Form – Meaning – Usage Synergy in LSP & Professional Communication: Computer Security in Terms of Frame Semantics

Ekaterina Isaeva, Olga Baiburova & Oksana Manzhula

Abstract This article deals with computer security terminology from the perspective of Fillmore's frame semantics. Cognitive linguists have proved that semantics is realised in context and contributes to cognition. This article aims to analyse which semantic roles are prevalent for using computer security terms in context. Our evidence proves that the term's meaning and semantic role in the frame corresponding to a communicative event are interrelated. The research has been carried out on a manually collected corpus of computer security texts, comprising terms in their contexts. The data are analysed as follows. First, a thematic categorisation of terms is carried out. Then semantic frame modelling is applied. After that, we generalise our findings and achieve sufficient abstraction in the conclusion about the presence of form – meaning – usage interdependence in professional discourse and LSP. Finally, we discuss the place of semantic framing in the multimodality of professional communication regarding the logic and philosophy of language.

Keywords computer security discourse, LSP, professional communication, semantic framing, semantic role, transdiscursive communication

1 Introduction

We present a study of computer security (CS) terminology, carried out within a project "Special Knowledge Mediation by Means of Automated Ontological and Metaphorical Modelling". The project aims to find effective ways to transfer, receive, process, and store specialised knowledge. This knowledge is acquired through professional experience, stored as mental models, and represented via a language for specific purposes (LSP). All these are integral components of professional communication, and each of them is crucial for successful knowledge transfer and acquisition.

This article examines form – meaning – usage interdependence in professional discourse. As we showed earlier (Isaeva 2019: 81), accidental cognitive framing of specialised concepts in transdiscursive (between experts and nonexperts) professional communication can cause significant loss of transferred information. Therefore, finding interdependence between grammar, semantics, and pragmatics, referred to as form, content, and usage, respectively, will be helpful in deliberate cognitive framing for enhancing professional communication. Additionally, the findings can be applied for text-mining and machine learning as far-sighted goals. Thus, the results, which tackle different aspects of linguistics, applied to the specific field of professional communication, i. e., CS, could be of interest to those involved in the studies of structural and derivational grammar, semantics, syntax, discourse, cognitive and computational linguistics, terminology, and mediation.

Zitiervorschlag / Citation:
Isaeva, Ekaterina / Baiburova, Olga / Manzhula, Oksana (2022): „Form – Meaning – Usage Synergy in LSP & Professional Communication: Computer Security in Terms of Frame Semantics." *Fachsprache. Journal of Professional and Scientific Communication* 44.3–4: 169–191.

We have compiled and examined a collection of the CS terms and a corpus of LSP texts contextualising the terms. The database is built as an integral corpus of texts centred around selected terms. This is relevant to take them inseparably, for the terms' semantic frames can be reconstructed only within their context. For this reason, in this paper, we will refer to this combination as the corpus of terms. We collected the corpus within a project on an interdisciplinary terminological dictionary development. The project is ongoing at the Department of English for Professional Communication of Perm State University and is included in an ESL course for non-linguistic faculties. The second-year CS students have collected the corpus used for our research. During the course (1 academic year), the students had a monthly task to read contemporary specialised texts, including journal articles, books, and documentation on computer virology and select words, which had a specific meaning in CS. The students worked in one document shared for editing via Google sheets to collect unique terms. The terms have been stored with their contexts and supplied with specialised definitions by CS experts. The terms have been sorted into predefined thematic categories according to their contextual meaning, i. e., the meaning realised in the context of a professional communication event: *Virus type, Malicious activity / Malefactor, Software, Hardware, Vulnerability, Operating systems, Safeguard measures, Computer networks, Mathematics / Functions, Data,* and *Programming languages*. We have selected only nominative terms, i. e., nouns and noun groups. A noun group is "a group containing at least one noun or pronoun (the head) and often other items such as determiners, adjectives, and prepositional phrases" (The Free Online English Dictionary), e. g., *computer virus*. So, the nominative terms made up a subcorpus of 355 units.

We aim to analyse which semantic roles (SRs) are prevalent for CS terms in context. We use the semantic frame modelling method, which consists in assigning Fillmore's SRs to the participants of an event or situation in professional communication.

2 Background knowledge and current vistas of semantic framing

Katsnelson believed that the word form and the mental content are given in the language in a complex and contradictory unity. To reveal their dialectics means to trace the transitions from the meanings of words to concepts and from grammatical categories to categories of thought (Katsnelson 2010: 397). This idea correlates with the theory of a bilateral sign, i. e. the relationship between 'the signifier' (a linguistic form) and 'the signified' (the meaning of the form) (Saussure 1959). The dichotomy of language and thinking was examined by von Humboldt, who believed that the forces that generate language and thought are inseparable (Humboldt 1984: 305), and Sapir-Whorf, who stated that a person's picture of the world is primarily determined by the system of the language he speaks (Whorf 1956).

The language grammatical system preserves the structural nature of human consciousness and reflects the natural world in a folded and syncretic state (Solomonick 2011: ii–iv) formalised to semantic frames. The frame comprises elements assigned with standardised SRs (Fillmore 1971). We apply this logic to specialised texts, which preserve the grammatical structure of the language but are filled with specialised lexics, capable of evoking abstract descriptions of professional situations through semantic frames (L'Homme 2017: 8).

Fillmore's theory has been comprehensively studied and implemented in computational linguistics. The theory's potential is evident in natural language processing and machine learning due to its aptitude for standardisation and categorisation. Furthermore, the labelling of SRs provides an easy way to conceptual modelling and, thus, conceive the logic and the mechanism

of thinking. Due to its rule-based nature, this ability is scaled to artificial thinking, crucial for natural language processing and machine learning.

The task of mapping word tokens to frames they evoke, and for each frame, finding and labelling its argument phrases with frame-specific SRs, is well developed on the technical side. However, there is still a problem related to a small amount of manually pre-trained data for supervised training to achieve precise automatic parsing (Kshirsagar et al. 2015: 218).

Impressive results in frame semantics have been achieved by Faber/Cabezas-García (2019) and the LexiCon Research Group (2021), who elaborated efficient methods for parsing, lexicon building, and semiautomated extraction of metaphor-related terms in the environmental domain. However, the domain of CS lacks well-elaborated automatic semantic parsing, and there is a demand for manual semantic research underpinning automatic parsing.

3 Proving evidence for form – meaning – usage synergy

3.1 Logic of the analysis

SRs are the roles that a noun phrase (NP) may play with respect to the action or state described by a governing verb (V), commonly the sentence's main verb. An SR is "a part of the predicate semantics that reflects the general properties of the predicate argument" (Plungian 2003: 3). For instance, in 'a virus infected the computer', *infected* is the predicate, while *virus* and *computer* are the predicate arguments. Establishing relations between the predicate and its arguments allows for formal semantic analysis of the meaning underlying the utterance based on the SRs labelling of NP+V units. To illustrate how meaning unveils in the discourse, i. e. in usage, and is determined by grammar and syntax represented in SRs, i. e. form, we apply semantic framing on our sample corpus. The labelling has been done manually to all the term parts of NP+V units regarding the basic features of the SRs.

We concentrated on the SRs traditionally singled out in the frame semantics: Agent, Counteragent, Objective, Perceptive, Cause, Benefactive, Addressee, Patient, Result, Locative, Trajectory, Instrument, and Goal. Additionally, we suggest new SRs, namely Specifier (cf. section 3.2) and quasi-Agent (cf. section 3.14), especially relevant for specialised discourse. Since we are interested in the pragmatic conditionality of word meanings, we apply the principle of SR's labelling to the terms in their contexts and infer the interdependence between the SRs and the terms' categories. So, the logic of our analysis includes the following steps: 1) an SR description; 2) sample analysis, i. e., determining an SR in the term's NP+V unit based on their semantic meanings retrieved from dictionary definitions; 3) inferences on the role–category interrelations. To obtain the meaning of the term, we used official corpus-based dictionaries, such as "The Free Online English Dictionary" from Macmillan Publishers and "The Longman Dictionary of Contemporary English Online"; the collection of dictionaries by subject, e. g., "The Free Dictionary" by Farlex or other published professional sources (books, articles, etc.) and professional IT and CS encyclopaedias or fora, e. g. "Techopedia" defining novel terms not registered in the official dictionaries.

3.2 Pragmatic potential of the Agent

The Agent is one of the leading SRs, an active participant, i. e. a person, a subject, an animated pathogen, or a natural force performing an action or exercising control over the situation

(Fillmore 1968: 24, Cook 1998: 5). Such nouns as *heat* and *wind*, being inanimate but representing objects that can act, are also considered the Agents (Chafe 1970: 7). In CS, the Agent is generally introduced by inanimate nouns, which designate entities capable of operating on themselves or others, "usually to bring about some change in the location or properties of itself or others" (Downing/Locke 1992: 5). Thus, the Agent's typical characteristic features, such as animation, intent, motivation, and responsibility, are attributed to inanimate professional concepts.

In our corpus, the Agent comprises the terms belonging to the *Malicious activity / Malefactor* category (11 cases). The less represented categories include *Virus type, Software, Hardware, Vulnerability, Operating systems* (Figure 1).

