Лингвистика и образование. 2023. Том 3. №3. С. 24-35
Linguistics & education 2023 Vol. 3, No. 3. P. 24-35

Научная статья
УДК 81'23-811
https://doi.org/10.29039/2712-9519-2023-3-24-35

5.9.8 Теоретическая, прикладная и сравнительно-сопоставительная лингвистика

ТЕРМИНОЛОГИЧЕСКИЕ НОМИНАЦИИ КАК РЕЗУЛЬТАТ ИНТЕРПРЕТАЦИИ ЭКСПЕРТНОГО ЗНАНИЯ НА УРОВНЕ СОЗНАНИЯ И ЯЗЫКА (на материале англоязычных терминов информационной безопасности) Часть II

Татьяна Васильевна Дроздова
Астраханский государственный технический университет, Астрахань, Россия
drozdova_astu@mail.ru

Аннотация. В статье рассматривается ряд терминологических номинаций из области информационной безопасности, создание и функционирование которых обусловлено концептуализацией и интерпретацией на ментальном и языковом уровнях формируемого и репрезентируемого знания. В данной части статьи рассматривается обусловленность терминотворчества взаимодействием когнитивных и языковых механизмов. Подтверждается вовлеченность в процессы концептуализации, интерпретации и языковой номинации знания различного типа.

***Ключевые слова*:** концептуализация, интерпретация, знание, фрейм, языковая номинация, термин.

Для цитирования: Дроздова Т.В. Терминологические номинации как результат интерпретации экспертного знания на уровне сознания и языка (на материале англоязычных терминов информационной безопасности) Часть II // Лингвистика и образование. 2023. Том 3. №3. С. 24-35. https://doi.org/10.29039/2712-9519-2023-3-24-35

Original article

TERMINOLOGICAL NOMINATIONS AS REPRESENTING EXPERT KNOWLEDGE INTERPRETATION IN MIND AND LANGUAGE (illustrated by English information security terms) Part II

Tatiana V. Drozdova
Astrakhan state technical university, Astrakhan, Russia
drozdova_astu@mail.ru

Abstract. The article is devoted to the analysis of the interpretative role of mind and language in creating some terminological nominations to represent expert knowledge in the field of information security. This part of the paper considers the interrelation of cognitive and language mechanisms. It is proved that different types of knowledge are involved in term-formation.

Keywords: conceptualization, interpretation, knowledge, frame, verbal nominations, term.

For citation: Drozdova T.V. Terminological nominations as representing expert knowledge interpretation in mind and language (illustrated by English information security terms) Part II, Linguistics & education 2023;3:24-35. https://doi.org/10.29039/2712-9519-2023-3-24-35

Введение

Взаимосвязь языка и сознания, обусловливающая процесс языковой номинации, была подтверждена в первой части статьи на основе реконструкции в вербальном формате фрейма, рассматриваемого как когнитивная структура знания, репрезентирующая прототипическую ситуацию угрозы хищения конфиденциальной информации через незаконный доступ к системе ее хранения, в том числе путем психологического манипулирования ее обладателем. Решение дальнейших задач исследования связано с анализом действия интерпретации на ментальном и вербальном уровнях, которое реализуется посредством активации и взаимодействия когнитивных и языковых механизмов, обеспечивающих порождение терминологических номинаций с привлечением знания различного типа.

Терминообразование как результат интерпретации знания на ментальном и языковом уровнях

Содержание проанализированного эмпирического материала показывает, что, осмысляя ситуацию/событие возможного хищения информации, субъекты профессиональной деятельности, благодаря своим метакогнитивным способностям, активируют сформировавшуюся в процессе жизнедеятельности базу знаний и определяют событие как потенциальную угрозу носителю информации: субъекту, электронному устройству или иному средству ее хранения. Возможность передать этот смысл осуществляется через выбор имеющегося языкового знака, в значении которого сема «угроза» является ядерной. Выбор лексемы *threat* в качестве родового имени формируемого концепта расширяет экстенсионал значения слова (см. значение **1.** *a situation or activity that could cause harm or danger* в [1]). При этом результат действия когнитивного механизма перспективизации будет представлен лишь при употреблении данной единицы в специализированном контексте, будучи объективирован в дефиниции языкового знака, выполняющего здесь функцию термина: *A potential violation of security. Any circumstance or event with the potential*

to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service [2]. Заметим, что данная дефиниция содержит имена концептов, представленных слотами фрейма, репрезентирующего экспертное знание о прототипической ситуации (см. Часть I данной статьи).

