УДК 81-139

DOI: 10.15593/2224-9389/2020.4.4

Я.Н. Березина

Получена: 03.09.2020

Принята: 15.10.2020

Опубликована: 20.01.2021

Санкт-Петербургский Федеральный
исследовательский центр Российской
академии наук,
Санкт-Петербургский институт информатики
и автоматизации Российской академии наук,
Лаборатория кибербезопасности
и постквантовых криптосистем,
Санкт-Петербург, Российская Федерация

СТРУКТУРНО-СЕМАНТИЧЕСКИЕ ОСОБЕННОСТИ ТЕРМИНОВ В СОВРЕМЕННОМ АНГЛИЙСКОМ ЯЗЫКЕ НА МАТЕРИАЛЕ ПОДЪЯЗЫКА КРИПТОГРАФИИ

Проведено комплексное исследование английской терминологии подъязыка криптографии в структурно-семантическом аспекте. Криптография является одной из самых древних научных дисциплин, которая насчитывает приблизительно 4500 лет. История развития криптографии проделала длинный путь от этапа наивной криптографии до этапа компьютерной криптографии. И на протяжении всего этого времени параллельно с развитием данной науки развивалась и ее терминосистема. В настоящее время терминология криптографии представляет собой специфический пласт лексики, включающий в себя однокомпонентные и многокомпонентные термины, охватывающие такие разделы криптографии, как получение скрытой информации, симметричные и асимметричные криптосистемы, квантовую криптографию, управление ключами, хеш-функции, системы электронной цифровой подписи и другие. Материалом исследования послужили 358 слов и словосочетаний, которые относятся к английской терминологии в области криптографии, отобранные методом сплошной выборки из словарей и тематических интернет-ресурсов. Научная новизна работы заключается в том, что в ней впервые осуществлен структурно-семантический анализ терминологической лексики подъязыка криптографии в английском языке. Также проведена систематизация отобранных терминов по их тематическим группам и подгруппам. Специфика данной терминосистемы заключается в том, что по мере расширения научного знания в области криптографии растет число терминов с несколькими компонентами, что обусловлено тенденцией к точности выражения смысла терминов, так как с добавлением компонентов в термине уменьшается степень его полисемии, что важно при наличии быстрорастущего количества терминов в данной сфере.

Ключевые слова: терминология, терминосистема, подъязык криптографии, криптография, английский язык.

Ya.N. Berezina

Federal Research Center of the Russian Academy
of Sciences (SPC RAS),
St. Petersburg Institute for Informatics
and Automation of the Russian Academy
of Sciences, Laboratory of Cybersecurity
and Post-quantum Cryptosystems,
St. Petersburg, Russian Federation

Received: 03.09.2020

Accepted: 15.10.2020

Published: 20.01.2021

STRUCTURAL AND SEMANTIC FEATURES OF TERMS IN MODERN ENGLISH ON THE MATERIAL OF THE SUBLANGUAGE OF CRYPTOGRAPHY

The article is devoted to a comprehensive study of the English terminology of the cryptography sublanguage in the structural and semantic aspect. Cryptography is one of the oldest scientific disciplines, dating back approximately 4,500 years. The history of the development of cryptography has come a long way from the stage of naive cryptography to the stage of computer cryptography. And throughout this time, in parallel with the development of this science, its terminological system also developed. Currently, the terminology of cryptography is a specific layer of vocabulary, which includes single-component and multi-component terms covering such sections of cryptography as obtaining hidden information, symmetric and asymmetric cryptosystems, quantum cryptography, key management, hash functions, electronic digital signature systems and others. The research material was 358 words and phrases that relate to English terminology in the field of cryptography, selected by continuous sampling from dictionaries and thematic Internet resources. The scientific novelty of the work lies in the fact that it was the first to carry out a structural-semantic analysis of the terminological vocabulary of the cryptography sublanguage in English. The systematization of the selected terms by their thematic groups and subgroups was also carried out. The specificity of this term system is proved by the fact that as scientific knowledge in the field of cryptography expands, the number of terms with several components increases due to the tendency towards the accuracy of expressing the meaning of terms. With the addition of components in a term, the degree of its polysemy decreases, which is important in the presence of the rapidly growing number of terms in a given area.