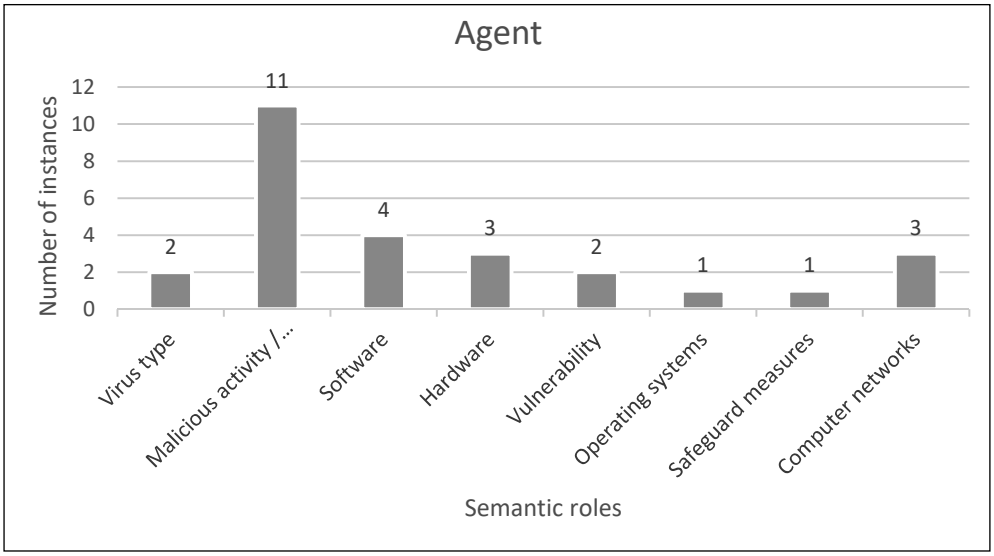

Figure 1: Distribution of the Agent role in the CS discourse

An example of the Agent played by the term designating a virus type is given in (1):

(1) The *Trojan* keeps records of the checksums for the obtained data. (Mamedov/ Sinitsyn 2016)

Sample (1) illustrates the capability of *the Trojan*, i. e. "a program that seems useful but is designed to be harmful, for example by stealing or destroying information" (The Free Online English Dictionary), to perform intelligent actions such as *keeping records*.

The verbs expressing the Agents' actions contain the semes of animacy, activeness, and deliberateness:

- *attempt*, i. e. "to make an effort to achieve or complete (something difficult)" (English Dictionary, Thesaurus & Grammar Help),
- *download*, i. e. "to move information to your computer from another computer system or the Internet" (The Free Online English Dictionary),
- *bypass*, i. e. "avoid dealing with someone or something, especially because you think you can achieve something more quickly without using them" (The Free Online English Dictionary),

- *target*, i. e. "intend or try to attack someone or something" (The Free Online English Dictionary),
- *keep records*, i. e. "to regularly record written information somewhere" (The Longman Dictionary).

All these activities are typical of humans. They comprise the idea of reaping the benefit, putting it into practice, implementing, etc. These verbs designate the activity typical of malware. They have negative connotations and deliver the meaning of over-persuading, instigating, and involving in some troublesome business.

Terminological categories of *Malicious activity / Malefactor* and *Software* designate the programs, whose prototypes, i. e. their biological counterparts, are pathogen agents, propagating, spreading, and causing infectious diseases. All these imply agency as the ability to act as the initiator of some action.

Although SRs are primarily concerned with the semantic relations of the arguments and their predicates, their syntactic relations cannot be neglected. These relations are described through the argument's position relative to its predicate and the part of the sentence the argument occurs in. This is particularly relevant if the study results are to be used in automatic parsing. Suppose semantic and syntactic properties of the instigator of the action disagree, e. g. in sentences with the passive structure. In that case, it makes sense to think of introducing quasi-roles[1], here quasi-Agent, which will contribute to the precision of the data description and rules formulating to achieve a higher quality of automatic parsing. In our corpus, the terminological categories that represent this quasi-role include *Malicious activity / Malefactor* and *Software*, for example:

(2) Spain and Poland have been two countries traditionally targeted by *SMS scams* and similar *malware*. (GReAT 2017a)

The term *SMS scam* refers to malware ("any software that brings harm to a computer system" [Techopedia]), which occurs when cybercriminals use false text messages asking customers to provide personal or financial information. Both terms (*SMS scam* and *malware*) execute the action denoted with the verb *target*, typical of the Agent. The preposition *by* shows that the participant following it is active and is the initiator of the action. Yet, the originally inanimate nature of the term and its syntactic role in the passive structure make us doubt a pure Agent role of *SMS scam* and consider it from the prism of quasi-realisation. To define the quasi-Agent role, we highlight its right-handed position regarding the predicate, the presence of the preposition *by*, preceding the argument designating the doer of the action, expressed by the predicate.

3.3 Pragmatic realisation of the 'shadow Agent'

The next SR of the Counteragent is a participant in a situation that qualifies through a counteraction relationship. The "shadow Agent" (Paducheva 2004: 361) implies "the force or resistance against which the action is carried out" (Fillmore 1971: 376) or "a substance that impedes the commission of an action" (Gak 1998: 413).

We define the Counteragent as a right-handed argument of the predicate, expressing a

[1] Here, the idea of quasi-roles is given as possible solution to the problem of syntactic-semantic mismatch in the roles distribution within the professional discourse. The aspect needs further research.

computer or cyberworld entity, action, or process which enters into counteraction relations with the Agent, i. e. the Agent acts against or prevents something unwanted expressed through the Counteragent.

In the Counteragent role, the terms from the categories of *Malicious activity / Malefactor, Safeguard measures, Software,* and *Operating systems* can be found (Figure 2).

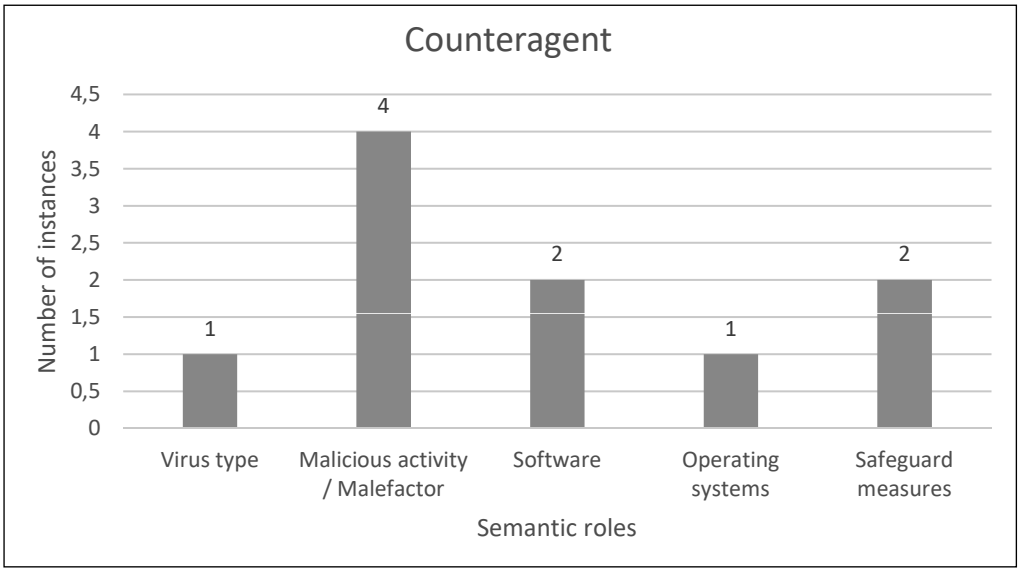

Figure 2: Distribution of the Counteragent role in the CS discourse

The most frequent category is *Malicious activity / Malefactor* exemplified in (3):

(3) If the victim successfully combats *SYN-flood*, the attacker can switch the scenario on the control panel and evaluate the victim's reaction. (Makrushin 2017)

The term *SYN-flood* stands for "a type of network or server degradation attack in which a system sends continuous SYN requests to the target server to make it overconsumed and unresponsive" (Techopedia). This action is malicious, for it causes soft- or hardware malfunction or information security breach. When taking countermeasures against such kinds of activities, the most likely verbs to deliver them are

- *combat*, i. e. "do something in order to try to stop something bad from happening or a bad situation from becoming worse" (The Free Online English Dictionary),
- *prohibit*, i. e. "officially stop something from being done, especially by making it illegal" (The Free Online English Dictionary),
- *disable*, i. e. "deliberately make a machine or piece of equipment impossible to use" (The Longman Dictionary),
- *attack*, i. e. "deliberately use violence to hurt a person or damage a place" (The Longman Dictionary).

These verbs imply carrying out deliberate actions against something, being part of countermeasures. They also comprise the meaning of preventing something from happening, fighting or destructing. The actions are usually executed against something unwanted.