Следует также указать, что в дискурсе информационных технологий источник предполагаемой угрозы интерпретируется как связанный с данным понятием отношением «событие-источник события». Таким образом, механизм когнитивной метонимии обусловливает выбор данного термина для обозначения источника угрозы, а термин становится многозначным вследствие действия языкового механизма метонимического переноса значения: *threat – the potential source of an adverse event* [3]. Дальнейшая интерпретация знания о концепте реализуется через когнитивный механизм профилирования одного из концептуальных признаков, а именно «локация источника угрозы относительно системы/устройства хранения информации». На уровне языка с целью обозначения противопоставляемых на основе этого признака субкатегориальных концептов по модели аналитического деривата Attr+N создаются обозначения полученного результата субкатегоризации:

inside(r) threat – an entity with authorized access (i.e., within the security domain) that has the potential to harm an information system of enterprise through destruction, disclosure, modification of data, and/or denial of service

outside threat – an unauthorized entity from outside the security domain that has the potential to harm an information system of enterprise through destruction, disclosure, modification of data, and/or denial of service [3].

Аналогично рассмотренным выше процессам интерпретации знания о событии и выбору мотивирующих оснований порождения его обозначения можно, по-видимому, объяснить и ментальную интерпретацию субъектом познания отдельных действий злоумышленника по отношению к материальной

системе хранения информации. Для обозначения таковых используются единицы общенационального языка с последующим эксплицированием признака «область реализации действия» в дефиниции таких терминологизуемых единиц (*intrusion – unauthorized act of bypassing the security mechanisms of a system*; то же - *penetration* [3]). Необходимость профилирования определенных признаков концептуализируемого действия реализуется в языке через механизм аналитической деривации. В ономасиологической модели таких единиц профилируемый признак всегда представлен эксплицитно:

- наличие/отсутствие права на получение информации при совершении действия в отношении ее владельца или устройства ее хранения: *unauthorized access, unauthorized disclosure*; элемент *information* здесь имплицирован мотивирующим суждением и подвергается эллипсу при образовании деривата;

- способ совершения действия: *online attack,* или *cyberattack*; в последнем термине элемент *cyber-* сохраненная часть слова *cyberspace*; ср. *cyber attack - an attack via cyberspace targeting the enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information* [3]; данную языковую единицу можно рассматривать как результат действия языкового механизма аббревиации (конкретно – стяжения);

- имплицируемый результат и оценка действия: *data breach*; порождение этого термина обусловлено действием механизма концептуальной метонимии: ментальная интерпретация помещает в фокус внимания смысл *someone does something that goes against accepted rules or social behaviour* [1], а на языковом уровне осуществляется метонимический перенос значения слова *breach* по модели СИТУАЦИЯ – ДЕЙСТВИЕ (в этой ситуации). В результате во внутренней форме языкового знака профилируется объект действия и имплицируется результат действия (*failure to secure information)* и его негативная оценка (*goes against accepted rules or social behaviour*).

Ономасиологический анализ аналитических дериватов показывает, что категориальная принадлежность номинируемого концепта не всегда

эксплицирована элементом, выполняющим роль ономасиологического базиса, ср.: *inside(r) threat* (категория субъекта не представлена в материальной структуре знака *threat*) и *unauthorized user* (категория субъекта представлена элементом -*er*).

Осмысление и интерпретация концептуализируемой информации осуществляется также с опорой на специальное знание как из собственной области субъекта научно-практической деятельности, так и из других областей знания. Концептуализация инструментов воздействия на носителя информации (субъекта или устройство) с целью хищения информации опирается на знание о разработке программного обеспечения – компьютерных программ, которые могут служить таким инструментом. Родовое имя концепта COMPUTER PROGRAMM (ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ/ КОМПЬЮТЕРНАЯ ПРОГРАММА) представлено на базовом уровне категоризации термином *software*. Полагают, что в качестве термина области информационных технологий эта единица появилась в английском языке в 1960-х годах как противоположная по значению другому термину – *hardware* – и была образована по той же модели [4]. В последующем основа – *ware* приобрела в терминосистеме информационных технологий статус терминоэлемента, используемого при создании ряда терминов по словообразовательным моделям английского языка (*spyware, scareware, etc.)*; при этом значение термина *software* полностью сохраняется. В аспекте воздействия на систему хранения информации этот концепт интерпретируется через профилирование отрицательной оценки: *malicious software* (термин существует также в форме аббревиатуры-сращения *malware*).

