УДК 81.26 DOI: 10.14529/ling200110

ЖАНРОВО-СТИЛИСТИЧЕСКИЕ ОСОБЕННОСТИ АНГЛОЯЗЫЧНЫХ НАУЧНЫХ СТАТЕЙ ПО КРИПТОГРАФИИ

Я.Н. Березина
Санкт-Петербургский институт информатики и автоматизации Российской академии наук, г. Санкт- Петербург, Россия

Исследование посвящено рассмотрению жанрово-стилистических особенностей научных ст тей по криптографии на английском языке. Актуальность исследования обусловлена активным и тересом современной лингвистики к научным текстам, в частности к жанру научной статьи, так к наука является одной из главных областей, в которой реализуется доминирующее положение ан лийского языка во всем мире. Его активно используют при проведении международных семинар и конференций, на английском языке публикуются научные статьи, книги, исследования и мон графии ученых из разных стран. Целью данного исследования является выявление жанровых, ле сических, морфологических и синтаксических особенностей англоязычных научных статей криптографии. В ходе исследования были применены следующие методы: текстологический ан лиз, описательный метод и сравнительный метод. Результаты работы позволили выявить и описа жанрово-стилистическую специфику научных статей по криптографии на английском языке. С ласть применения исследования включает в себя возможность применения полученных данных п чтении вузовских курсов по лингвистике, письменному переводу, а также стилистике. Также лог ка и методика исследования могут быть применены для дальнейшего изучения жанровых и стил стических особенностей научных статей на других языках.

Ключевые слова: научный стиль, речевой жанр, английский язык, научная статья, криптография.

В современных условиях глобализации все большую значимость приобретает обмен научными знаниями и последними достижениями в различных отраслях науки. Каждый день появляются сотни научных выводов, достижений и открытий, поэтому исследование научных текстов представляет собой не только важную задачу для научной сферы, но также и для жизни общества в целом. Одним из основных способов передачи последних научных достижений является жанр научной статьи. Анализ научных статей представляет огромный интерес для лингвистов, который в основном сосредоточен на таких аспектах как: цель общения, способ речевого воздействия, различные взаимосвязи компонентов коммуникации и т. д.

Данное исследование направлено на анализ жанрово-стилистических особенностей статей по криптографии. Анализ проводился на материале 30 статей по криптографии на английском языке, опубликованных в следующих научных журналах: Journal of Cryptology; Journal of Mathematical Cryptology; Information Management and Computer Security; International Journal of Information and Computer Security; International Journal of Network Security; The International Arab Journal of Information Technology; International Journal of Information and Computer Security.

Основными для данного исследования являются понятия «речевой жанр» и «научный стиль».

Речевым жанром является относительно устойчивый стилистический, тематический, а также композиционный тип высказываний или текстов [3].

Речевые жанры делятся на простые (первичные) и сложные (вторичные). К простым речевым жанрам относится непосредственно речевое общение. А к сложным – научные статьи, художественные произведения и т. д. [2].

Научный стиль представляет собой функциональный стиль речи, реализующий функцию сообщения. В качестве главных стилевых черт принято выделять точность, сжатость, логичность изложения, информативную насыщенность, формальность, объективность, абстрактность, а также последовательность [1]. Данные стилевые черты наиболее ярко проявляются в жанре научной статьи. Научная статья является законченным авторским произведением, в котором описываются последние результаты исследований и научных открытий [5].

Основными функциями научного стиля являются передача логической информации, доказательство ее новизны и ценности, а также активизация логического мышления читателя [8].

Жанровые особенности

Основной целью научного дискурса является сообщение о проведенных исследованиях и способах их получения, полученный результат, а также формулировка и обоснование новых идей. Как следствие, научный дискурс в основном состоит из рассуждения и описания [6].

Главная цель жанра научной статьи – информативная. В анализируемых статьях авторы сообщают результаты последних научных исследований и открытий по криптографии.

В научных статьях автор часто прямо формулирует цель своего исследования:

1. *This work focuses* the problem of increasing the integral implementation efficacy of block ciphers [16].

2. *The paper develops* the cipher design approach based on the use of data-dependent (DD) operations (DDOs) [16].

Автор текста выступает в роли специалиста в области криптографии, адресаты научного текста – специалисты, интересующиеся последними результатами фундаментальных и прикладных исследований в области систем и средств защиты информации.

Тема анализируемых статей – сфера криптографии. В рассматриваемых научных статьях исследуются актуальные проблемы систем и способов шифрования, алгоритмы и протоколы цифровой подписи, аутентификация, виды шифрования, эффективные средства защиты информации.

