptive designations were suggested fairly evenly by both groups, with 18 from experts and 12 from the general public. Borrowed designations once again ranked lowest in frequency for both groups, with the majority proposed by experts.

Interestingly, certain designations were proposed by multiple respondent groups: *šlamštas* (‘rubbish’ for Concept 2, ‘spam’) was suggested by students and graduates, each group including both experts and members of the general public; *nulinė spraga* (‘zero gap’ for Concept 10, ‘zero-day vulnerability’) was proposed only by graduates, who included both experts and members of the general public.

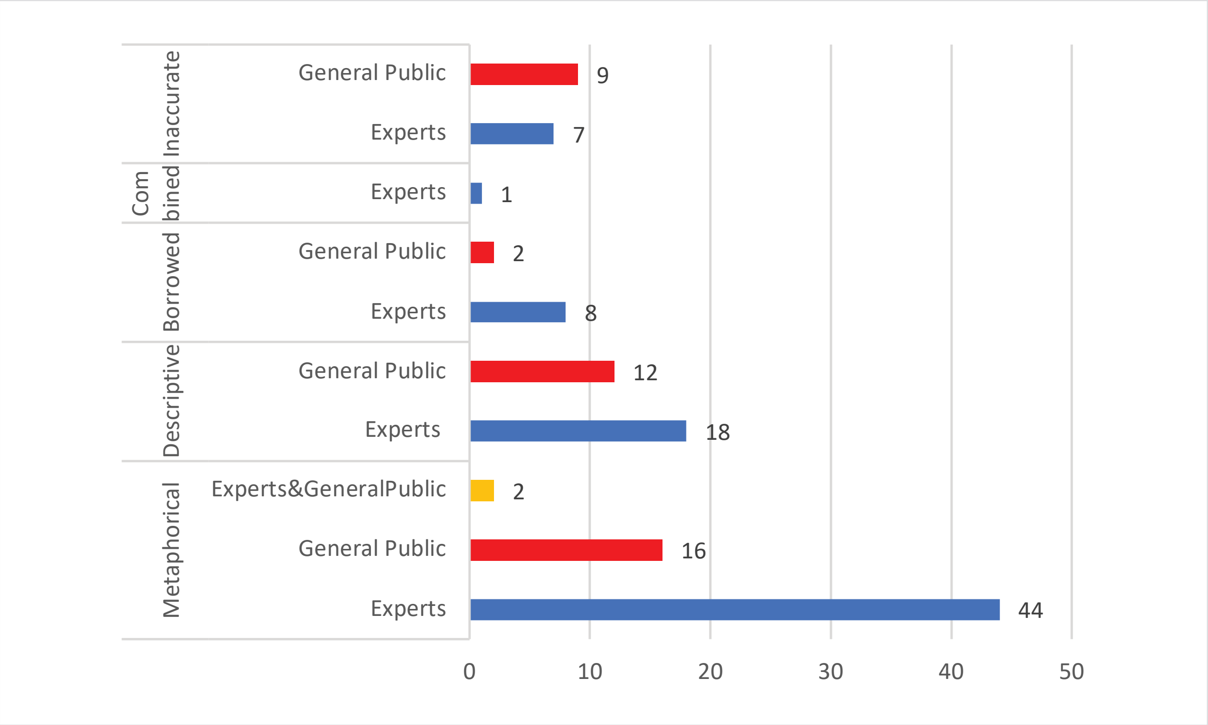

Fig. 6 Proposal counts by formation pattern in General Public vs. Experts segmentation

The charts also show inaccurate designations in both segmentations. However, deeper insights emerge from an all-groups analysis: 6 inaccurate designations were provided by students-experts (studying IT-related fields), 5 by students-general public, 4 by graduates-general public, and 1 by a graduate-expert.

Survey Results (3)

In the final stage of the research, a detailed qualitative analysis of the terminological proposals within each formation pattern was conducted to identify formation tendencies specific to each pattern.

Metaphorical Designations

The largest group of proposals falls into the category of metaphorical designations, comprising 62 proposals in total, ranging from 0 to 16 proposals per concept. Some closely mirror the lexical structure of the corresponding English metaphorical terms and may be considered lexical calques. Some incorporate slight modifications of the designations suggested by the survey organisers. However, the majority represent entirely original formations. To reveal the tendencies of metaphor creation, metaphorical proposals for each concept will be discussed separately.