Более интересным представляется то, что при концептуализации разных типов программного обеспечения и интерпретации полученного знания осуществляется обращение к модели концептуальной метафоры АРТЕФАКТ – ЭТО СУБЪЕКТ с последующим профилированием концептуальных признаков этого «субъекта» по выполняемому им действию: *spyware*, *scareware, adware* (в

данном случае имеет место аббревиация: *ad* – от *advertizing*; "*software that automatically displays or downloads advertising*" [4].

Отдельные элементы экспертного знания, участвующие в интерпретации новой информации, в свое время были обозначены единицами повседневного языка, получившими в дискурсе информационных технологий новое значение вследствие действия когнитивного механизма метафоры и языкового механизма метафоризации, например по модели ЗРИТЕЛЬНОЕ ДЕЙСТВИЕ – ЭТО ОБОНЯТЕЛЬНОЕ ДЕЙСТВИЕ: *sniffing* (от *sniff – to smell something* [1]) – *seeing all packets, which are passed through wires or sometimes through air for wireless networks* [3]. Интерпретация информации об инструменте, осуществленная с привлечением когнитивного механизма метафтонимии по моделям ДЕЙСТВИЕ – ИСПОЛНИТЕЛЬ ДЕЙСТВИЯ + АРТЕФАКТ – ЭТО СУБЪЕКТ, обеспечила создание имени компьютерной программы как деривата *sniffer* (основа *sniff-* + категоризатор *-er*), в образной форме профилирующего принцип действия этой программы, раскрываемый в дефиниции термина*: an application or device that can read, monitor, and capture network data exchanges and read network packets. If the packets are not encrypted, a sniffer provides a full view of the data inside the packet* [5]. *Malicious actors can use sniffers to capture encrypted data like passwords and usernames in network traffic* [6].

Интерес представляет и образование термина на основании интерпретирующего сравнения использования программного обеспечения (действие) с повседневным знанием о процессе рыбалки, когда используется определенная наживка (здесь, например, какая-то бесплатная программа и т.п.). При этом на языковом уровне интенционально меняется материальная форма терминологической номинации: ***phishing (n.)*** *"fraudulent attempt to obtain sensitive information such as usernames, passwords and credit card details by disguising oneself as a trustworthy entity in an electronic communication", (by 2000 many sources cite usage from 1995 among hackers, and the thing itself was active by then); an alteration of* ***fishing*** *(n.); perhaps by influence of* ***phreak*** *and the U.S. rock band Phish, which had been performing since 1983* [4]. См. также: *Phishing is a type*

of internet fraud that seeks to acquire a user's credentials by deception. It includes the theft of passwords, credit card numbers, bank account details, and other confidential information. Phishing messages usually take the form of fake notifications from banks, providers, e-pay systems, and other organizations. The phishing attempt will try to encourage a recipient, for one reason or another, to enter/update personal data [6].

Примером концептуализации информации с ее последующей интерпретацией через обращение к понятиям других областей знания (в частности социологии) может послужить формирование содержания концепта *social engineering* (и производного от него *social engineer*). В фокус внимания ставится смысл «умение организовать чью-либо деятельность с целью достижения планируемого результата путем манипулирования (убеждения)» (см. *Social engineering originally mean that planned social change could be achieved by manipulation, usually by governments* [7]). В области информационной безопасности этот смысл далее уточняется в аспекте объекта манипулятивного воздействия и целевой направленности манипулирования. Отрицательная оценка содержится в дефиниции термина: она представлена в семантике слова *manipulation,* а также в семантике иных лексических единиц, репрезентирующих содержание понятия (подчеркнуто нами): *Social engineering can be defined as the act of manipulating human beings, most often with the use of psychological persuasion, to gain access to systems, containing data, documents, and information that the social engineer should not have access to obtain* [8, с. 1]. *The practice of penetrating system security by tricking individuals into divulging passwords and information about network vulnerabilities* [5].

Примером метафорической интерпретации информации о компьютерной программе в аспекте профилирования ее действия, основанной на знании из области естественных наук, является использование для обозначения такой вредоносной программы термина соответствующей терминологии *virus*. Модель концептуальной метафоры АРТЕФАКТ – ЭТО ЖИВОЙ ОРГАНИЗМ обусловливает метафоризацию данной лексической единицы в терминосистеме информационных технологий в целом, а дефиниция термина эксплицирует

профилируемый признак, закрепленный в значении лексической единицы в терминосистеме-источнике (подчеркнуто нами): *Malware that replicates, commonly by infecting other files in the system, thus allowing the execution of the malware code and its propagation when those files are activated* [5]. *A Virus is a malicious computer program that is often sent as an email attachment or a download with the intent of infecting that device. Once the device is infected, a virus can hijack the web browser, display unwanted ads, send spam, provide criminals with access to the device and contact list, disable security settings, scan, and find personal information like passwords* [9].