Keywords: *terminology, sublanguage of cryptography, cryptography, the English language, cryptography terms.*

Введение

Благодаря стремительному развитию науки изучение и анализ терминологии являются одной из наиболее важных проблем общего языкознания в современном мире. На данный момент исследование терминологии представляет собой отдельную дисциплину, которая характеризуется своими методами и предметом исследования. Терминология активно привлекает внимание исследователей, так как в ней отражаются процессы не только научно-технического прогресса, но также и социального развития общества.

Место термина в лексической системе языка

Широкая распространенность терминов в научно-технических текстах обусловлена необходимостью в обозначении комплексных однокомпонентных и многокомпонентных понятий, а также уточнении тех или иных явлений, закономерностей или профессиональных объектов по мере их изучения.

Несмотря на огромное количество исследований в области терминологии (работы Г.О. Винокура, Б.Н. Головина, Д.С. Лотте, А.А. Реформатского, С.В. Гринева и др.), до сих пор не было выделено единого и общепринятого понятия «термин».

Существуют три основные точки зрения ученых о том, какое место занимает термин во всей лексической системе языка [1]:

- 1) термины являются искусственно созданными знаками;
- 2) термины являются частью лексики литературного языка;
- 3) термины образуют автономный раздел лексики.

По мнению А.В. Суперанской, каждая из этих точек зрения является верной в связи с тем, что она возникла в определенных условиях у тех или иных исследователей, поэтому, основываясь на каждую из них, можно построить свою концепцию терминологии и самого термина [2].

С точки зрения А.А. Реформатского, термины – это «слова специальные, ограниченные своим особым назначением; слова, стремящиеся быть однозначными как точное выражение понятий и название вещей» [3].

В свою очередь, исследователь В.В. Виноградов выделил следующую роль термина в лексической системе языка: «слово выполняет номинативную или дефинитивную функцию, или является средством четкого обозначения, и тогда оно – простой знак, или средством логического определения, тогда оно – научный термин» [4, с. 12–13].

С позиции исследователя И.С. Квитко, «термин – точный носитель информации о научном понятии» [5, с. 19].

В своей работе «Терминоведение» В.М. Лейчик отмечает, что «термин – это лексическая единица определенного языка для специальных целей, обозначающая общее – конкретное или абстрактное – понятие теории определенной специальной области знаний или деятельности» [6, с. 21].

В данной работе при анализе терминологии подязыка криптографии будет использоваться определение понятия «термин» исследователя В.М. Лейчика.

Подязык сферы криптографии

Объединение терминов по определенной тематике называется подязыком. Научная речь и подязыки представляют огромный интерес для исследователей, так как любой подязык сочетает в себе как общую, так и специальную лексику.

На данный момент большое внимание привлекает к себе подязык криптографии с его широко используемой и стремительно развивающейся терминосистемой. Криптография является одной из самых древних научных дисциплин, которая насчитывает около 4500 лет. Это связано с тем, что на протяжении развития письменности шифрованию и дешифрованию сообщений и информации уделялось большое внимание, так как человечество нуждалось не только в сокрытии определенной информации (шифровании), но и в ее открытии (дешифровании). История развития криптографии проделала длинный путь от этапа наивной криптографии до этапа компьютерной криптографии. И с XX века акцент данной науки сместился с языковедческих образцов на математику. В настоящее время криптография представляет собой комплексную и интенсивно развивающуюся науку, которая включает в себя множество различных разделов: получение скрытой информации, симметричные и асимметричные криптосистемы, квантовую криптографию, управление ключами, хеш-функции, системы электронной цифровой подписи (ЭЦП) и др.[7].

Данные изменения нашли отражение в терминологии криптографии. Однако, несмотря на широкую востребованность этой науки во всем мире, до сих пор не проводилось изучение ее терминосистемы, поэтому целью данного исследования является изучение подязыка криптографии в структурно-семантическом аспекте для установления универсальных специфических свойств данной терминосистемы.