Текст научной статьи обычно делится на несколько основных частей: введение, основная часть и заключение. Средний объем анализируемых статей – 5–10 страниц.

Основное содержание научных статей в сфере криптографии включает большой объем не только теоретической, но и практической информации, поэтому текст статьи содержит формулы, графики, схемы, таблицы и диаграммы.

Лексические особенности

Лексика научных статей по криптографии делится на 3 пласта:

1) Термины *(anonymity, authentication, broadcast encryption, ciphers, cryptography, coded message, cryptogram, cryptanalysis, cipher text, protocol, data security, digital signatures, identification, encrypted message, encryption, coding, decoding, decipherment, decryption, secret key, public key, symmetric cryptosystem, key, distribution, asymemetric cryptosystem, encryption scheme, blockchain, secret language, secret message, secret writing, keyword, watchword).*

Использование научной терминологии является одной из характерных особенностей лексического состава научной литературы. Термины обеспечивают точность и ясность понимания научной мысли. По мнению исследователя В.Н. Комиссарова, терминами являются слова и словосочетания, которые обозначают специфические понятия и объекты, с помощью которых оперируют специалисты в той или иной научной и технической областях. Основными признаками термина являются независимость от контекста, объективность, а также точность [7].

В научных текстах по криптографии термины преобладают над другими видами специальной лексики.

2) Общеупотребительные слова (*plan, example, word, today, this, that, man, to see, to understand, to have, to make, to report, important, difficult, practical, great, possible*).

Другой особенностью научного текста является использование общеупотребительных слов. Доля общеупотребительной лексики в научной прозе может меняться в зависимости от состава читателей. Тексты, которые направлены на широкий круг читателей, содержат в себе большой процент общеупотребительной лексики, а в текстах, предназначенных для специалистов той или иной научной области, этот процент значительно снижается [4].

В научных статьях по криптографии доля общеупотребительных слов незначительная. Это связано с тем, что статьи данной тематики в основном предназначены для специалистов, которые интересуются проблемами защиты информации, а не для широкого круга читателей.

3) Общенаучные слова (*information, modernization, addition, introduction, modification, variation, analysis, exploration, study, issue, importance, research, innovation, solution, acknowledgement, conditions, trend, rates, acceptance, effects, factors, direction, tendency*).

Общенаучные слова представляют собой неотъемлемый пласт научной речи, которые используются для описания научных явлений и объектов в разных областях науки и техники [4].

В научных текстах по криптографии авторы часто используют общенаучные слова для описания своей научной деятельности.

Морфологические особенности

Для обозначения своего мнения автор использует личное местоимение 1-го лица в форме именительного падежа множественного числа в активной конструкции. Преобладание именных конструкций в научных статьях дает возможность большего обобщения.

1. *We have* also *performed* statistic experiments that proved the theoretic calculation [16].

2. In Eagle-128 *we have used* an advanced cryptoscheme providing transformation of both the left and the right data subblocks, the time delay of one round being significantly reduced [17].

3. *We present* two variants of our scheme [11].

Для характеристики своей интеллектуальной деятельности автор использует пассивные конструкции.

1. In this paper, another approach to increase the efficiency of the FPGA implementation of the DDO-based ciphers *is introduced* [16].

2. Further research *is needed* to optimize the cryptographic protocols for use in the private cloud [12].

Наряду с пассивными конструкциями в научных статьях часто употребляются конструкции с “one” и безличной формой с “It”.

1. Taken together, *one* could argue that the two results are in some sense incomparable [9].

2. Now *one* can see the results [20].

3. *It is obvious that* the proposed applied methodology of Eagle-128 achieves higher through put values [16].

4. *It seems that* the blind collective DS scheme is attractive for application in the electronic money systems in which the electronic banknotes are issued by several banks [16].

Также научные статьи по криптографии содержат большое количество схем, таблиц и формул и указания на них по тексту.

1. The same considerations regarding the use of a safe prime and decoding efficiency as in *Section 7* apply here [10].

2. Formally, the obfuscated program is given in *Algorithm 3* [19].

3. It follows that *Problem 5.1* has a spectrum of difficulty, ranging from easy in the extreme low-density case to hard in the medium-/high-density case [15].

Синтаксические особенности

Одной из главных особенностей синтаксиса научного стиля является преобладание сложноподчиненных предложений. Немногочисленные простые предложения отличаются наличием большого количества однородных членов. Связи между элементами в научном тексте выражены эксплицитно, что ведет к использованию разнообразных союзных слов и союзов, таких как: than, or, that, as, and that, thereby, therewith, therefore, hereby, hence, а также двойных союзов: as... as, both…and, whether… or, not merely…but also.