Можно отметить и использование знания мифологической картины мира в процессе концептуализации и интерпретации инструментов, применяемых злоумышленником с целью получения доступа к информации. Так, профилирование признака «скрытая угроза» и использование модели концептуальной метафоры АРТЕФАКТ – ЭТО МИФОЛОГИЧЕСКИЙ ОБЪЕКТ (представляющий скрытую угрозу) дает основание для выбора в качестве обозначения такой компьютерной программы прецедентного имени *Trojan horse (Trojan) – a program containing hidden code allowing the unauthorized collection, falsification, or destruction of information* [2]. Данный термин в терминосистеме информационных технологий имеет статус фразеологической единицы, при этом его эллиптическая форма используется для обозначения разновидности концептуализируемого понятия, в содержании которого фокусируется тип похищаемой информации (подчеркнуто нами): *Banker Trojan – a malicious computer program that intercepts sensitive personal information and credentials for accessing online bank or payment accounts* [6].

Примером обращения к собственно языковому знанию при генерировании обозначения концептуализируемого действия и его интерпретацию через понятие «грабеж», могут служить термины *clickjacking* и *cryptojacking*. Очевидно, что без знания значения словообразовательных элементов и модели образования сложнопроизводной единицы создание указанных единиц было бы невозможным (см. исходное: ***hijack (v.)*** *by 1922 (perhaps c. 1918), American*

English, of unknown origin; perhaps from high(way) + jacker "one who holds up" (agent noun from ***jack*** *(v.)). In early use "to rob (a bootlegger, smuggler, etc.) in transit;" sense of "seize an aircraft in flight" is 1968 (also in 1961 variant skyjack), extended 1970s to any form of public transportation.* Related: *Hijacked*; *hijacking*. Related: *Hijacker*. [4]. В данном случае можно реконструировать действие механизма концептуальной деривации, обеспечивающего перенос в фокус внимания смыслов, представленных ядерными семами производящих основ при формировании содержания нового концепта. В каждом из созданных терминов во внутренней форме языковой единицы фокусируется смысл *rob* (или *seize*), но второй фокус совпадает не полностью: в одном случае – это действие, приводящее к хищению информации, а в другом фокусируется и информация об объекте хищения (в данном случае это деньги в виртуальной форме) (подчеркнуто нами):

Clickjacking involves tricking someone into clicking on one object on a web page while they think they are clicking on another. The attacker loads a transparent page over the legitimate content on the web page so that the victim thinks they are clicking on a legitimate item when they are really clicking on something on the attacker's invisible page. This way, the attacker can hijack the victim's click for their own purposes. Clickjacking could be used to install malware, gain access to one of the victim's online accounts, or enable the victim's webcam [6].

Cryptojacking consists of hackers using the computing power of a compromised device to generate or "mine" cryptocurrency without the owner's knowledge. Mining can be performed either by installing a malicious program on the target computer or through various kinds of fileless malware. Sometimes attackers take over part of the computer's processing power when a page containing a special mining script is opened [6].

Объем статьи не позволяет проанализировать все термины из полученной в ходе исследования выборки, входящие в разные слоты фрейма, репрезентирующего знание о прототипической ситуации потенциального хищения информации в процессе Интернет-коммуникации. Возможно, не все

термины данной области, объективирующие концепты, характеризующие описываемую ситуацию, были учтены нами. В работе также не рассматривались обозначения концептов, имеющие обобщающий характер, выступающие именами одноименных категорий и представленные в дефинициях этих концептов/понятий (например, *computer program*). Тем не менее, проведенный анализ позволяет сделать определенные выводы о роли интерпретирующей деятельности сознания и интерпретирующей функции языка в порождении терминологических номинаций, репрезентирующих экспертное знание.

Заключение

Реконструкция ментальной структуры хранения экспертного знания о прототипической ситуации, репрезентирующей множество вариантов ее реализации в реальном мире, наряду с анализом объективирующих ее элементы языковых единиц-терминов, подтверждает взаимодействие ментальных и языковых процессов и механизмов. Концептуализация и интерпретация действуют практически одновременно на ментальном и языковом уровнях, обусловливая выбор вербальной формы передачи полученной информации/знания. Несмотря на то, что в специализированных областях их действие в определенной степени зависит от контекста (домена, области экспертного знания), субъект познавательной деятельности активирует всю базу имеющегося у него знания, что позволяет создавать не только языковые знаки с легко читаемой внутренней формой, эксплицирующей содержание концепта, но и образные номинации, семантика составных элементов которых может имплицировать отдельные смыслы, либо такие единицы никаким образом не отражают это содержание, характеризуясь идиоматичностью.