Материалом исследования послужили 358 слов и словосочетаний, которые относятся к английской терминологии в области криптографии и отобраны из следующих словарей: Oxford dictionary of English [8], Collins English dictionary and thesaurus [9], Chambers Dictionary of Synonyms and Antonyms [10], Webster's New World Dictionary of Synonyms [11], а также специальных тематических интернет ресурсов [12–15].

Структурные особенности криптографических терминов

Проанализировав структуру английских терминов подязыка криптографии, можно выделить следующие группы:

1. Однокомпонентные термины, составляющие 17 % от общего количества проанализированных терминов. Например: *cryptography, code, cryptogram, cracking, cryptograph, cryptanalyst, algorithm, blockchain, protocol, cipher, encryption, coding, decoding*.

2. Двухкомпонентные термины, составляющие 46 % от общего количества проанализированных терминов. Например: *coded message, cryptographic systems, encrypted message, symmetric cryptosystem, asymmetric cryptosystem, secret language, digital signature, hash functions, dictionary attack, message authentication*.

3. Трехкомпонентные термины, составляющие 23 % от общего количества проанализированных терминов. Например: *digital signature standart, file transfer protocol, rainbow table attack, public key cryptography, server gated cryptography*.

4. Четырехкомпонентные термины, составляющие 8 % от общего количества проанализированных терминов. Например: *secret key message authentication, authenticated secret key encryption, shared secret key agreement*,

5. Пятикомпонентные термины, составляющие 6 % от общего количества проанализированных терминов. Например: *secure multipurpose internet mail extensions, hash-based message authentication code, derived unique key per transaction*.

Анализируя полученные данные, необходимо отметить, что количество многокомпонентных терминов в подязыке криптографии значительно превышает число однокомпонентных. Двухкомпонентные термины составляют 46 % и трехкомпонентные – 23 % от общего количества рассматриваемых терминов, из чего можно сделать вывод, что термины с двумя и тремя компонентами наиболее часто применяются в сфере криптографии в связи со своей краткостью, точностью, простотой и контекстуальной независимостью. Далее по мере увеличения компонентов прослеживается уменьшение числа терминов. Так, пятикомпонентные термины составили всего 6 % от всех проанализированных терминов. Также чем выше число компонентов в термине, тем чаще начинают применяться аббревиатуры, что связано с удобством их использования. Например: *(SASL) Simple Authentication and Security Layer, (CHAP) Challenge-Handshake Authentication Protocol, (S/MIME) Secure Multipurpose Internet Mail Extensions*.

Проведенный анализ показал, что широкое распространение терминов с несколькими компонентами указывает на то, что они представляют собой оптимальное языковое средство при номинации тех или иных научных явлений, процессов и понятий в современной науке. Более того, многокомпонентные термины находятся среди важнейших лексических конститuentов научного текста вследствие своей большой семантической емкости.

Также необходимо отметить, что характерной особенностью терминов с несколькими компонентами, которая отличает их от однокомпонентных терминов, является устойчивость к проявлению неоднозначности в другом макроконтексте. Так, *secret key message authentication* сохраняет свое значение при переходе из терминологии криптографии в терминологию смежных научных областей.

Семантические особенности криптографических терминов

С точки зрения семантического содержания криптографических терминов английского языка были выделены следующие группы:

1. Термины, относящиеся к криптографическим алгоритмам, которые, в свою очередь, делятся на:

а) бесключевые алгоритмы, которые не используют в своих вычислениях никаких ключей. К этой группе относятся следующие термины: *hash functions, hash, keyless cryptography*;

б) одноключевые алгоритмы, с помощью которых можно шифровать и дешифровать информацию, используя один и тот же ключ. Например: *Twofish, Blowfish, Serpent, International Data Encryption Algorithm, Data Encryption Standard, Secret-Key Message Authentication, Secret-Key Encryption, Authenticated Secret-Key Encryption*;

в) двухключевые алгоритмы, в которых на различных стадиях работы применяется открытый ключ для шифрования информации, а закрытый – для ее дешифрования. Например: *RSA Algorithm, Diffie-Hellman Algorithm, Escrowed Encryption Standard, Digital Secure Algorithm, Error-Correcting Code Memory, Shared Secret Key Agreement*.

2. Термины, обозначающие составные части и процесс создания алгоритма. Например: *plaintext, key size, key length, block size, block cipher, stream cipher, throughput*.