For Concept 2 ‘spam’, four metaphorical designations were proposed, based on the metaphor of rubbish and a combination of rubbish and meat metaphors. Three of the designations incorporate the root of the noun *šlamštas* (‘rubbish’), such as *šlamštas* (‘rubbish’) and *elektroninis šlamštas* (‘electronic rubbish’). One proposed designation was particularly original – *šlamštiena* (‘rubbish meat’). This word is included in the Lithuanian database of neologisms where its meaning is explained as ‘low-value information or work’ (Lietuvių kalbos najažodžių duomenynas, 2025). In the survey, this neologism was suggested as a designation for ‘spam’. The respondent, who proposed this designation, explained their proposal by drawing a parallel between the original English term *spam* and the Lithuanian neologism: the English term originally referred to canned meat (spiced ham). Similarly, *šlamštiena* refers to meat, as it is formed by combining *šlamštas* ('rubbish') with the suffix *-iena*, which is commonly used to denote meat (e.g., *kiaulė* ('pig') ➙ *kiauliena* ('pork'), *jautis* ('bull') ➙ *jautiena* ('beef')). Another proposal, *paštetas* ('liver pâté'), is also related to meat and likely stems from the original English meaning of *spam*.

For Concept 3 'DoS attack', two metaphorical designations were proposed. Both are based on a metaphor related to bee life, specifically, colonies of bees / swarms. The respondent suggested a longer and a shorter variant of the designation: *fiktyvių užklausų spiečiaus ataka* ('bogus query swarm attack') and *užklausų spiečiaus ataka* ('query swarm attack'). These designations incorporate the noun *spiečius* ('swarm'), which primarily refers to a colony of bees formed when a large group of bees splits. In this context, *spiečius* is used metaphorically to describe a large number of attacks (bogus queries) following one another. The metaphor is original, no similar English formations were detected by the author of the article in the English corpora.

For Concept 8 'MitM attack', eight metaphorical designations were suggested. They are based on the metaphors of intermediary, mysterious figures and grabbing/stealing. Most proposals include denotations of an intermediary. 4 of them are multi-word expressions: *"žmogaus tarpe" ataka* 'man in interspace attack', *kibernetinio tarpininko ataka* 'cyber intermediary attack', *įsiterpiančiojo asmens ataka* 'intervening person attack', *intarpo ataka* 'insert attack. One designation is an original compound composed of the preposition *tarp* 'between' and the noun *ataka* 'ataka' - *tarpataka* 'between-attack'. Two proposals stand out as particularly distinct from the rest, being highly expressive and based on visual associations with mysterious figures. One of them – the designation *maskės ataka* ('mask attack') – evokes the image of a criminal concealing their identity behind a mask. For some reason, the borrowing *maskė* is used instead of the standard Lithuanian noun *kaukė*, which adds a more colloquial tone to the designation. Another designation – *SVETIMO ataka* ('stranger attack') likely draws inspiration from the science fiction horror film *Alien* (1979), the Lithuanian title of which is *Svetimas* ('Stranger'). These designations may seem to carry a more playful tone, with a touch of humour. However, they also reflect considerable creativity, indicating that the respondents were not only having fun but also thoughtfully considering the core characteristics of the concept. One more designation suggested for this concept is *nugvelbimo ataka* ('grabbing/stealing attack'). It draws a parallel between physical-world grabbing/stealing and the activity in cyberspace, where sensitive or confidential data is intercepted and taken without authorization, emphasizing the illicit nature of the attack.

Concept 5 'brute force attack' received the highest number of metaphorical designations (16), which make up 62% of all proposals for this concept. The suggested metaphors are based on various realia that are compared with diverse characteristics of the concept: physical force (brute nature of force and activity of using force), persistence, something out of norms, good fortune that happens by chance, and master key.

Four metaphors based on the meaning physical force closely resemble the English term in their lexical structure, incorporating nouns and/or adjectives associated with 'force' and 'brute/rough'. Examples include *grubios jėgos ataka* ('rough force attack'), *brutalaus įsilaužimo ataka* ('brutal break-in attack'), *brutaliai paprasta ataka* ('brutally simple attack'), and *forsavimo ataka / forsavimas* ('forcing attack / forcing'). One suggested designation includes abbreviation *BJ* referring to *brutali jėga* 'brute force' – *BJ ataka* 'brute force attack'. Two proposals included the deverbal noun *nulaužimas*, which in its primary meaning refers to physically breaking something off (e.g., a tree branch). However, in modern Lithuanian, it is often used in the context of hacking. This metaphoric meaning is also reflected in the proposals: *slaptažodžio nulaužimo ataka* ('password cracking attack') and *paskyros nulaužimas* ('account cracking').

