



Научно-исследовательский журнал «Современный ученый / Modern Scientist»

<https://su-journal.ru>

2025, № 8 / 2025, Iss. 8 <https://su-journal.ru/archives/category/publications>

Научная статья / Original article

Шифр научной специальности: 5.9.8. Теоретическая, прикладная и сравнительно-УДК 81.119

## Механизмы лингвистического шифрования как элемента межкультурной коммуникации

<sup>1, 2</sup> Носова В.Д.

<sup>1</sup> Государственный университет просвещения,

<sup>2</sup> Университет мировых цивилизаций

**Аннотация:** целью проводимого исследования является изучение механизмов лингвистического шифрования как элемента межкультурной коммуникации совместно с диахроническим анализом эволюционных изменений основных положений криптографии от древних методов до современных технологий. К задачам данной работы относится рассмотрение эволюционных изменений лингвистических и математических аспектов кодирования для последующего выявления роли межкультурной коммуникации в процессе совершенствования методов лингвистического шифрования.

В работе использованы методы коммуникативного анализа, включая репрезентацию, семиотическое моделирование, кодирование и декодирование текстов, а также историко-сравнительный анализ криптографических алгоритмов. Автор подчеркивает ключевую роль лингвистического шифрования в обеспечении конфиденциальности данных. Моделирование процессов кодирования, согласно основным положениям шифра Цезаря, квадрата Виженера и машины "Энигма", показало прямую зависимость уровня сложности алгоритма обработки вводящей информации от технологического и культурно-исторического этапа развития социума.

Лингвистическое шифрование как языковая единица реализации межкультурной коммуникации находится на стыке таких наук, как лингвистика, криптография и теория информатики, что позволяет говорить о возможности применения полученных результатов исследования для создания учебно-методических разработок для последующих междисциплинарных исследований, объединяющих языкознание, математику и информатику.

**Ключевые слова:** квадрат Виженера, код, криптография, лингвистическое шифрование, шифр Цезаря, Энигма

**Для цитирования:** Носова В.Д. Механизмы лингвистического шифрования как элемента межкультурной коммуникации // Современный ученый. 2025. № 8. С. 144 – 151.

Поступила в редакцию: 1 апреля 2025 г.; Одобрена после рецензирования: 1 июня 2025 г.; Принята к публикации: 18 июля 2025 г.

## Mechanisms of linguistic encryption as an element of intercultural communication

<sup>1,2</sup> Nosova V.D.

<sup>1</sup> Federal State University of Education,

<sup>2</sup> University of World Civilizations

**Abstract:** the purpose of the research is this study is to examine the mechanisms of linguistic encryption as an element of intercultural communication, combined with a diachronic analysis of the evolutionary changes in cryptographic principles from ancient methods to modern technologies. The objectives of this work include analyze of the evolutionary changes in linguistic and mathematical aspects of encoding together with the identification of the intercultural communication role in improving linguistic encryption methods.

The research employs methods of communicative analysis, including representation, semiotic modeling, text encoding and decoding, as well as historical-comparative analysis of cryptographic algorithms. The author emphasizes the crucial role of linguistic encryption in ensuring data confidentiality. Modeling of encoding processes based on the fundamental principles of the Caesar cipher, the Vigenère square, and the Enigma machine revealed a direct correlation between the complexity of information processing algorithms and the technological and socio-historical stage of societal development.

Linguistic encryption, as a language-based tool for intercultural communication, lies at the intersection of linguistics, cryptography, and information theory. This interdisciplinary nature suggests that the study's findings can be applied to developing educational and methodological materials for future research bridging linguistics, mathematics, and computer science.

**Keywords:** Vigenère square, code, cryptography, linguistic encryption, Caesar cipher, Enigma

**For citation:** Nosova V.D. Mechanisms of linguistic encryption as an element of intercultural communication. Modern Scientist. 2025. 8. P. 144 – 151.

*The article was submitted: April 1, 2025; Approved after reviewing: June 1, 2025; Accepted for publication: July 18, 2025.*

### Введение

Вступление человечества во второе тысячелетие характеризуется не только сменой существующего геополитический миропорядка, но знаменуется фундаментальными изменениями в научных парадигмах многих социально-гуманитарных и технических дисциплин – разработка радиоэлектронных средств коммуникации, положившая начало четвертой информационной революции, обращение к антропоцентрической концепции, развитие учебно-методологической базы межкультурной коммуникации как самостоятельной отрасли лингвистики, возникшей в условиях послевоенных глобализационных процессов и т.п.

В условиях цифровизации всех коммуникативных процессов, которые, в свою очередь, определили создание новых способов обмена как текстовыми, так и аудио- и медиафайлами посредством сети Интернет и соответствующих виртуальных помощников, особое внимание стало уделяться механизмам кодирования вводящих данных с целью уменьшения «объема» транслируемых сообщений для последующего ускорения процесса их передачи, а также соблюдения принципа конфи-

денциальности. Последним уже долгое время занимается такая отрасль языкознания, как лингвистическое шифрование.