3. Термины, относящиеся к процессу шифрования информации. Например: *code, coded message, cryptogram, cryptograph, cipher, encryption key, encrypted message, encryption, coding, encryption scheme, encryption time*.

4. Термины, которые относятся к процессу дешифрования информации. Например: *decoding, decryption, decryption key, decipherment, decryption time*,

5. Термины, относящиеся к видам атак с целью взлома зашифрованных данных. Например: *brute force attack, dictionary attack, rainbow table attack*.

В результате проведенного семантического анализа терминологии подязыка криптографии было установлено, что термины с одним компонентом в большинстве случаев выражают базовые понятия, которые относятся к процессу шифрования и дешифрования. Например: *code, cipher, decoding, decipherment, decryption*. В свою очередь, многокомпонентные термины чаще всего обозначают понятия, которые относятся к различным видам криптографических алгоритмов. Например: *Secret-Key Message Authentication, Secret-Key Encryption, Authenticated Secret-Key Encryption*. Более того, чем больше частей в криптографическом термине, тем точнее он передает то или иное понятие. В качестве примера можно рассмотреть пятикомпонентный термин: *hash-based message authentication code*. Данный многокомпонентный термин максимально передает функции описываемого объекта *code*. Благодаря компоненту *authentication* очевидно, что это не обычный код, а код аутентификации сообщений (проверки подлинности), а по компонентам *hash-based message* понятно, что это код, который использует хэш-функции. Из этого следует, что с помощью различных определителей и детализаторов базисный термин приобретает качество повышенной информативности, общее значение которого уточняется и конкретизируется. В то же время весь комплекс

компонентов передает понятийное содержание термина, а не одно конкретное слово.

Кроме того, в результате проведенного анализа было замечено, что в подязыке криптографии наряду с терминами активно используются слова общей лексики. Например: *task, problem, digit, message, key, analysis, scheme, sender, recipient, numbers*. Данные слова не обозначают понятия, которые относятся только к подязыку криптографии, поэтому они не были рассмотрены в проведенном исследовании.

Заключение

В результате проведенного исследования подязыка криптографии было установлено, что главной структурной особенностью криптографических терминов является преобладание двухкомпонентных и трехкомпонентных терминов. Данное явление обусловлено тенденцией к точности выражения смысла того или иного термина, так как с добавлением компонентов в термине уменьшается степень его полисемии, что важно при наличии быстрорастущего количества терминов в данной сфере.

Более того, к семантической особенности можно отнести то, что однокомпонентные термины выражают базовые понятия, относящиеся к процессу шифрования и дешифрования, в то время как многокомпонентные термины используются для обозначения различных криптографических алгоритмов.

Таким образом, в современных условиях ускоренного научно-технического прогресса терминология приобретает особое значение, так как является одним из главных способов сохранения новой информации и обмена ею. Терминология криптографии в английском языке представляет собой широкий пласт лексики с определенными структурно-семантическими особенностями, который значительно отличается от общеупотребительных слов и от литературного языка, и вследствие чего занимает особое место в лексической системе английского языка.

Список литературы

1. Бугорская Н.В. Проблема термина и терминологические проблемы. – Барнаул: Изд-во Алтайск. гос. ун-та, 2007.
2. Суперанская А.В., Подольская Н.В., Васильева Н.В. Общая терминология: Вопросы теории. – М.: Едиториал УРСС, 2003.
3. Реформатский А.А. Введение в языковедение. – М.: Аспект Пресс, 2010.
4. Виноградов В.В. Русский язык (Грамматическое учение о слове). – М.: Учпедгиз, 1947.
5. Квитко И.С. Термин в научном документе. – Львов: Вища школа, 1976.
6. Лейчик В.М. Терминоведение: предмет, методы, структура. – М.: ЛИБРОКОМ, 2009.