One proposed designation is the noun *determinacija* ('determination'), most likely based on the notion of persistence. It reflects the relentless nature of a brute force attack, where the attacker is determined to break into a system by trying various combinations until the correct one is found, aligning with the idea of persistent effort.

Two metaphorical designations are based on the meaning referring to something out of norms. They include original self-made adjectives that carry connotations of extreme behaviour. The adjective *beskrupulė* is derived from the noun *skrupulas* ('scruples, hesitation, fear, remorse'). Thus, the designation *beskrupulė ataka* ('unscrupulous attack') suggests an attack that is pursued with complete disregard for ethics and moral principles, focusing solely on achieving its goal. The adjective *beskaitlė* is derived from the adjective *skaitlus* (‘numerous, abundant’). The designation *beskaitlė ataka* (‘numberless attack’) conveys an attack characterised by an overwhelming or endless number of attempts, emphasising the persistence and disregard for boundaries that are characteristic of brute force attacks.

One metaphorical designation is based on the meaning referring to good fortune that happens by chance. It includes an idiomatic expression, conveying this meaning – *aklos sėkmės išpuolis* (‘blind luck attack’). By using this expression, the respondent likely aimed to highlight the random, trial-and-error nature of brute force attacks, which involve systematically trying all possible passwords or encryption keys until the correct one is found – essentially relying on chance and luck.

Two proposals include the noun *visraktis* with the meaning ‘master key’ – a key that can open multiple locks, even if each lock has its own unique key: *visrakčio ataka* (‘master key attack’) and *visrakčio parinkimo ataka* (‘master key selection attack’). The respondent who proposed these designations explained their reasoning, arguing that the English metaphor *brute force* is not suitable for this concept. In their view, *brute* suggests a scenario where someone smashes glass, breaks down doors, and quickly grabs valuables. In contrast, brute force attacks do not involve physical force but rather the exploitation of security vulnerabilities. The respondent draws a parallel between this process and situations in which mechanical locks are unlocked with a master key. This metaphor is original, no similar English formations were detected by the author of the article in the English corpora.

Two designations (*slaptažodžio žvejyba* ‘password fishing’, *duomenų žvejyba* ‘data fishing’) – while reflecting some characteristics of the concept – are too similar in lexical structure to the English term *phishing*, which designates a different concept. Therefore, in the author’s opinion, they are not suitable, as it would be better for clarity and distinctiveness to reserve these or similar designations for phishing-related concepts.

For Concept 6 ‘phishing’, two metaphorical designations were suggested. One is based on the metaphor of fishing – *duomenų žvejyba* (‘data fishing’). This designation mirrors the lexical structure of the English blending *phishing*, which combines the words *password + fishing*. However, instead of using the noun meaning ‘password,’ the respondent suggests using the noun *duomenų* (‘data’), most likely because this term more accurately reflects the concept. Phishing refers not only to the theft of passwords but also to other forms of personal data that may be targeted. Another proposal is based on the metaphor of an enticing dance – *viliotinis* ‘enticing dance’. This metaphor is original and carries a humorous tone. However, though it may seem amusing, it aptly captures the idea of something enticing, aligning with the goal of phishing, which is to attract and trick the target.

For Concept 7 ‘botnet’, five metaphorical designations were proposed. All of them are based on metaphors involving mindless creatures controlled by an external force. Two proposals include the noun *zombiai* (‘zombies’) in multi-word expressions: *zombių tinklas* (‘zombie network’) and *skaitmeninių zombių tinklas* (‘digital zombie network’). One proposal includes the abbreviation – *SZ tinklas* (‘digital zombie network’). The other two proposals incorporate the noun *robotas* (‘robot’) in innovative Lithuanian formations: *robotinklas* (‘robot network’) and *užvaldytas robotynas* (‘robot network under control’). The former is a compound word created by combining the first two syllables of *robotas* with the noun *tinklas* (‘network’), while the latter uses the suffix *-ynas*, often employed for nouns referring to places with a large quantity of something (e.g., *gėlynas* (‘flower bed’) or *žvaigždynas* (‘constellation’)).