Активация базы знания субъекта с целью сопоставления новой информации с имеющимся знанием обеспечивает действие таких когнитивных механизмов как фокусирование, или профилирование (отдельных смыслов), концептуальная деривация, концептуальная метонимия, метафора и метафтонимия. Профилируемые, или фокусируемые смыслы (концептуальные и атрибутивные признаки) соответствуют направлениям интерпретации знания.

На языковом уровне языковые механизмы реализуют действие когнитивных механизмов. Интерпретация и объективация экспертного знания посредством языка осуществляется через механизмы метонимического и метафорического переноса значения, словопроизводства, включая производство сложных, сложнопроизводных единиц и аналитических дериватов, аббревиацию.

Созданные обозначения отдельных концептов/понятий области информационной безопасности свидетельствуют о реализации селективной функции интерпретации мира в языке. Термины, представляющие обозначения концептов на суперординатном уровне, служащие также названиями категорий данной экспертной сферы деятельности, свидетельствуют о наличии у интерпретации классифицирующей функции. В формировании терминологических номинаций, содержащих единицы с оценочной семантикой, усматривается проявление оценочной функции интерпретации. Анализ созданных субъектами научно-практической деятельности терминологических единиц подтверждает особую роль языковой когниции в процессе терминопорождения: без знания языка (и в частности, моделей словопорождения) объективация субъектами результатов познавательной деятельности в экспертной области была бы невозможна.

Список источников

1. Macmillan English Dictionary for Advanced Learners. Bloomsbury Publishing. 2002. – 1692 p.
2. Information Security Glossary of Terms. Recommended Practice. – Washington, DC, USA. Magneta Book. 2020. – 30 p.
3. Paulsen C., Buyers R. Glossary of Key Information Security Terms / editor R. Kissel. – US Department of Commerce. National Institute of Standards Technology. 2019. – 223 p.
4. Online etymology dictionary. URL: https://www.etymonline.com/ (дата обращения: 28.04.2023).
5. Rigdon J.C. Dictionary of Computer and Internet terms (in 2 volumes). – Microsoft Corporation. Eastern Digital Resources. 2016. – 1447 p.
6. Top Cybersecurity Terms. URL:https://www.allot.com/100-plus-cybersecurity-terms-definitions/ (дата обращения: 27.04.2023).
7. Social Research Glossary URL: https://www.qualityresearchinternational.com/socialresearch/socialengineering.htm (дата обращения: 03.05.2023).

8. Washo A.H. An interdisciplinary view of social engineering: A call to action for research // Computers in Human Behavior Reports. 2021 – Vol. 4 – Pp. 100-126.
9. 100+Cybersecurity Terms. URL:https://www.globalknowledge.com/ca-en/topics/cybersecurity/glossary-of-terms/ (дата обращения: 27.04.2023).

References

1. Macmillan English Dictionary for Advanced Learners. – Bloomsbury Publishing. 2002. – 1692 p.
2. Information Security Glossary of Terms. Recommended Practice. – Washington, DC, USA. – Magneta Book. 2020. – 30 p.
3. Paulsen C., Buyers R. Glossary of Key Information Security Terms / editor R. Kissel. – US Department of Commerce. National Institute of Standards Technology. 2019. – 223 p.
4. Online etymology dictionary. URL: https://www.etymonline.com/ (date of application: 28.04.2023).
5. Rigdon J.C. Dictionary of Computer and Internet terms (in 2 volumes). Microsoft Corporation. Eastern Digital Resources. 2016. – 1447 p.
6. Top Cybersecurity Terms. URL:https://www.allot.com/100-plus-cybersecurity-terms-definitions/ (date of application: 27.04.2023).
7. Social Research Glossary URL: https://www.qualityresearchinternational.com/socialresearch/socialengineering.htm (date of application: 03.05.2023).
8. Washo A.H. An interdisciplinary view of social engineering: A call to action for research // Computers in Human Behavior Reports. 2021 – Vol. 4 – Pp. 100-126.
9. 100+Cybersecurity Terms. URL:https://www.globalknowledge.com/ca-en/topics/cybersecurity/glossary-of-terms/ (date of application: 27.04.2023).

Дроздова Татьяна Васильевна	доктор филологических наук, доцент, Астраханский государственный технический университет, Астрахань, Астрахань drozdova@astu.org
Drozdova Tatyana Vasilievna	doctor of philology, associate professor, Astrakhan state technical university, Astrakhan drozdova@astu.org