7. Молдовян Н. А. Криптография: от примитивов к синтезу алгоритмов. – СПб.: БХВ-Петербург, 2004.
8. Stevenson A. (ed.). Oxford dictionary of English. – Oxford University Press, USA, 2010.
9. Sinclair J.M. (ed.). Collins English dictionary and thesaurus. – NY.: Harper Collins, 1993.
10. Manser M.H. (ed.). Chambers Synonyms and Antonyms. – Chambers Harrap Publishers L, 2004.
11. Webster's II New College Dictionary / Webster's New World Dictionary et al. (ed.). – Houghton Mifflin Harcourt, 2005.
12. A Survey on Cryptography Algorithms [Электронный ресурс]. – URL: https://www.researchgate.net/publication/326582882_A_Survey_on_Cryptography_Algorithms (дата обращения: 27.08.2020).
13. Cryptography Terms and Concepts for Developers [Электронный ресурс]. – URL: <https://dev.to/paragonie/you-wouldnt-base64-a-password-cryptography-terms-and-concepts-for-developers> (дата обращения: 27.08.2020).
14. What is Cryptography? – An Introduction to Cryptographic Algorithms [Электронный ресурс]. – URL: <https://www.edureka.co/blog/what-is-cryptography/> (дата обращения: 27.08.2020).
15. Explain the term Cryptography in brief [Электронный ресурс]. – URL: <https://www.golangprograms.com/what-is-cryptography.html> (дата обращения: 27.08.2020).

References

1. Bugorskaia N.V. Problema termina i terminologicheskie problemy [The term problem and terminological problems]. Barnaul, Altai State University, 2007.
2. Superanskaia A.V., Podol'skaia N.V., Vasil'eva N.V. Obshchaia terminologiya: Voprosy teorii [General terminology: Theoretical issues]. Moscow, Editorial URSS, 2003.
3. Reformatskii A.A. Vvedenie v iazykovedenie [Introduction to linguistics]. Moscow, Aspekt Press, 2010.
4. Vinogradov V.V. Russkii iazyk (Grammaticheskoe uchenie o slove) [The Russian language (Grammatical teaching about the word)]. Moscow, Uchpedgiz, 1947.
5. Kvitko I.S. Termin v nauchnom dokumente [Term in a scientific document]. Lvov, Vishcha shkola, 1976.
6. Leichik V.M. Terminovedenie: predmet, metody, struktura [Terminology: subject, methods, structure]. Moscow, LIBROKOM, 2009.
7. Moldovian N.A. Kriptografiia: ot primitivov k sintezu algoritmov [Cryptography: From primitives to algorithm synthesis]. St. Petersburg, BKhV-Peterburg, 2004.
8. Stevenson A. (ed.). Oxford dictionary of English. Oxford University Press, USA, 2010.
9. Sinclair J.M. (ed.). Collins English dictionary and thesaurus. N.Y.: Harper Collins, 1993.
10. Manser M.H. (ed.). Chambers Synonyms and Antonyms. Chambers Harrap Publishers Ltd., 2004.

11. Webster's II New College Dictionary. Houghton Mifflin Harcourt, 2005.
12. A Survey on Cryptography Algorithms. Available at: https://www.researchgate.net/publication/326582882_A_Survey_on_Cryptography_Algorithms (accessed 27 August 2020).
13. Cryptography terms and concepts for developers. Available at: <https://dev.to/paragonie/you-wouldnt-base64-a-password-cryptography-terms-and-concepts-for-developers> (accessed 27 August 2020).
14. What is Cryptography? – An Introduction to cryptographic algorithms. Available at: <https://www.edureka.co/blog/what-is-cryptography/> (accessed 27 August 2020).
15. Explain the term cryptography in brief. Available at <https://www.golang-programs.com/what-is-cryptography.html> (accessed 27 August 2020).

Сведения об авторе

БЕРЕЗИНА Яна Николаевна

e-mail: yana.berezina.french@mail.ru

Младший научный сотрудник Лаборатории кибербезопасности и постквантовых криптосистем, Санкт-Петербургский Федеральный исследовательский центр Российской академии наук; Санкт-Петербургский институт информатики и автоматизации Российской академии наук (Санкт-Петербург, Российская Федерация)

About the author

Yana N. BEREZINA

e-mail: yana.berezina.french@mail.ru

Junior Researcher, Laboratory of Cybersecurity and Post-quantum Cryptosystems, St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS), St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences (Saint-Petersburg, Russian Federation)