Both *zombiai* (‘zombies’) and *robotas* (‘robots’) describe entities that automatically execute commands given by an external force. The metaphor of a ‘zombie network’ is not original, as it is also used in English as an alternative to the term *botnet*. In contrast, the ‘robot network’ metaphor appears to be a original creation in this context.

For Concept 8 ‘hacker’, two metaphorical designations were proposed, each reflecting a different perspective. The first designation is based on the metaphor of an intruder/burglar – *kibernetinis įsibrovėlis* (‘cyber intruder’). This term includes the noun *įsibrovėlis* (‘intruder, burglar’), emphasising the role of hackers as unauthorised individuals who gain access to systems, much like burglars breaking into homes. The second designation is based on the metaphor of a computer professional – *kompiuterių meistras* (‘computer master’). This humorous designation implies that hackers are not just intruders but, in fact, highly skilled IT professionals.

Concept 9 'honeypot method' received the second highest number of metaphorical designations (14), accounting for 78% of all proposals for this concept. The designations are based on the metaphors related to trap, ambush and bait, and honey.

Eight of the proposals are original Lithuanian metaphors formed with nouns referring to traps. Four of these incorporate modifiers indicating that the traps are designed specifically for burglars. Three of these are multi-word expressions: *įsilaužėlių pinklės* ('burglar's snare'), *įsilaužėlių spąstai* ('burglar's trap'), and *įsilaužėlių gaudyklė* ('burglar's catcher'), while one is a compound word created by the respondent: *įsilaužgaudis* ('burglar-catcher'). The single-word variants of the above-mentioned multi-word expressions were also proposed as possible designations: *pinklės* ('snare'), *spąstai* ('trap'), and *gaudyklė* ('catcher'). All of these designations suggest that hackers (referred to as burglars) are lured into systems designed to deceive and monitor them. Another proposed designation is also an original Lithuanian metaphor based on the concept of a flytrap: *musgaudis* ('flytrap'). This metaphor emphasizes the idea of luring an intruder into a controlled environment, much like a flytrap attracts and captures flies.

The three proposals include nouns/noun phrases referring to ambush and bait: *pasalos metodas* ('ambush method'), *jauko metodas* ('bait method'), and *lengvo grobio metodas* ('easy prey method'). The designation *pasalos metodas*, based on the meaning of ambush, focuses on the idea of luring and positioning the target for an unexpected attack, a concept often used in military contexts. In contrast, *jauko metodas* and *lengvo grobio metodas* are based on the idea of an ambush in fishing and hunting, where a fish or predator is lured with bait.

Three metaphorical designations include nouns referring to honeypot, honey and beehives: *medaus puodo metodas* ('honeypot method'), *medaus metodas* ('honey method'), and *medaus ir avilio metodas* ('honey and beehive method'). While the honeypot metaphor is also used in English (in the compound *honeypot*), the beehive metaphor is an original creation in this context, further enhancing the idea of an environment designed to attract and trap intruders.

For Concept 10 'zero-day vulnerability', nine metaphorical designations were proposed, based on the metaphors of the number zero, a day, a state of being hot, and a state of being fresh.

Two designations are similar to their English counterparts in lexical structure but are shorter, with 'zero day' replaced by just 'zero': *nulinė spraga* ('zero gap') and *nulinis pažeidžiamumas* ('zero vulnerability'). The other two are also similar to the English ones, but in this case, the word meaning 'zero' is omitted, and 'day' is retained with additional modifiers: *šios dienos spraga* ('this day gap') and *paskutinės dienos spraga* ('last day gap'). One proposal includes the adjective meaning 'hot': *karšta spraga* ('hot gap'). This metaphor refers to a situation that is very new, much like a dish that is hot when it has just been prepared. Four proposals include the adjective meaning 'fresh': *šviežia spraga* ('fresh gap'), *šviežiausia spraga* ('the freshest gap'), *šviežiausia žinoma spraga* ('the freshest known gap'), *šviežiausias pažeidžiamumas* ('the freshest vulnerability'). These metaphors refer to a situation that is very new, with the parallel being drawn to fresh food products.

Descriptive Designations

Descriptive designations hold the second position among respondents' proposals, comprising 30 proposals in total, ranging from 0 to 7 per concept. The lexical structures of descriptive designations for the same concept vary, depending on how explicitly and accurately respondents intended to depict the concept and which characteristics they chose to emphasise.