3.4 Pragmatic diversity of the Objective

The Objective is an item, "the action is directed to" (Cook 1998: 5), affected by the action (Fillmore 1968: 25). The Objective usually acts as a direct complement and "the object that is exposed by the verb" (Downing/Locke 1992: 5). All these features bring us to the following definition of the Objective – a right-handed argument of the predicate expressing a computer or cyberworld entity manipulated by someone or something defined by the argument. However, the entity does not change or cease existing as a result of this manipulation.

In CS, the Objective is rather heterogeneous regarding terminological categories (Figure 3):

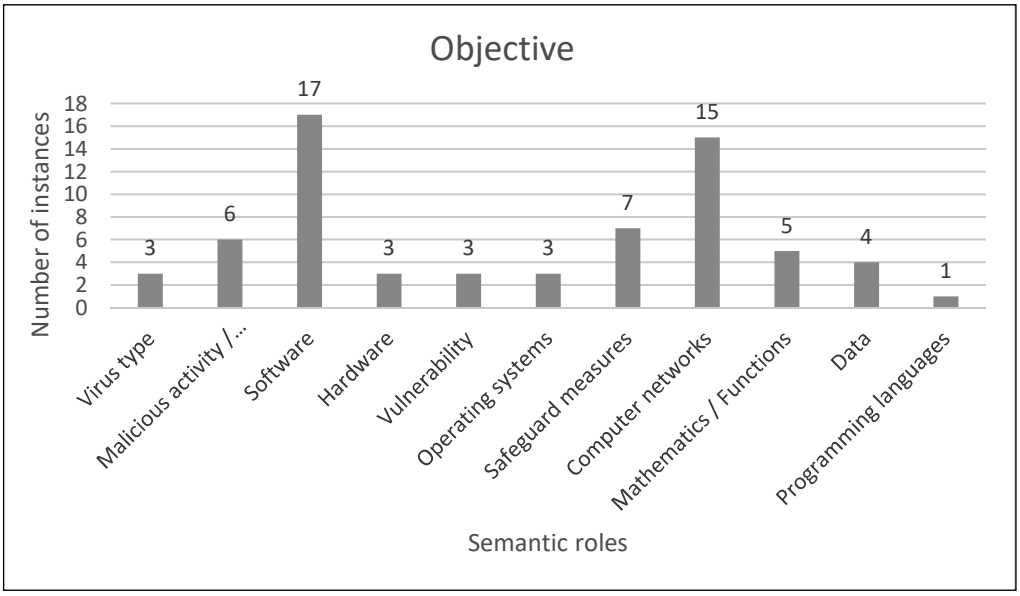

Figure 3: Distribution of the Objective role in the CS discourse

The most typical categories are Software and Computer networks. The Objective is often implemented by terms denoting: mechanisms, tools, operations, network clients, software, and malware, like *malicious code*, i. e. "a code causing damage to a computer or system" (Techopedia), as in (4):

(4) A vulnerability is a fault in a program's implementation that can be used by attackers to gain unauthorised access to data, inject *malicious code* or put a system out of operation. (Zakorzhevsky 2015)

Among the verbs conveying this SR are *include*, *receive*, *download*, and *check*. They are used with the terms of the *Software* category due to the common seme of object manipulation inherent in these verbs. They imply moving something from one location to another, holding something, and the presence or quality testing.

The categories of *Software* and *Computer networks*, primarily referring to the software part of the networks, are significant for the Objective because programs are engaged in different kinds of activities, including the network ones, carried out by some other participants but do not usually undergo any changes.

3.5 Tangibility of the computer security Perceptive

The Perceptive is "an integral semantic attribute for right-handed arguments of most sensory verbs" (Amirova 2002: 119). This SR indicates that the object is perceived by the Agent through physical senses. This act of perception usually evokes emotions or cognitive change in the Agent.

The Perceptive is provided by the terms of *Virus type, Malicious activity / Malefactor, Software, Hardware, Vulnerability, Operating systems, Safeguard measures,* and *Computer networks* (Figure 4).

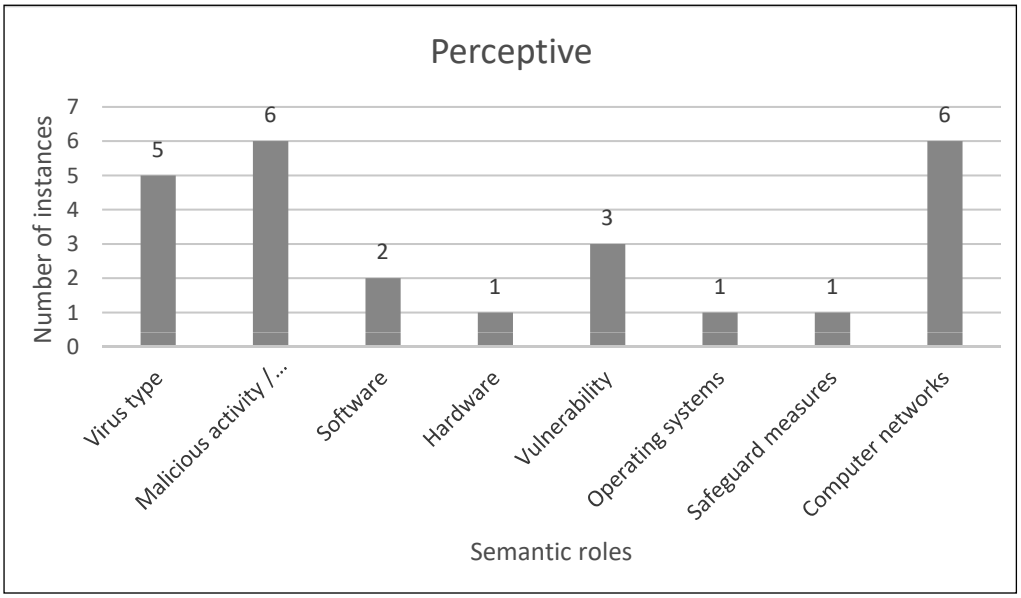

Figure 4: Distribution of the Perceptive role in the CS discourse

The most substantial categories are *Malicious activity / Malefactor, Computer networks,* and *Virus type*. The Perceptive is played by the following subcategories: kinds of law breach, techniques or attack vectors, computer programs, attack scenarios, and processes, like *leak*, i. e. "the origin of secret information that becomes known, or the act of making it known" (Cambridge Dictionaries Online), as in (5):

(5) These are focused on analysing single apps to detect information *leaks* through inter-component communications, ICC. (Blasco/Chen 2018)

The verbs that appear in CS texts to convey the relations between the Agent and the Perceptive are *detect*, *identify, consider, hear about*, etc., which mean perceiving something, making it evident, and finding. The Perceptive can also be highlighted by the words *remind*, *like*, *similar to*, *under the veil*, and others, which express comparison with some object or process, determining identity, matching unique features. These words signal the attempt of the entity behind the Agent to precept or cognise the entity expressed by the Perceptive.

The dominance of the categories of *Malicious activity / Malefactor, Computer networks,* and *Virus type* can be explained by the fact that the CS concepts designated by the terms of these categories are still to be understood, recognised, and conceptualised by the user, who can

do nothing but observe the malicious acts, which are primarily executed in or via computer networks.

3.6 Connotative specificity of the Cause

The Cause's function is "to lead to a change in the state of Affected Participant" (Downing/Locke 1992: 25). The participant in the Cause role expresses the reason for the state occurrence or change.

Though the Cause is exemplified by the terms belonging both to the categories of *Malicious activity / Malefactor* or *Virus type* and *Safeguard measures* or *Software*, it always bears a negative connotation. In (6), *OPSEC* (*Operations Security)* involves the identification and protection of generally unclassified critical information or processes that a competitor or adversary can use to gain real information when pieced together (Unuchek 2017). It designates the process thought to safeguard data. However, in practice, it contributes to the growth of illicit business and crime:

(6) Due to its robust anonymity, *OPSEC* techniques, low prices, and client-oriented strategy, the Dark Web remains an attractive medium for conducting illicit businesses and activities. (Unuchek 2017)

Consistency checks in (11) denote "a test performed to determine if the data has any internal conflicts" (Computer Hope) but, due to their co-occurrence with the negatively connotated adjective *insufficient,* represent the cause of unwanted actions:

(7) He has reported a number of serious vulnerabilities: Remote Code Execution from web scripts, arbitrary device firmware modification due to insufficient *consistency checks* ... (Threat intelligence report for the telecommunications industry 2016)

The Cause markers are the prepositions *due to* and *because of*, which indicate a cause-and-effect relationship between the participants and the events and express neutral and negative meaning. This property correlates with another feature of the Cause mentioned above, i. e. the usage of adjectives like *insufficient*, *poor*, *inadequate*, *wrong*, *improper,* or the terms, like *Trojan*, *malware*, *adware*, both with a negative connotation. The Cause helps the reader understand why a particularly adverse effect occurs.