1. About 1960, cryptosystems were put into service which were deemed strong enough to resist a known plaintext cryptanalytic attack, *thereby* eliminating the burden of keeping old messages secret [18].

2. These concerns are mainly about the cloud operators having the chance of reaching the sensitive data, and *therefore* reduce the adoptability of cloud computing in many fields, such as the financial industry and governmental agencies [14].

3. *Hence*, it is potentially easier to instantiate (with a concrete hash fiction) the Fiat-Shamir transform for the construction in this paper [14].

Строгое деление на абзацы играет одну из главных ролей в раскрытии логической структуры научной статьи. Каждый абзац начинается с ключевого предложения, в котором, как правило, заключена основная мысль. Для того чтобы усилить логическую связь между предложениями, часто используются устойчивые выражения и наречия: nevertheless, taking into consideration, taking into account, to sum up, to conclude, on the other hand, as a result, thanks to, instead of, finally, thus, in addition, again, indeed, actually, besides, moreover и т. д.

1. *Nevertheless*, the GOST R 34.10-94 or GOST R 34.10-2001 (like DSA and ECDSA) are official standard [16].

2. *Thus*, the protocol performs correctly [10].

3. *Besides,* the NL value and the algebraic degree of BF, differential characteristics (DCs) of the CE are important to characterize CEs as cryptographic primitives [16].

4. *In addition*, two comparison models, Performance/Area and Performance/ (Area*Frequency), are used [19].

Также логическое подчеркивание может выражаться лексически: to note, in consequence of this, another point of considerable interest is, it is by no means trivial, the problem is, one interesting method is и т. д.

1. *Note that* Definition 4.1 for VBB obfuscation is given in asymptotic terms with respect to a security parameter λ [13].

2. *One interesting method* to build block ciphers *is* which hardware-oriented ciphers based on controlled operations [15].

Заключение

Жанр научной статьи в англоязычном научном дискурсе обладает рядом специфических черт. Основная цель коммуникации анализируемого жанра – информативная. Содержанием статьи является описание последних научных исследований и их результатов.

Стилистические особенности англоязычных научных статей по криптографии включают в себя: широкое использование научной терминологии, общенаучной и нейтральной лексики; использование пассивных конструкций, безличных предложений и авторского (лекторского) «мы»; преобладание сложноподчиненных предложений, прямой порядок слов, разнообразие союзов и специальных вводных выражений.

Также необходимо отметить, что стремительное развитие науки и техники приводит к необходимости формирования специального языка, с помощью которого можно было бы наилучшим образом передавать научные знания разным адресатам, а также описывать новые реалии. И важную роль в решении этой задачи играет лингвистический анализ научных статей на разных языках.

Литература

1. Арнольд, И. В. Стилистика. Современный английский язык: учебник для вузов / И.В. Арнольд. – 4-е изд., испр. и доп. – М.: Флинта: Наука, 2002. – 384 с.

2. Бахтин, М.М. Проблема речевых жанров / М.М. Бахтин // Литературно-критические статьи. – М., 1986. – С. 428–472.

3. Бахтин, М.М. Эстетика словесного творчества / М.М. Бахтин. – М.: Искусство, 1979.

4. Ванников, Ю.В. Типы научных и технических текстов и их лингвистические особенности / Ю.В. Ванников. – М.: ВЦП, 1984. –240 с.

5. Гальперин, И.Р. Стилистика английского языка / И.Р. Гальперин. – М.: Высшая школа, 1981. – Т. 334. – С. 4.

6. Кашкин, В.Б. Научный дискурс: теория и практика: учеб. пособие / В.Б. Кашкин, А.А. Болдырева. – Воронеж: Воронежский гос. техн. ун-т, 2005. – Научный дискурс. – 252 с.

7. Комиссаров, В.Н. Теория перевода / В.Н. Комиссаров. – М., 1990. – Т. 8.

8. Чернявская, В.Е. Некоторые текстообразующие факторы научно-критического текста / В.Е. Чернявская; Акмол. ЦНТИ. Отд. межотрасл. информ. – Акмола: Акмол. обл. межотрасл. УНТИ, 1995. – 170 с.

9. Chakraborti, A. On the optimality of non-linear computations for symmetric key primitives / A. Chakraborti, D. Nilanjan, N. Mridul // Journal of Mathematical Cryptology. – 2019. – Vol. 12, no. 4. – P. 241–259.

10. Gayathri, J. A survey on security and efficiency issues in chaotic image encryption / J. Gayathri, S. Subashini // International Journal of Information and Computer Security. – 2016. – Vol. 8, no. 4. – P. 347–381.