For Concept 2 'spam', the proposed four descriptive multi-word expressions differ in their heads, which denote texts, letters and bulk messages, while modifiers refer to their unsolicited or unreliable nature: *nepageidaujamai siunčiami tekstai* ('unsolicited sent texts'), *nepageidaujamos masinės žinutės* ('unsolicited bulk messages'), and *nepatikimas laiškas* ('unreliable letter'). In addition, a single-word proposal was submitted highlighting another aspect of spam – namely, its frequent advertising purpose: *reklama* ('advertisement').

Descriptive proposals for Concept 3 'DoS attack' focus on the outcome of the attack but highlight different aspects of service disruption: total loss of access (*atkirtimas* 'cut-off') and interruptions in service availability (*aptarnavimo trikdymo ataka* 'service disruption attack', *trikdžiai* 'disruptions').

For Concept 4 ‘MitM attack’, the two proposed descriptive multi-word expressions have different lexical structures, highlighting different aspects of the concept: *neteisėtas žinutės perėmimas* (‘unauthorised interception of a message’) highlights the act of unlawfully accessing a message during transmission, while *konfidencialumo pažeidimas* (‘breach of confidentiality’) highlights the result of that act – the violation of data privacy and exposure of sensitive information.

For Concept 5 ‘brute force attack’, the respondents proposed seven descriptive multi-word expressions, all of them having the same head with the meaning ‘attack’. However, their modifiers differ. Five of the designations include the modifier with the meaning ‘password’ and a modifier denoting various activities directed toward a password (intercepting, guessing, generating) or attributes of a password being attacked (security): *slaptažodžių perėmimo ataka* ‘password interception attack’, *slaptažodžių spėjimo ataka / slaptaždžių spėliojimo ataka* ‘password guessing attack’, *slaptažodžių generavimo ataka* ‘password generating attack’, *slaptažodžių saugumo ataka* ‘password security attack’. One proposal highlights the generating algorithm of the software (*generatoriaus ataka* ‘generator attack’), while the last one focuses on how the generation is performed (*tiesioginė variantų perrinkimo ataka* ‘direct variant reselection attack’).

For Concept 6 ‘phishing’, two descriptive designations were proposed, both referring to the method of the attack – social engineering. One designation states this explicitly (*masinė socialinės inžinerijos ataka* ‘massive social engineering attack’), while another conveys the same idea in a concise compound – *socataka* ‘social attack’.

For Concept 7 ‘botnet’, two descriptive designations explicitly denote the devices and their unauthorized control: *neteisėtai valdomų kompiuterinių/skaitmeninių įrenginių tinklas* (‘network of illegally controlled computer/digital devices’), while one designation focuses only on the control aspect: *užvaldytas tinklas* (‘controlled network’).

Similarly, for Concept 9 ‘honeypot method’, one proposed descriptive designation is especially accurate, indicating several aspects of the method (*saugumo modeliavimo imitacijos metodas* ‘security modelling simulation method’), while another briefly highlights the aim of the method – *apgaulės metodas* ‘deception method’.

For Concept 10 ‘zero-day vulnerability’, one of the proposed descriptive designations highlights the product with the vulnerability: *produkto pirminis pažeidžiamumas* (‘the product’s primary vulnerability’). Other descriptive designations emphasise the nature of the vulnerability. Since a zero-day vulnerability refers to a security flaw that has been disclosed but not yet patched, some designations focus on its recent discovery (*ką tik nustatyta kibernetinė spraga* ‘gap that has just been detected’, *naujas pažeidžiamumas* ‘new vulnerability’), while others highlight its unmanaged state (*nežinoma spraga* ‘unknown gap’, *nenustatyta saugumo spraga* ‘security gap that has not been detected’, *laiku neaptikta spraga* ‘gap that has not been detected in time’). Some of the designations of the latter type may be misleading, as a zero-day vulnerability is not necessarily unknown; rather it is known but still unpatched.

Borrowed Designations

Borrowed designations hold the third position, comprising a total of 10 proposals. They vary in their degree of localisation and can be grouped into two groups: localised/semi-localised borrowings and unlocalised borrowings.