3.7 The search for the Benefactive of the computer security issues

The Benefactive, means "the possession of an object with state verbs or a participant in the transfer of information with procedural and action verbs" (Cook 1998: 151). The Benefactive is "an object for which an action is performed" (Downing/Locke 1992: 152), "a person or object that receives something as a result of an action" (Brinton 2000: 82), but "it is not necessary to receive benefits" (Downing/Locke 1992: 152). Beneficial verbs denote the possession or transfer of property. Despite their generally positive connotation, the case, often associated with the Dative, can be positive and negative, i. e. a person can gain or lose the property. This fact brings us to further deliberations, outside the scope of this paper, about splitting this SR into three, namely expressing positive, negative, and neutral influence. In our corpus, the Benefactive occurs with such verbs as *have, possess, inherit, give, fetch, buy, cook (make),* etc.

The Benefactive is carried out by the terms of *Malicious activity / Malefactor, Software, Safeguard measures,* and *Computer networks*. The distinctive feature of the SR is the preposition *for*, which helps to express the idea that some actions open new functions to the notions following this preposition. In CS, the implications might be either positive or negative for the user. In (8), the work of a particular method enables *Internet Explorer* to become a medium for malicious activity:

(8) Since this method only works for *Internet Explorer*, the malware needs to force the user to access internet banking via that browser. (Marques 2016)

The fact that the Benefactive is exemplified by the terms of the categories *Malicious activity / Malefactor, Software,* and *Safeguard measures,* and *Computer networks* can be explained by the peculiarities of the CS discourse, where a lot of efforts are taken to improve computer and communication protection or, vice versa, malware.

3.8 Pragmatic function of the Addressee

The Addressee is the person to whom the action is directed (Apresjan 1995: 25). In the Addressee role, we have identified only two terms belonging to the categories of *Computer networks* (14) and *Malicious activity / Malefactor* (15). This SR is played by the terms, designating network software, like *remote server* in (9) or *the money mule's cell phone number* in (10).

(9) The stolen Paypal credentials were forwarded to another *remote server* located in Mexico. (Naor/Alon 2016)

A remote server is "a server that is dedicated to handle users that are not on the LAN but need remote access" (What is a remote server 2017). This term belongs to the Computer networks category. In (9), *the remote server* acts as a personified addressee to which an object (here *credentials*) is forwarded. Personification and anthropomorphism of software and hardware is a widespread phenomenon found throughout in the CS discourse (Isaeva/Baiburova/Manzhula 2022). The *remote server* occurs in the frame, which evokes a mental construction of the event of human-to-human interaction, namely forwarding something from one person to another. This is a case of the metaphor representing a behavioural comparison.

(10) The attacker issues a money transfer to *the money mule's cell phone number*. (GReAT/Naor 2016)

Here, we witness an example of anthropomorphism in the CS concepts, which arises within the 'transfer to' frame. The Addressee is the money mule's cell phone number, i. e. the cell phone number of a person allowing their account to be used to receive fraudulent funds and then withdrawing the money on behalf of a fraudster ("Gang of fraudsters and 'money mules' sentenced for £200k scam" 2019). The CS event triggers the metonymic transfer of the money mule's intimateness and their SR to the number of cell phones used in the malicious activity. In the frame of a typical CS event, the Addressee is attributed to some device, hardware, a user, or any victim of a malefactor which receives some malware or fraudulent item.

3.9 A computer security Patient as the Object exposed to change

The Patient is "the recipient the impact is directed to and whose physical state, including position in space, changes as a result of this situation" (Fillmore 1968: 68). It refers to "a person or object exposed and undergoing a change" (Brinton 2000: 22). This SR is illustrated by the groups of terms determining *Software, Operating systems,* and *Computer networks* since they are the primary targets for manipulation and change by the malefactor using the malware, e. g. (11):

(11) The attackers try to avoid an early detection due to wrong timeserver settings, since the current *NTP Server entry* will be overwritten by the previous malicious requests. (Ortloff 2016)

NTP Server entry is a record of the server location, which refers to a "protocol used to synchronise computer clocks across data networks" (Techopedia). The term denotes data communication rules exposed to manipulation and change. They can be expressed in language by such verbs as

- *configure,* i. e. "to arrange something or change the controls on a computer or other device so that it can be used in a particular way" (Cambridge Dictionaries Online),
- *overwrite,* i. e. "replace a computer file with a different one" (Cambridge Dictionaries Online),
- *disable*, i. e. "permanently or temporarily turn off" (Computer Hope).

The verbs' semantics contains the semes of change and influence. The terms of the groups of *Software, Operating systems,* and *Computer networks* occur as the Patient for they determine computer items prone to manipulations, unable to influence the event causing their alterations.

3.10 Types of the Result of the computer security activities

The Result is "an object or creature arising from an action" (Fillmore 1968: 25). The SR comprises the terms of *Virus type, Malicious activity / Malefactor, Software, Operating systems, Safeguard measures, Computer networks, Data* (Figure 5).

The distinctive groups are *Software, Virus type,* and *Malicious activity / Malefactor*. The terms can designate attacks, forms of cybercrime, computer operations, and software, e. g. (12):

(12) They created an illegal *add-on* to the legal RBS product. (Stoyanov 2016)

The Result is delivered with the verbs:

- *create*, i. e. "to make something new or original that did not exist before" (The Free Online English Dictionary),
- *implement*, i. e. "to carry out; put into action" (Collins),
- *develop*, i. e. "to invent something or bring something into existence" (Cambridge Dictionaries Online),
- *cause*, i. e. "to produce a result" (Your Dictionary),
- *perform*, i. e. "to do an action or piece of work" (Cambridge Dictionaries Online).

These verbs contain the seme of producing something.

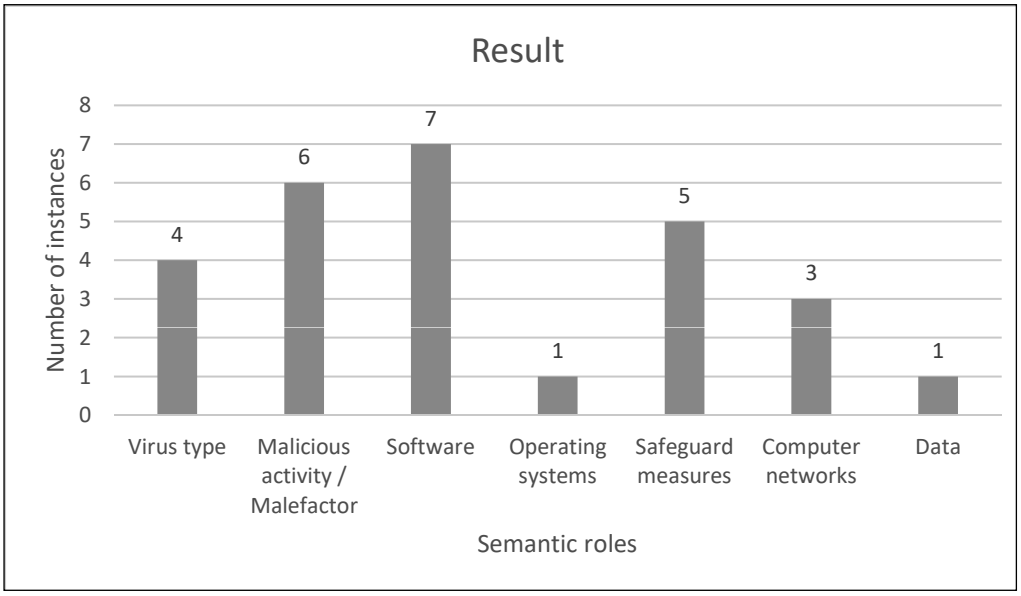

Figure 5: Distribution of the Result role in the CS discourse

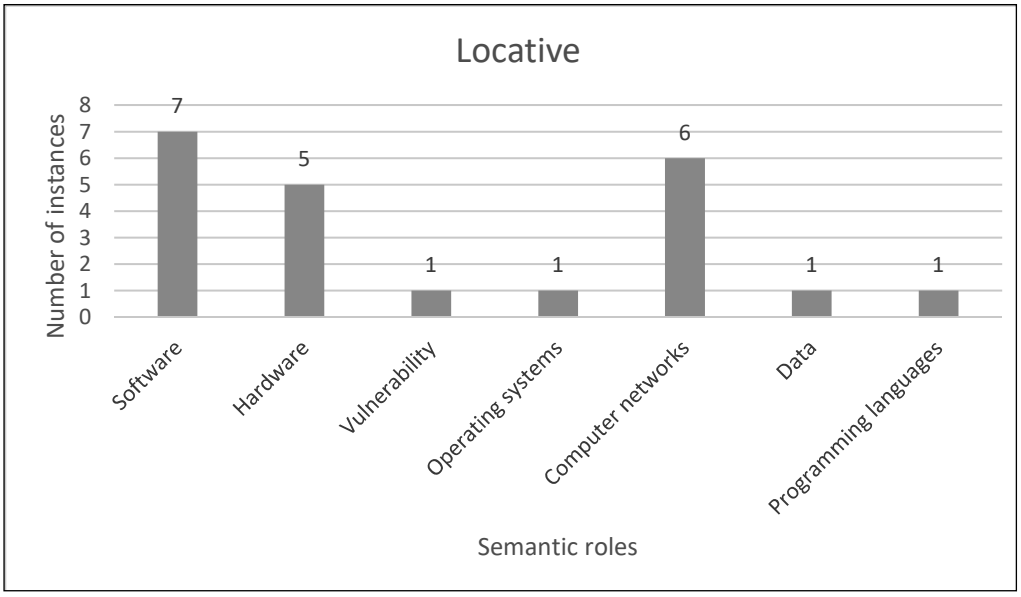

Figure 6: Distribution of the Locative role in the CS discourse

3.11 Spatial orientation: Locative

The Locative is the place of action, physical location, or spatial orientation (Fillmore 1968: 25; Cook 1998: 127). This case has two types, indicating the state and direction.