11. Hermelin, M. Multidimensional Linear Cryptanalysis / M. Hermelin, J.Y. Cho, K. Nyberg // Journal of Cryptology. – 2019. – Vol. 32, no. 1. – P. 1–34.

12. Jakobsen, S.K. Information Theoretical Cryptogenography / S.K. Jakobsen // Journal of Cryptology. – 2017. – Vol. 30, no. 4. – P. 1067–1115.

13. Jovanovic, P. Beyond Conventional Security in Sponge-Based Authenticated Encryption Modes / P. Jovanovic, A. Luykx, B. Mennink // Journal of Cryptology. – 2019. – V. 32, no. 3. – P. 895–940.

14. Kuppuswamy, P. Hybrid encryption/ decryption technique using new public key and symmetric key algorithm / P. Kuppuswamy, S.Q. Al-Khalidi // International Journal of Information and Computer Security. – 2014. – Vol. 6, no. 4. – P. 372–382.

15. Maene, P. Single-Cycle Implementations of Block Ciphers / P. Maene, I. Verbauwhede // Proceeding LightSec 2015 Revised Selected Papers of the 4th International Workshop on Lightweight Cryptography for Security and Privacy. – 2015. – V. 9542. – P. 131–147.

16. Moldovyan, N.A. New Class of Cryptographic Primitives and Cipher Design for Networks Security / N.A. Moldovyan, A.A. Moldovyan, M.A. Eremeev, N. Sklavos // International Journal of Network Security. – 2006. – Vol. 2, no. 2. – P. 114–125.

17. Moldovyan, N.A. Pure DDP-Based Cipher: Architecture Analysis, Hardware Implementation Cost and Performance / N.A. Moldovyan, N. Sklavos, O. Koufopavlou. // Int. Arab J. Inf. Technol. – 2005. – No. 2. – P. 24–32.

18. Rakesh, K. A novel framework for secure file transmission using modified AES and MD5 algorithms / K. Rakesh, M. Geetu // International Journal of Information and Computer Security. – 2015. – Vol. 7. – No. 2/3/4. – P-91-112.

19. Ratnakumari, C. Additively LWE Based Homomorphic Encryption for Compact Devices with Enhanced Security / C. Ratnakumari, V.K. Gunta // International Journal of Network Security. – 2019. – Vol. 21, no. 3. – P. 378–383.

20. Sujarani, R. A nonlinear two dimensional logistic-tent map for secure image communication / R. Sujarani , D. Manivannan // International Journal of Information and Computer Security. – 2018. – Vol. 10, no. 2/3. – P. 201–215.

Березина Яна Николаевна, младший научный сотрудник лаборатории кибербезопасности и постквантовых криптосистем, Санкт-Петербургский институт информатики и автоматизации Российской академии наук (Санкт-Петербург), yana.berezina.french@mail.ru

Поступила в редакцию 12 августа 2019 г.

DOI: 10.14529/ling200110

GENRE-STYLISTIC FEATURES OF ENGLISH-LANGUAGE SCIENTIFIC ARTICLES ON CRYPTOGRAPHY

I.N. Berezina, *yana.berezina.french@mail.ru*
St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences,
St. Petersburg, Russian Federation

The research is devoted to consideration of genre and stylistic features of scientific articles on cryptography in English. The relevance of the study is due to the active interest of modern linguistics to scientific texts, in particular to the genre of scientific articles, as science is a major domain where the preeminence of English is realized. It is widely used in international workshops and conferences; scientific articles, books, research papers and monographs of scientists from different countries are published in English. The purpose of this research is to specify genre, lexical, morphological and syntactic features of English-language scientific articles on cryptography. The method of textual analysis, descriptive method and comparative method were used in the course of the research. The research results allowed

identifying and describing the genre and stylistic specificity of scientific articles on cryptography in English. The data obtained can be used in teaching university courses in linguistics, translation, and stylistics. Besides, the research methodology can be applied for further study of genre and stylistic features of scientific articles in other languages.

Keywords: scientific style, speech genre, English, scientific article, cryptography.