The localisation of the designations of the first group differs, e.g. the designation of Concept 2 ‘spam’: *spemas* has the Lithuanian ending and adapted spelling to match the Lithuanian pronunciation, while the designation of Concept 9 ‘honeypot method’: *honeypotas* has only the Lithuanian ending added. Two borrowings are formed by adding the Lithuanian suffixes and endings to the English abbreviations: Concept 3 ‘DoS attack’: *dosinimas* (suffixes *-in-* and *-im-* and ending *-as*), *DOSas* (ending *-as*). Two multi-word borrowings incorporate English abbreviations as modifiers: Concept 4 ‘man-in-the-middle attack’: *MiM ataka*; Concept 5 ‘brute force attack’: *BF ataka*.

The designations of the second group of borrowings are original English words. Two of them differ from the English equivalents given in the survey, likely reflecting the associations triggered by the concepts for the respondents: Concept 5 ‘brute force attack’: *determination*; Concept 7 ‘botnet’: *Skynet*. The two remaining designations coincide with the English equivalents given in the survey, suggesting that the respondents would like to have the Lithuanian term as close to the English equivalent as possible: Concept 10 ‘zero-day vulnerability’: *zero-day, zero-day vulnerability*.

One of the provided examples is a combined designation comprising a descriptive constituent (*duomenų viliojimas* ‘data seduction’) and a borrowed constituent – the original English term in standard Lithuanian quotation marks („*phishing*“): Concept 6 ‘phishing’: *duomenų viliojimas „phishing“.*

Inaccurate Designations

16 designations are inaccurate as they do not accurately represent the concepts presented in the survey. Some of them, while being inventive, actually designate similar concepts, but these concepts belong to a different concept class, e.g. for Concept 4 ‘botnet’, the designations *nuotolinė kompiuterinių tinklų ataka* ‘remote attack of computer networks’, *programinio kodo ataka* ‘programme code attack’, *zombinimas* ‘zombieing’ are provided. These designations refer to activities, whereas the concept belongs to the entity class. Similarly, the designation *vidurnakčio ataka* ‘midnight attack’ provided for Concept 10 ‘zero-day vulnerability’ denotes an activity, while the concept itself falls under the entity class.

Conclusion

The conducted research leads to the following conclusions:

1. Distribution of proposals across respondent groups and individual concepts: Notable differences were observed both across respondent groups and individual cybersecurity concepts. In the Students vs. Graduates segmentation, graduates submitted significantly more responses with term proposals than students (35% vs. 65%), and in the General Public vs. Experts segmentation, experts contributed more than the general public (38% vs. 62%). Certain concepts also elicited considerably more proposals than others, ranging from 1 to 26, indicating that while some concepts have widely accepted designations, others remain terminologically unstable and invite alternative proposals.
2. Designation formation patterns and their distribution across respondent groups: The majority of proposed designations were metaphorical (52%), followed by descriptive (25%) and borrowed ones (8%), indicating a preference for metaphorical naming, likely because it facilitates the expression of complex concepts by linking them to familiar real-world associations. Most metaphorical and descriptive designations were proposed by graduates (in Students vs. Graduates segmentation) and experts (in General Public vs. Experts segmentation), whereas borrowed designations were evenly distributed between students and graduates but appeared notably more frequently among experts than the general public.
3. Tendencies in designation formation:
    - Metaphorical designations: Some metaphorical designations closely mirrored English terms, but most were original formations, drawing parallels between malicious cyber activities and various real-world domains, such as nature (bee swarms), food (meat), tools (master key), and crime (intruders, burglars, stealing), or imaginative elements, including mysterious figures and mindless creatures. Defensive cyber techniques were often associated with hunting (traps, flytraps, ambushes, and bait).
    - Descriptive designations: Lexical structures of descriptive designations varied depending on how explicitly respondents aimed to represent a concept and which characteristics they emphasised. Some designations captured several characteristics, while others focused on a single one, reflecting the varying importance respondents placed on different aspects of the concept.
    - Borrowed designations: These designations varied in their degree of localisation: some single-word proposals adapted spelling and added Lithuanian endings, while others retained English spelling adding Lithuanian endings or suffixes plus endings; multi-word proposals combined English modifiers (abbreviations) with Lithuanian headwords; and unlocalised forms remained entirely in English.
    - Inaccurate designations: A common inaccuracy observed among the proposals was confusion regarding the concept class – most notably, using activity-denoting designations to name entity concepts.

The findings of this research highlight the creative potential of Lithuanian language users in generating terminology and underscore the importance of integrating their input into the development of Lithuanian terminology, particularly in rapidly evolving domains such as cybersecurity. Future research could be expanded by the investigation of user-generated terminology across different domains, as well as by exploring how such neological activities could contribute to the education and communication of specialised knowledge.