The Locative is provided by the terms of *Software, Hardware, Vulnerability, Operating systems, Computer networks, Data,* and *Programming languages* (Figure 6).

Most of the terms determine computer networks, protocols, traffic, types of websites, terminals, and parts of a computer; e. g. *hard drive* in (13), i. e. "the part of a computer where information and programs are stored, consisting of hard disks and the electronic equipment that reads what is stored on them" (The Longman Dictionary):

(13) The malicious program was unusual. Unlike most other malware, it left no traces on the *hard drive* of the system attacked and worked only in the RAM of the machine. (Stoyanov 2016)

The Locative verbs include *appear, leave traces*, *write*, *find*, and *work*. Their semantics contains the realisation of some activity in a particular place, namely some electronic or digital environment.

3.12 Spatial orientation: Trajectory

The Trajectory denotes "the path in which they move from one place to another in the process of action" (Brinton 2000: 68). As the Trajectory, the terms of *Hardware, Operating systems,* and *Computer networks* appear (Figure 7).

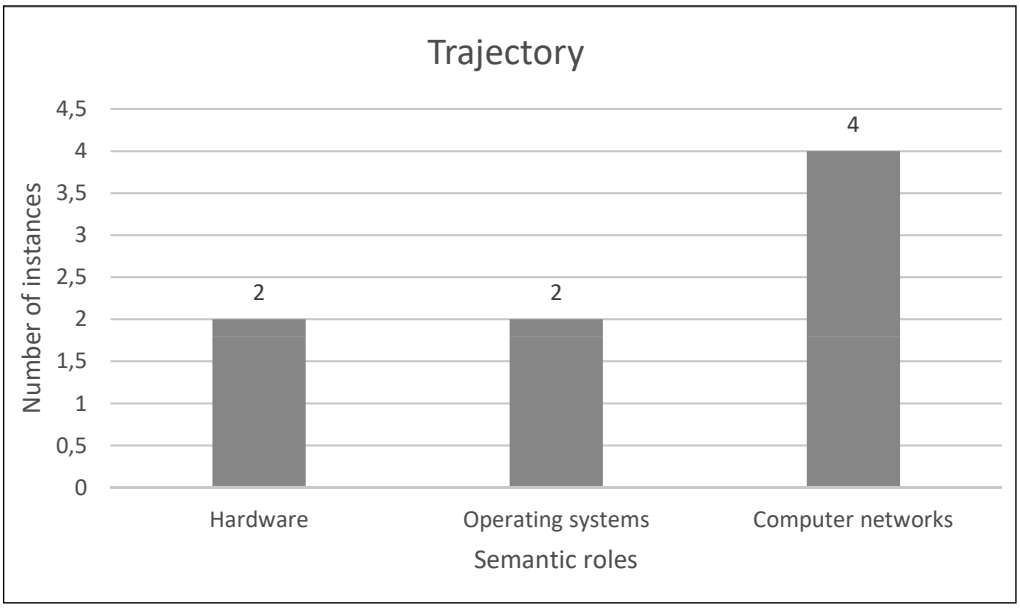

Figure 7: Distribution of the Trajectory role in the CS discourse

In (14), *inter-component communications (ICC)* determine the mechanisms forming "the basis of a broader environment designed to support the construction of educational applications

[…] constructed by end-users […] by assembling high-level, domain-specific software components into functional wholes" (Koutlis et al. 1998):

(14) These are focused on analysing single apps to detect information leaks through *inter-component communications, ICC.* (Blasco/Chen 2018)

The Trajectory is delivered with the prepositions *through*, *via*, *along,* and *over,* introducing the medium or channel for program or data flow transmission.

3.13 Spatial orientation: Goal

The Goal denotes where some software or malefactor gets access to, or some file or data are uploaded/downloaded to/on. This SR is low-frequent in our dataset. We have identified ten cases in *Safeguard measures, Computer networks, Malicious activity / Malefactor, Software, Hardware,* and *Data* (Figure 8).

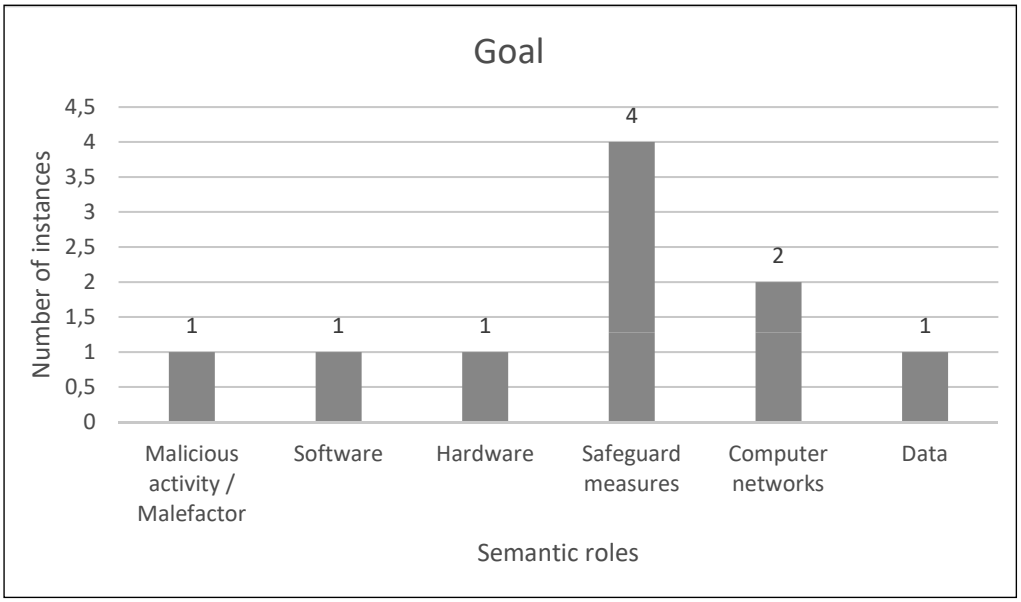

Figure 8: Distribution of the Goal role in the CS discourse

For example, the *Safeguard measures* category contains terms for types of data encryption, passwords, and other security technologies:

(15) After infecting their victims with banking malware and obtaining their phone numbers, they called the CSP's support and […] asked for a new SIM card to be activated, thus gaining access to *OTP.* (Threat intelligence report for the telecommunications industry 2016)

In (15), *OTP (One-Time Password)* stands for "an automatically generated numeric or alphanumeric string of characters that authenticates the user for a single transaction or session" (Techtaget 2021). This numeric string became a goal for banking malware whose activity is expressed with *gain access to*.

3.14 Descriptive function of the Specifier

To elaborate the descriptive function of the forward terms in noun phrases, i. e. noun+noun phrases, we introduce the Specifier. The Specifier complements another argument and consequently is not directly related to the predicate but adds new qualities to the main argument in the noun phrase. This SR is typical of the English language for the nouns in this SR carry out the attributive grammatical function and help to determine particular types of safeguard measures, commands, instructions, computer networks, software, or malicious activity, e. g. *spoofing,* which stands for "hacking or deception that imitates another person, software program, hardware device, or computer, with the intentions of bypassing security measures" (Computer Hope):

(16) NBNS is vulnerable to *spoofing* attacks. (Assolini/Makhnutin 2013)

Spoofing determines the type of NBNS vulnerability.

A Specifier can occur after a specified noun. In this case, the Specifier is introduced with the preposition *of*, as seen in (17):

(17) This threat was originally discovered by a bank's security team, after detecting Meterpreter code inside the physical memory of *a domain controller*. (GReAT 2017b)

Here *a domain controller*, i. e. "a server that responds to security authentication requests within a Windows Server domain" (Techopedia), specifies compromised hardware, particularly the physical memory which hosts malicious software.