References

1. Arnol'd, I. V. *Stilistika. Sovremennyj anglijskij yazyk* [Stylistics. Modern English]. 4th ed. Moscow, Flinta, Nauka, 2002. 384 p.
2. Bakhtin M.M. *Problema rechevykh zhanrov* [The problem of Speech Genres]. Moscow, 1986, pp. 428–472.
3. Bakhtin M.M. *Estetika slovesnogo tvorchestva* [Aesthetics of Verbal Creativity]. Moscow, Iskusstvo, 1979.
4. Vannikov Yu.V. *Tipy nauchnykh i tekhnicheskikh tekstov i ikh lingvisticheskie osobennosti* [Types of Scientific and Technical Texts and Their Linguistic Features]. Moscow, VTSP, 1984. 240 p.
5. Gal'perin I.R. *Stilistika anglijskogo yazyka* [Stylistics of the English Language]. Moscow, Vysshaya shkola, 1981, vol. 334, p. 4.
6. Kashkin V.B. *Nauchnyj diskurs: teoriya i praktika: ucheb. posobie* [Scientific Discourse: Theory and Practice: Study Guide]. Voronezh, Voronezh State Technical University, Nauchnyj diskurs, 2005. 252 p.
7. Komissarov V.N. *Teoriya perevoda* [Translation theory]. Moscow, 1990. Vol. 8.
8. Chernyavskaya V.E. *Nekotorye tekstoobrazuyushhie faktory nauchno-kriticheskogo teksta* [Some text-forming factors of a scientific critical text]. Akmol. TSNTI. Otd. mezhotrasl. inform. Akmola: Akmol. obl. mezhotrasl. UNTI, 1995. 170 p.
9. Chakraborti A., Nilanjan D., Mridul N. On the Optimality of Non-Linear Computations for Symmetric Key Primitives. *Journal of Mathematical Cryptology*. 2019, vol. 12, no. 4, pp. 241–259.
10. Gayathri J., Subashini S. A Survey on Security and Efficiency Issues in Chaotic Image Encryption. *International Journal of Information and Computer Security*. 2016, vol. 8, no. 4, pp. 347–381.
11. Hermelin M., Cho J.Y. & Nyberg K. Multidimensional Linear Cryptanalysis. *Journal of Cryptology*. 2019, vol. 32, no. 1, pp. 1–34.
12. Jakobsen S.K. Information Theoretical Cryptogenography. *Journal of Cryptology*. 2017, vol. 30, no. 4, pp. 1067–1115.
13. Jovanovic P., Luykx A., Mennink B. Beyond Conventional Security in Sponge-Based Authenticated Encryption Modes. *Journal of Cryptology*. 2019, vol. 32, no. 3, pp. 895–940.
14. Kuppuswamy P., Al-Khalidi S.Q. Hybrid Encryption/decryption Technique Using New Public Key and Symmetric Key Algorithm. *International Journal of Information and Computer Security*. 2014, vol. 6, no. 4, pp. 372–382.
15. Maene P., Verbauwhede I. Single-Cycle Implementations of Block Ciphers. *Proceeding LightSec 2015 Revised Selected Papers of the 4th International Workshop on Lightweight Cryptography for Security and Privacy*. 2015, vol. 9542, pp. 131–147.
16. Moldovyan N.A., Moldovyan A.A., Eremeev M.A., Sklavos N. New Class of Cryptographic Primitives and Cipher Design for Networks Security. *International Journal of Network Security*. 2006, vol. 2, no. 2, pp. 114–125.
17. Moldovyan N.A., Sklavos N., Koufopavlou O. Pure DDP-Based Cipher: Architecture Analysis, Hardware Implementation Cost and Performance. *Int. Arab J. Inf. Technol*. 2005, no. 2, pp. 24–32.
18. Rakesh K., Geetu M. A novel framework for secure file transmission using modified AES and MD5 algorithms. *International Journal of Information and Computer Security*. 2015, vol. 7, no. 2/3/4, P-91-112.
19. Ratnakumari C., Gunta V. K. Additively LWE Based Homomorphic Encryption for Compact Devices with Enhanced Security. *International Journal of Network Security*. 2019, vol. 21, no. 3, pp. 378–383.
20. Sujarani R., Manivannan D. A Nonlinear Two Dimensional Logistic-tent Map for Secure Image Communication. *International Journal of Information and Computer Security*. 2018, vol. 10, no. 2/3. pp. 201–215.

Iana N. Berezina, junior researcher cybersecurity and post-quantum cryptosystems, St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences (St. Petersburg), yana.berezina.french@mail.ru

Received 12 August 2019

ОБРАЗЕЦ ЦИТИРОВАНИЯ

Березина, Я.Н. Жанрово-стилистические особенности англоязычных научных статей по криптографии / Я.Н. Березина // Вестник ЮУрГУ. Серия «Лингвистика». – 2020. – Т. 17, № 1. – С. 53–57. DOI: 10.14529/ling200110

FOR CITATION

Berezina I.N. Genre-Stylistic Features of English-Language Scientific Articles on Cryptography. *Bulletin of the South Ural State University. Ser. Linguistics*. 2020, vol. 17, no. 1, pp. 53–57. (in Russ.). DOI: 10.14529/ling200110