Conflict of Interest

The author declares no conflict of interest regarding the publication of this article.

References

1 Afentoulidou, V., & Christofidou, A. (2021). It's a long way to a dictionary: Towards a corpus-based dictionary of neologisms. In Z. Gavriilidou, L. Mitits, & S. Kiosses (Eds.) Lexicography for Inclusion: Proceedings of the 19th EURALEX International Congress (Volume 2, pp. 597-606). Democritus University of Thrace.

2 Bueno, P. J., & Freixa, J. (2022). Lexicographic detection and representation of Spanish neologisms in the COVID-19 pandemic. In A. Klosa-Kückelhaus & I. Kernerman (Eds.), Lexicography of Coronavirus-related Neologisms (pp. 73-92). De Gruyter. https://doi.org/10.1515/9783110798081-005

3 Cabré Castellví, M. T., Estopà Bagot, R., & Vargas-Sierra, C. (2012). Neology in specialized communication. Terminology, 18(1), 1-8. https://doi.org/10.1075/term.18.1.01int

4 Cabré, T. (2023). Terminology: Cognition, Language and Communication. John Benjamins Publishing Company.

5 Costa, R., Ramos, M., Salgado, A., Carvalho, S., Almeida, B., & Silva, R. (2022). Neoterm or neologism? A closer look at the determinologisation process. In A. Klosa-Kückelhaus & I. Kernerman (Eds.), Lexicography of Coronavirus-related Neologisms (pp. 237-260). De Gruyter. https://doi.org/10.1515/9783110798081-012

6 Chyrvonyi, O. S. (2024). The evolution of social media language: A sociolinguistic analysis of recent neologisms. Transcarpathian Philological Studies, 35, 127-132. https://doi.org/10.32782/tps2663-4880/2024.35.22

7 Druță, I. (2013). Neology, neonymy, neosemy: Terminological perspective. In I. Boldea (Ed.), Studies on Literature, Discourse and Multicultural Dialogue. Section: Language and Discourse (pp. 749-758). Arhipelag XXI.

8 European Union. (2025). IATE: InterActive Terminology for Europe. Retrieved June 2025 from https://iate.europa.eu/

9 Guilbert, L. (1975). La créativité lexicale. Librairie Larousse.

10 Humbley, J. (2018). Term formation and neology. In J. Humbley, G. Budin, & C. Laurén (Eds.), Languages for special purposes: An international handbook (pp. 437-452). De Gruyter Mouton. https://doi.org/10.1515/9783110228014-022

11 International Organization for Standardization. (2019). ISO 1087:2019(en), Terminology work and terminology science - Vocabulary. Retrieved June 2025 from Lithuanian Academic Electronic Library (eLABa).

12 Lietuvių kalbos naujažodžių duomenynas. (2025). Retrieved June 2025 from https://ekalba.lt/naujazodziai/

13 Llopart-Saumell, E., & Cañete-González, P. (2023). Are Stylistic Neologisms More Neological? A Corpus-Based Study of Lexical Innovations of Women and Men. Languages, 8(3), Article 175. https://doi.org/10.3390/languages8030175

14 Mikelionienė, J. (2025). Neonyms in the database of Lithuanian neologisms: Probability and reality. In Proceedings of the 1st International Workshop on Terminological Neologisms Management (NeoTerm 2025). CEUR Workshop Proceedings, 3972. Retrieved June 2025 from https://ceur-ws.org/Vol-3972/

15 Miliūnaitė, R. (2020). Neologijos terminija ir "Lietuvių kalbos naujažodžių duomenyno" praktika. Terminologija, 27, 81-107. https://doi.org/10.35321/term27-04

16 Mockienė, L. (2016). Formation of terminology of constitutional law in English, Lithuanian and Russian (Doctoral thesis, Mykolas Romeris University).