This SR might occur in any thematic category (Figure 9):

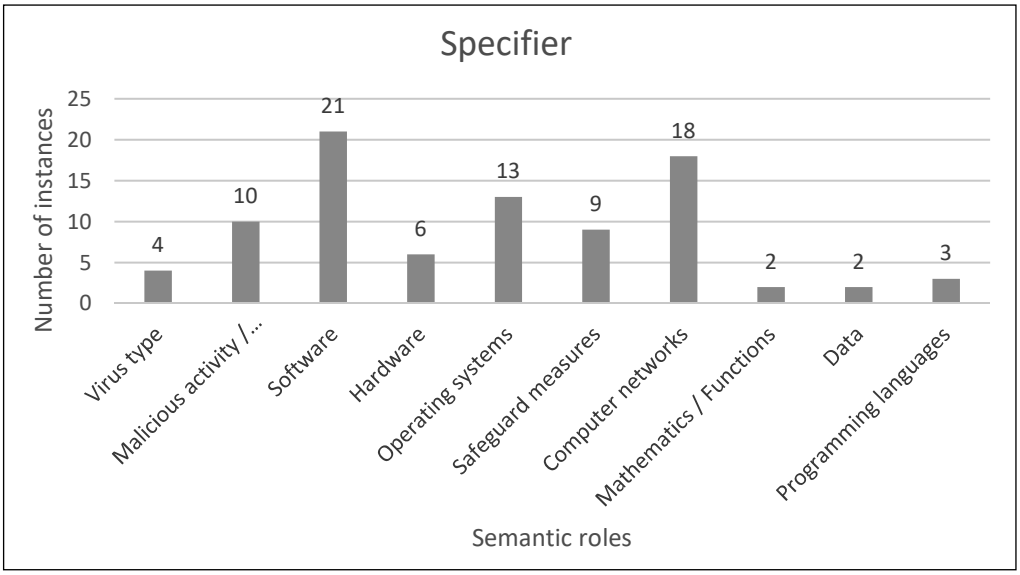

Figure 9: Distribution of the Specifier role in the CS discourse

The Specifier at the cognitive level helps establish the structural organisation of the device and assume possible adverse effects.

3.15 An instrumental part of the computer security activities

The Instrument is an "inanimate force or object involved in an action" (Fillmore 1968: 25), "a mean by which an event is raised, or a tool, usually, an inanimate one used to carry out an action" (Brinton 2000: 168). The Instrument is realised by various term groups – *Malicious activity / Malefactor, Software, Hardware, Operating systems, Safeguard measures, Computer networks, Mathematics / Function, Data,* and *Programming languages* (Figure 10).

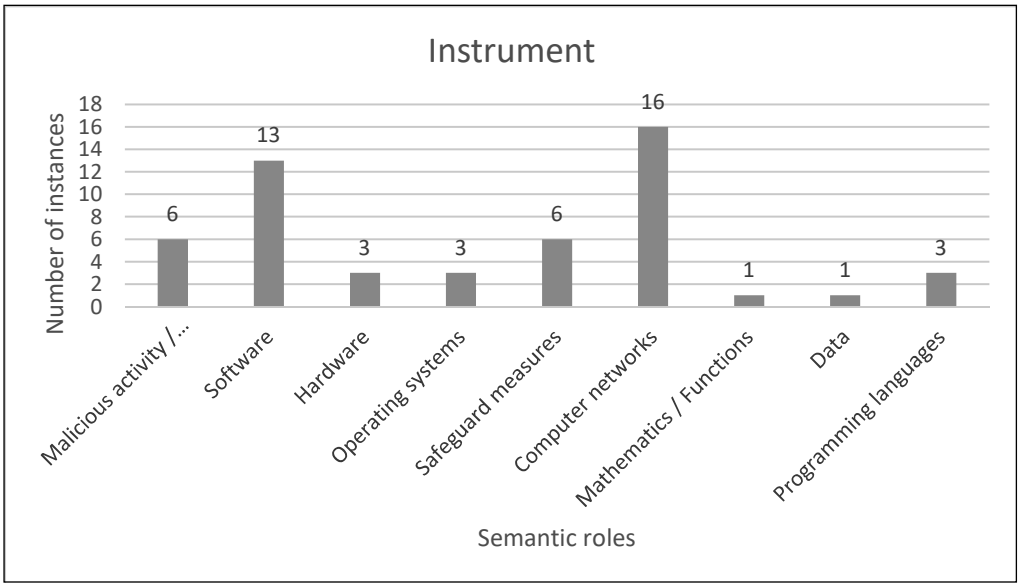

Figure 10: Distribution of the Instrument role in the CS discourse

The most frequent groups are *Computer networks* and *Software*. The terms often designate concepts that can be subdivided into three main groups:

a) Using software for data protection, e. g. *AES*, i. e. *Advanced Encryption Standard,* which is a symmetric-key block cypher algorithm and U.S. government standard for secure and classified data encryption and decryption (Techopedia), e. g. (18):

(18) The files are encrypted using *AES* with CBC mode. (Naor/Alon 2016)

In (18), the Instrument mode helps the reader understand what tool has been used to secure data.

b) Using malware, e. g. *Lurk* in (19) for data violation:

(19) At that time, the "company" had two key "products": the malicious program, *Lurk*, and a huge botnet of computers infected with it. (Stoyanov 2016)

The noun, executing the Instrument, *Lurk,* designates a versatile malicious computer program of a Trojan type, which "can steal money from bank customers" (Shulmin/Prokhorenko 2016). The preposition *with* introduces the Instrument of the pronoun *it* (*Lurk*). This SR helps infer

the latent Agent for better understanding that malware is only a tool used by a plotter to execute malicious actions.

c) Using software as a vulnerability for a data violation. Example (20) represents a CS conundrum when software initially developed for CS protection is used as a tool for malicious actions:

(20) After using *anti-rootkits* Brazil's cybercriminals went deeper and started to develop their own bootloaders. (Marques 2016)

Here (in 20), *anti-rootkit*, i. e. "a tool designed to identify various threats like a rogue and suspicious processes, hooks or modules, registry keys, modified files, and known / unknown rootkits" (Lad 2011), becomes a vulnerability that can be abused. The Instrument is introduced with the verbs *use* and *utilise* and the preposition *with*.

4 Results

We have analysed the SR distribution in the context of CS terms in professional communication. The terms have been sorted into 11 categories. The categories have been devised collaboratively by cognitive linguists and CS experts. Employing domain experts in the project is an effective way to overcome the problem of low lexicographers' and terminologists' expertise in the field (L'Homme 2017: 11). At the stage preceding data collection, the choice of the categories was motivated by the experts with reference to the aspects covered in the CS courses. Subsequent semantic analysis of each term in the corpus and the continuous database enrichment with new terms caused further finetuning in the categories. Thus, the categories are domain-specific. They generally incorporate information on the main participants of the CS events, types of their interaction, typical settings and media or environment, methods and techniques used in the domain, etc. The terms from the selected corpus have been assigned SRs based on their contextual meaning. The statistic shows the SRs prevailing in our dataset (Figure 11).

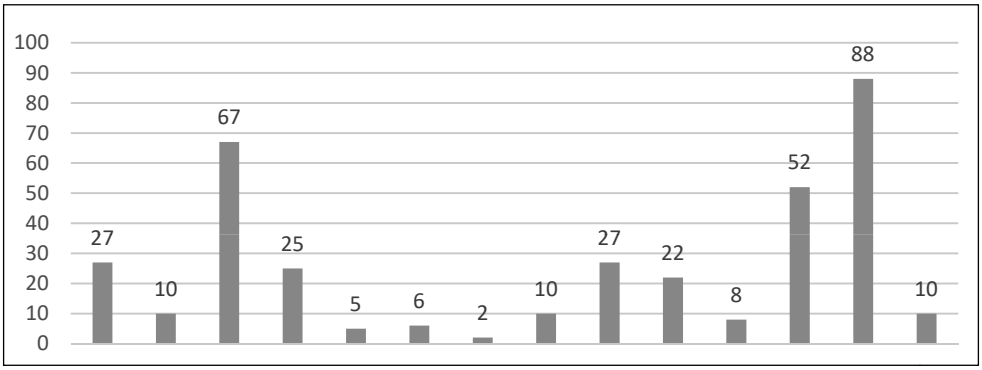

Figure 11: SR metrics in the dataset

Figure 11 shows that the most numerous SRs are Specifier, Objective, and Instrument. The Specifier can hardly count as typical of only the CS discourse because it is common for English grammar in general. High frequency of the Objective was also expected for a specialised discourse, where manipulation with objects is a routing business. However, in CS, the objects are

primarily digital, thus, intangible. Specific to our dataset is the actualisation of the SRs with a frequency rate of 52 and below.

We have determined a certain dependence of SRs on the terms' thematic groups.

- Thus, the **Agent** is enacted by the terms denoting participants able to initiate or cause some action, as a rule, a malicious or defensive one. The difference from the non-specialised discourse is that the terms acquire animacy and exhibit metaphoricity. This is due to the essential property of the Agent to label the animate instigator of the action.
- In professional communication, passive constructions, in which the initiator of action is presented indirectly, are frequent. Such a participant does not occupy the subject position in the sentence and is introduced with the preposition *by*. That is why a new SR of the **quasi-Agent** has been added to designate an activity implementer in passive constructions and back syntactic and semantic synergy.
- The **Counteragent** is the Agent's antipode. It represents the force or the initiator of the force, against which the Agent's effort is directed. Accordingly, in our corpus of CS texts, the most numerous group for this SR has been *Malicious activity / Malefactor*.
- The **Objective** represents the most prominent feature of inanimateness attributed to computer entities brought to action by computer experts or users. The Objective occurs in almost any category and designates computer tools, programs, network clients, mechanisms, etc. However, the most illustrative category is *Software*. The category includes computer programs engaged in different kinds of activities carried out by other participants who operate these programs but do not change them.
- The **Perceptive** is also typical of the categories determining entities that do not perform any self-activity but occur as objects seen, heard, or sensed by other participants. The SR is regular of the *Malicious activity / Malefactor* terms. In many cases, users become aware, passively observe or express some attitude to malicious actions in the computer sphere but cannot influence the situation.
- As the **Cause**, there occur the terms for programs or activities generating a problem for CS. They mainly refer to *Malicious activity / Malefactor, Virus type, Software,* and *Safeguard measures*. The latter proves that cybercriminals take advantage even of CS measures.
- The **Benefactive** is typical of *Malicious activity / Malefactor, Software,* and *Safeguard measures*. The terms in this SR designate computer entities, which get new features or qualities from other computer entities.
- The **Addressee** is mainly found in the categories of *Computer networks* and *Malicious activity / Malefactor*, which contain terms for network software, device, hardware, or a computer user, who receives malware.
- The high frequency of the **Patient** in such categories as *Software, Computer networks, Data*, and *Operating systems* proves that the entities designated by these terms often suffer from malware and are modified because of malicious actions.
- The **Result** is attributed to what usually emerges from the fraudulent situations, the most relevant category being *Malicious activity / Malefactor*.
- The place where malware is likely to be found is determined by the **Locative** or the **Trajectory**. They are nominated by the terms from *Hardware, Computer networks, Software,* and *Operating systems*.
- And finally, to identify the SR of terms that define the features of a CS item, we have

added the **Specifier**. It is situated immediately before the specified word or after it. In the latter case, it is preceded by the preposition *of*.

So, all the basic SR have been identified in the CS discourse, and their attribution to particular thematic categories has been reasoned.

5 Discussion

The results can be interpreted through the philosophy of sign systems. LSP representing a separate branch of natural language, follows the logic attributed to any sign system. According to Solomonick (2011), this logic occurs in three types. The first one is the logic of the correspondence between the language system and reality. This means that the language reproduces events to preserve the same relations and dependences as in real life. To illustrate this assumption, one should refer to the semantic frame, which mirrors scenarios of everyday real-life situations. Thus, the SRs and their valences match real-life stereotypical participants entering similar relations (21):

(21) *Colluding apps* bypass the security measures enforced by sandboxed operating systems such as Android. (Blasco/Chen 2018)

Colluding apps play the Agent SR. They change the trajectory of their movement not to come in contact with (i. e. *bypass*) an unwanted obstacle (i. e. *security measures*, which play the Objective SR). *Sandboxed operating systems such as Android* play a double SR – the Counteragent with respect to *colluding apps* and the quasi-Agent with respect to *security measures.*

To understand this situation typical of the CS discourse, if one does not possess expert knowledge in this field, they rely on their daily experience and subconsciously find analogue situation models matching the semantic frame. Similar situations can occur in strategic games, military developments, hunting, etc. The choice depends on the background knowledge one has. This phenomenon of understanding one thing in terms of another is called *metaphor*. Our findings confirm that metaphorical mappings within the semantic frames in specialised discourse activate the background knowledge derived from similar contexts. This usefulness of embedding specialised concepts in everyday situations is highlighted by Faber/Cabezas-García (2019).

Another type of logic – intrasystem logic – sets the semiotic system's relations. It is imposed upon the real-life correspondence logic. This type of logic is described in studies carried out in grammar, morphology, syntax, etc. Our findings can also contribute to understanding the intrasystem logic, e. g. in (2) discussed earlier:

(2) Spain and Poland have been two countries traditionally targeted by *SMS scams* and similar *malware.* (GReAT 2017a)

The preposition *by* introducing the doer of the action in passive constructions works as the marker of the quasi-Agent. Meanwhile, the proposition *with* employed "for saying what is used for doing something" (The Free Online English Dictionary) is typical of the Instrument, as seen in (22):

(22) The "company" had two key "products": the malicious program, Lurk, and a huge botnet of computers infected *with it.* (Stoyanov 2016)

According to the third type of logic – communication or pragma-logic (Solomonick 2011), the same semantic frame is interpreted regarding a communicative situation in a particular discourse. For instance, the frame 'Agent *hijack* Objective' matches events in CS (23) and terrorist (24) discourses:[2]

(23) The virus […] *hijacked* another program known as Microsoft Outlook. (Christensen 1999)

(24) On Sept. 11, 2001, terrorists *hijacked* four separate planes. (Dilmore 2011)

6 Conclusion

Our research reveals the most representative SRs within thematic categories of the CS terminology. We approached this task from the cognitive perspective to rationalise the correlation between the formal SR categorisation of terms and pragmatically conditioned semantic categorisation of terms. Our findings illustrate that for interpreting CS terminology, the helpful technique is to appeal to a similar frame in another, more familiar discourse.

The classical Fillmore's frame semantic theory has been refined and extended – the quasi-Agent and Specifier SRs have been added, contributing to building a coherent system for framing events of professional communication.[3]

In our previous works (Isaeva/Burdina 2019, Isaeva/Crawford 2019), we have demonstrated the virtue of semantic framing for conceptual metaphorical modelling. The current results can be applied for cognitive mediation in professional communication to enhance specialised knowledge transfer. Based on a formalised SR distribution in a frame, it is possible to proceed to the discourse event simulation and metaphorical modelling in mental representation and cognition. Our further efforts will be fostered to apply text mining and automated metaphor identification in specialised texts.

Acknowledgements

We thank Tim and Karen Sadler (Oxford, UK) for proofreading the text.

References

Amirova, Oksana Georgievna (2002): *Semanticheskaja model anglijskih glagolov upravlenija* [Semantic Model of English Verbs of Governance]. PhD dissertation. Ufa.

Apresjan, Yurij Derenikovich (1995): *Selected Works.* 2nd ed. Vol. 1: *Lexical semantics (Synonymous means of language).* Moscow: Yazyki Russkoi Kultury.

Apresjan, Yurij Derenikovich (2009): *Issledovanija po semantike i leksikografii* [Works on Semantics and Lexicography]. Vol. 1. Moscow: Yazyki Slavyanskoi Kultury.

Brinton, Laurel J. (2000): *The Structure of Modern English: A Linguistic Introduction.* Amsterdam: Benjamins.

Chafe, Wallace L. (1970): *Meaning and Structure of Language.* Chicago: University of Chicago Press.

Cook, Walter Anthony (1998): *Case Grammar Applied.* Arlington: Summer Institute Linguistics.

[2] Examples (23) and (24) are cited from the Corpus of Contemporary American English (https://www.english-corpora.org/coca/).

[3] Given as a suggestion, which needs further investigation.

Downing, Angela / Locke, Philip (1992): *A University Course in English Grammar.* Hemel Hempstead: Prentice Hall.

Faber, Pamela / Cabezas-García, Melania (2019): "Specialised Knowledge Representation: from Terms to Frames." *Research in Language* 17.2: 197–211.

Fillmore, Charles J. (1968): "The Case for Case." *Universals in Linguistic Theory*. Eds. Emmon W. Bach / Robert Thomas Harms. New York: Holt, Rinehart & Winston. 1–88.

Fillmore, Charles J. (1971): "Types of Lexical Information." *Semantics. An Interdisciplinary in Philosophy, Linguistics and Psychology.* Eds. Danny D. Steinberg / Leon A. Jakobovits. Cambridge: Cambridge University Press. 370–392.

Fillmore, Charles J. (1982): „Frame Semantics." *Linguistics in the Morning Calm. Selected Papers from SICOL-1981*. Ed. The Linguistic Society of Korea. Seoul: Hanshin. 111–137.

Gak, Vladimir Grigorevich (1998): *Jazykovye preobrazovanija* [Language Transformations]. Moscow: Yazyki Russkoi Kultury.

Humboldt, Wilhelm von (1984): *Selected Works on Linguistics.* Moscow: Progress.

Isaeva, Ekaterina (2019): "Metaphor in Terminology: Finding Tools for Efficient Professional Communication." *Fachsprache. Journal of Professional and Scientific Communication* 41.1–2*:* 65–86.

Isaeva, Ekaterina / Baiburova, Olga / Manzhula, Oksana (2022): "Anthropomorphism in Computer Security Terminology Through the Prizm of Smart Cognitive Framing." *Science and Global Challenges of the 21st Century – Science and Technology. Perm Forum 2021*. Eds. Alvaro Rocha / Ekaterina Isaeva. Cham: Springer. 460–474.

Isaeva, Ekaterina / Burdina, Olga (2019): "Transdiscursive Term Transformation: The Evidence from Cognitive Discursive Research of the Term 'Virus'." *Current Approaches to Metaphor Analysis in Discourse*. Ed. Ignasi Navarro i Ferrando. Berlin/Boston: De Gruyter. 79–110.

Isaeva, Ekaterina / Crawford, Russ (2019): "Semantic Framing of Computer Viruses: the Study of Semantic Roles' Distribution." *Perm University Herald. Russian and Foreign Philology* 11.1: 5–13.

Katsnelson, Solomon Davidovich (2010): *Istoriko-grammaticheskie issledovanija* [Works on the history of grammar]. Saint Petersburg: Saint Petersburg Linguistic Society.