17 National Institute of Standards and Technology. (n.d.). Glossary. Computer Security Resource Center. Retrieved June 2025 from https://csrc.nist.gov/glossary

18 Rackevičienė, S., & Utka, A. (2024). Preferences of Lithuanian cybersecurity synonymous terms in different user groups. Kalbų studijos / Studies about Languages, 44, 107-122. https://doi.org/10.5755/j01.sal.1.44.36235

19 Sánchez Ibáñez, M., & Pérez Sobrino, P. (2024). Name it till you mean it: Intersections between formal and semantic neological procedures in naming emerging pandemic objects in Spanish. Language & Communication, 99, 274-288. https://doi.org/10.1016/j.langcom.2024.10.010

20 Skubis, I., Wodarski, K., & Boch, A. (2023). Language in the human-technology era. New terminology on the sex (robot) market - "digisexuality," "technosexuality" and "robosexuality" - a multilingual analysis and survey among students. Scientific Papers of Silesian University of Technology. Organization and Management Series, No. 189, 553-572. https://doi.org/10.29119/1641-3466.2023.189.35

21 Styshov, O. (2022). Neologisms of the military sphere in the modern Ukrainian language. LOGOS, 113. https://doi.org/10.24101/logos.2022.79

22 Szymańska, M. (2025). Linguistic creativity on digital platforms: Exploring neologism motivation on social media. Language & Dialogue. Online First. https://doi.org/10.1075/ld.00218.szy

23 Wolfer, S., & Klosa-Kückelhaus, A. (2023). Tracking the acceptance of neologisms in German: Psycholinguistic factors and their correspondence with corpus-linguistic findings. Humanities and Social Sciences Communications, 10(1), Article 547. https://doi.org/10.1057/s41599-023-01977-4

Santrauka

Sigita Rackevičienė.

Terminų kūrimas kibernetinio saugumo srityje: skirtingų vartotojų grupių pasiūlymai

Šiame darbe tęsiama terminologinės lietuvių kalbos vartotojų apklausos duomenų analizė, kurios pirmoji dalis paskelbta Rackevičienės ir Utkos (2024) straipsnyje. Minėtoje apklausoje dalyvavo 593 respondentai, priklausantys įvairioms amžiaus grupėms ir turintys skirtingą profesinę patirtį. Respondentų buvo prašoma įvardyti tinkamiausius lietuviškus terminus 10-iai kibernetinio saugumo sąvokų. Respondentai galėjo rinktis terminus iš pateiktų sinoniminių terminų sąrašų arba siūlyti savo sukurtus terminus bei pagrįsti savo pasirinkimus.

Ankstesniame straipsnyje buvo analizuojami kategoriniai duomenys, gauti iš pateiktų terminų sąrašų, o šis straipsnis nagrinėja tekstinius duomenis – respondentų pasiūlytus terminus. Atlikus kiekybinę ir kokybinę analizę, nustatyta, kurios respondentų grupės buvo produktyviausios siūlydamos terminus, kokioms sąvokoms pasiūlyta daugiausia terminų, kokie terminų darybos modeliai vyravo respondentų pasiūlymuose bei kokios darybos tendencijos būdingos kiekvienam modeliui.

Tyrimo rezultatai rodo, kad respondentai 126 kartus pasinaudojo galimybe pasiūlyti savo sukurtus terminus ir iš viso pateikė 119 skirtingų leksinių vienetų šios srities sąvokoms pavadinti, o tai liudija jų domėjimąsi terminija ir norą prisidėti prie jos plėtojimo. Tyrimas taip pat atskleidė svarbiausius siūlomų terminų darybos modelius, tarp kurių vyravo metaforinių terminų modelis, antrą poziciją užėmė aprašomųjų (tiesiogiai nusakančių sąvokos požymius), o trečią – pasiskolintų terminų modeliai. Detali kiekvieno modelio analizė atskleidė išradingas darybos strategijas, kurias respondentai taikė, kurdami savo terminų pasiūlymus. Tyrimo rezultatai rodo lietuvių kalbos vartotojų didelį kūrybinį potencialą, kuris gali tapti svarbiu indėliu, kuriant lietuviškus naujadarus, ypač tokiose sparčiai besivystančiose srityse kaip kibernetinis saugumas.

About the Authors

SIGITA RACKEVIČIENĖ

Professor at the Institute of Humanities at the Faculty of Human and Social Studies, Mykolas Romeris University, Vilnius, Lithuania

Research interests

Multilingual terminology (its conceptual, linguistic and pragmatic dimensions), terminography, corpus linguistics, computational linguistics

Address

Institute of Humanities, Faculty of Human and Social Studies, Mykolas Romeris University,
Ateities st. 20, LT-08303 Vilnius, Lithuania

E-mail

sigita.rackeviciene@mruni.eu

Orcid ID

0000-0001-5794-0296