Kshirsagar, Meghana / Thomson, Sam / Schneider, Nathan / Carbonell, Jaime / Smith, Noah A. / Dyer, Chris (2015): "Frame-semantic Role Labeling with Heterogeneous Annotations." *Proceedings of the 53rd Annual Meeting of the Association for Computational Linguistics and the 7th International Joint Conference on Natural Language Processing.* Vol. 2: *Short Papers,* Beijing. Association for Computational Linguistics. 218–224. https://aclanthology.org/P15-2036/ (06.09.2022).

L'Homme, Marie-Claude (2017): "Maintaining the Balance between Knowledge and the Lexicon in Terminology: A Methodology Based on Frame Semantics." *Lexicography* 4.1: 3–21.

Paducheva, Elena Viktorovna (2004): *Dinamicheskie modeli v semantike leksiki* [Dynamic Models in the Semantics of Vocabulary]. Moscow: Yazyki Slavyanskoi Kultury.

Plungian, Vladimir Aleksandrovich (2003): *Obshhaja morfologija: Vvedenie v problematiku* [General Morphology: an introduction]. 2nd ed. Moscow: Editorial URSS.

Rakhilina, Ekaterina Vladimirovna / Testelets, Yakov Georgievich (2016): "Nauchnoe nasledie Ch. Filmora i sovremennaja teorija jazyka" [Charles Fillmore's Legacy and Modern Theoretical Linguistics]. *Voprosy jazykoznanija* [Topics in the Study of Language] 2: 7–21.

Roth, Michael / Woodsend, Kristian (2014): "Composition of Word Representations Improves Semantic Role Labelling." *EMNLP 2014 – 2014 Conference on Empirical Methods in Natural Language Processing. Proceedings of the Conference*. 407–413. https://aclanthology.org/D14-1045/ (06.09.2022).

Saussure, Ferdinand de (1959): *Course in General Linguistics.* New York / Toronto / London: McGraw-Hili.

Solomonick, Abraham (2011): *Filosofija znakovyh sistem i jazyk* [Philosophy of Sign Systems and Language]. Moscow: LKI.

Whorf, Benjamin Lee (1956): *Language, Thought and Reality: Selected Writings of Benjamin Lee Whorf*. Cambridge, Mass.: MIT Press.

Sources of Linguistic Data

Assolini, Fabio / Makhnutin, Andrey (2013): "PAC – the Problem Auto Config." https://securelist.com/analysis/publications/57891/pac-the-problem-auto-config (10.09.2019).

Blasco, Jorge / Chen, Thomas M. (2018): "Automated Generation of Colluding Apps for Experimental Research." *Journal of Computer Virology and Hacking Techniques* 14.2: 127–138. https://link.springer.com/article/10.1007/s11416-017-0296-4 (14.09.2019).

Christensen, Damaris (1999): "Beyond Virtual Vaccinations. Developing a Digital Immune System in Bits and Bytes." *Science News* 156.5: 76–78.

Dilmore, Angie Kay (2011): "9/11 Ten Years Later." *Boys' Life*. 11 September 2011. Vol. 101 Issue 9, 26–29. Retrieved from Corpus of Contemporary American English (https://www.english-corpora.org/coca/) (06.09.2022).

"Gang of fraudsters and 'money mules' sentenced for £200k scam" (2019): *Financial Fraudster News*. https://www.financialfraudsternews.com/en/currency-fraud2/gang-of-fraudsters-and-money-mules-sentenced-for-200k-scam (19.09.2019).

GReAT (2017a): "Expensive Free Apps." *SECURELIST by Kaspersky*. https://securelist.com/expensive-free-apps/77083/ (14.09.2019).

GReAT (2017b): "Fileless Attacks against Enterprise Networks." *SECURELIST by Kaspersky*. https://securelist.com/blog/research/77403/fileless-attacks-against-enterprise-networks/ (15.09.2019).

GReAT / Naor, Ido (2016): "ATMZombie: Banking Trojan in Israeli Waters." *SECURELIST by Kaspersky*. https://securelist.com/atmzombie-banking-trojan-in-israeli-waters/73866/ (15.09.2019).

Koutlis, Manolis / Kourouniotis, Petros / Kyrimis, Kriton / Renieri, Nikolina (1998): "Inter-component Communication as a Vehicle towards End-user Modeling." *ICSE'98 Workshop on Component-Based Software Engineering, Kyoto, Japan, April 26*: 26f: https://icsa-conferences.org/series/CBSE/1998/papers/p7.html (06.09.2022).

Lad, Aditya (2011): "Top 7 Anti Rootkit Software for Windows." https://www.computerweekly.com/tip/Top-7-anti-rootkit-software-for-Windows (14.09.2019).

Makrushin, Denis (2017): "The Cost of Launching a DDoS Attack." *SECURELIST by Kaspersky*. https://securelist.com/analysis/publications/77784/the-cost-of-launching-a-ddos-attack/ (30.05.2019).

Mamedov, Orkhan / Sinitsyn, Fedor (2016): "A Malicious Pairing of Cryptor and Stealer." *SECURELIST by Kaspersky*. https://securelist.com/a-malicious-pairing-of-cryptor-and-stealer/76039/ (15.09.2019).

Marques, Thiago (2016): "The Evolution of Brazilian Malware." *SECURELIST by Kaspersky*. https://securelist.com/blog/research/74325/the-evolution-of-brazilian-malware/ (15.09.2019).

Naor, Ido / Alon, Noam (2016): "CryPy: Ransomware behind Israeli Lines." *SECURELIST by Kaspersky*. https://securelist.com/blog/research/76318/crypy-ransomware-behind-israeli-lines/ (14.09.2019).

Ortloff, Stefan (2016): "New Wave of Mirai Attacking Home Routers." *SECURELIST by Kaspersky*. https://securelist.com/new-wave-of-mirai-attacking-home-routers/76791/ (15.09.2019).

Shulmin, Alexey / Prokhorenko, Mikhail (2016): "Lurk Banker Trojan: Exclusively for Russia." *SECURELIST by Kasp*ersky. https://securelist.com/blog/research/75040/lurk-banker-trojan-exclusively-for-russia/ (15.09.2019).

Stoyanov, Ruslan (2016): "The Hunt for Lurk. How we helped to catch one of the most dangerous gangs of financial cybercriminals." *SECURELIST by Kaspersky*. https://securelist.com/analysis/publications/75944/the-hunt-for-lurk/ (15.09.2019).

"Threat Intelligence Report for the Telecommunications Industry" (2016): *SECURELIST by Kaspersky*. https://securelist.com/analysis/publications/75846/threat-intelligence-report-for-the-telecommunications-industry/ (15.09.2019).

Unuchek, Roman (2017): "Mobile Malware Evolution 2016." *SECURELIST by Kaspersky*. https://securelist.com/mobile-malware-evolution-2016/77681/ (15.09.2019).

"What is a remote server?" (2017): *Quora*. https://www.quora.com/What-is-a-remote-server (19.09.2019).

Zakorzhevsky, Vyacheslav (2015): "You can't be invulnerable, but you can be well protected". *SECURELIST by Kaspersky*. https://securelist.com/you-cant-be-invulnerable-but-you-can-be-well-protected/73160/ (15.09.2019).

Online resources and dictionaries

Cambridge Dictionaries Online. Cambridge University Press. http://dictionary.cambridge.org/ (15.09.2019).

Collins. Free Online Dictionary and Thesaurus. https://www.collinsdictionary.com/ (06.09.2022).

Computer Hope. https://www.computerhope.com/jargon.htm (15.09.2019).

English Dictionary, Thesaurus & Grammar Help (2010). https://www.lexico.com/en/ (15.09.2019).

FrameNet. https://framenet.icsi.berkeley.edu/fndrupal/ (22.08.2019).

GitHub. https://github.com/ (21.08.2019).

LexiCon Research Group (2021). http://lexicon.ugr.es/ (21.08.2021).

Techopedia. IT Dictionary for computer terms and technology (2016). https://www.techopedia.com/dictionary (15.09.2019).

Techtarget. Search Security (2021). https://www.techtarget.com/ (06.09.2022)

The Free Dictionary by Farlex: Dictionary, Encyclopedia, and Thesaurus, Collection of dictionaries by subject including medical and legal together with free and subscription encyclopedias, in ten languages (2003). http://www.thefreedictionary.com/ (14.09.2019).

The Free Online English Dictionary from Macmillan Publishers (2009). http://www.macmillandictionary.com/ (15.09.2019).

The Longman Dictionary of Contemporary English Online. http://www.ldoceonline.com/ (10.09.2019).

Your Dictionary. http://www.yourdictionary.com (15.09.2019).

Assoc. Prof. Ekaterina Isaeva, PhD
Head of the Department of English
for Professional Communication
Perm State University
15, Bukirev Str.
Perm, 614990
ekaterinaisae@psu.ru

Assoc. Prof. Oksana Manzhula, PhD
Department of English
for Professional Communication
Perm State University
15, Bukirev Str.
Perm, 614990
achilleon@mail.ru

Assoc. Prof. Olga Baiburova, PhD
Department of English
for Professional Communication
Perm State University
15, Bukirev Str.
Perm, 614990
olga3079@mail.ru