### Материалы и методы исследований

Изучение механизмов лингвистического шифрования является перспективным направлением лингвистического исследования. На данном этапе работы нами были использованы следующие методы коммуникативного анализа: метод репрезентации, метод семиотического моделирования, метод кодирования и декодирования текстов и др.

Материалами исследования послужили работы Аризијева А.Т. [2], Бабаша А. В. [3], Жировой И.Г. [1, 5], Здора С.Е. [6], Коржика В.И. [7, 8], Шолина И.М. [7], Harris R. [8], Kahn, D. [9], и др.

### Результаты и обсуждения

XX век как эпоха двух мировых войн дал большой толчок развитию такой науки как криптография, которая направлена на обеспечение конфиденциальности и целостности информации. Данная область знания прошла сложный путь от простых иконических шифров древности до комплексного битового конвертирования, или *хеширования*.

К первым известным человечеству примерам использования механизмов кодирования информации относят *шифр Цезаря*, датируемый I веком до н. э. Римский историк Светоний описывал его как метод целенаправленной замены каждого отдельного символа алфавита ' $N$ ' другой буквой, порядковый номер которой определялся фиксированным шагом. Таким образом, формула преобразования выглядела следующим образом:  $N \rightarrow N + k$ , где  $k$  обычно равнялось 3 (трем) [14]. Данный шифр, в первую очередь, использовался для перевода военных донесений, и для его декодирования использовались специальные приборы под названием скитала, или считала [12].

Попробуем закодировать фразу «Оставь надежду, всяк сюда входящий»/ 'Abandon all hope ye who enter here' из Божественной комедии Данте Алигьери, воспользовавшись формулой « $N \rightarrow N + 3$ » для русского языка и « $N \rightarrow N + 25$ » для английского языка:

Рус.: Оставь надежду, всяк сюда входящий → Сфхгегя ргжзйжц, ефвн фбжг епсжвълм;

Англ.: Abandon all hope ye who enter here → Zazmcnm zkk gnod xd vgn dmsdq gdqd.

Следующей значительной вехой в истории развития криптографии стал отказ от моноалфавитных шифров в пользу полиалфавитных, когда первые стали слишком уязвимы перед методом частотного анализа. Представленный в XV веке Л.Б. Альберти многоалфавитный способ кодирования уже подразумевал использование двух и/или более знаковых алфавитных систем, где переключение между языками также предполагало введение нового логического правила подстановки символа, все еще соответствующего принципу простой замены. На основе данного метода сначала была разработана таблица Тритемия, которая позднее эволюционировала в *квадрат Винжера* (рис. 1).

**Буквы исходного текста**

	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
А	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
Б	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А
В	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б
Г	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В
Д	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г
Е	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д
Ж	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е
З	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж
И	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З
Й	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И
К	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й
Л	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К
М	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л
Н	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М
О	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н
П	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О
Р	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П

**Буквы ключа**

Рис. 1. Квадрат Виженера для русского алфавита.  
Fig. 1. Vigenère cipher for Russian alphabet.

Квадрат или шифр Виженера, который благодаря своей устойчивости к «ручным взломам» просуществовал целых три столетия, был впервые описан в работе Блеза де Виженера '*Traicté des Chiffres*' («Трактат о шифрах»), основное положение которой об универсальности восприятия объектов и явлений окружающей действительности посредством представления их через призму некоего первичного естественного шифра, впоследствии легли в основу теории вероятности и научно-методологический базис кибернетики [3, 15].

Основным отличием подобной системы от ее предшественников стало использование не просто ключевого слова, где каждый символ будет совпадать с определенным шифралфавитом как в таблице Тритемия, а привлечение отдельного открытого текста, используемого в качестве промежуточного этапа для кодирования, который далее будет преобразован согласно данным *tabula recta* – табличный квадрат из 26 латинских букв, где каждый последующий буквенный ряд будет сдвинут влево на одно значение относительно заданной «оси координат» в арифметической прогрессии.

Рассмотрим следующий пример:

- 1) Открытый текст: 'The gostak distims the doshes'
- 2) Ключ 'cipher'
- 3) Код: VPT NSJVIZ KMJVQBZ XYG

LDZLVU

В рамках процесса кодирования исходная фраза фиксируется без пробелов, а ключ расширяется до размеров рассматриваемого сообщения (табл. 1).

Таблица 1

Кодирование сообщения согласно квадрату Вижерена.

Table 1

Message encoding according to the Vigenere square.

	Д А Н О	Т	Н	Е	Г	О	С	Т	А	К	Д	И	С	Т	И	М	С	Т	Н	Е	Д	О	С	Н	Е	С
		19	7	4	6	14	18	19	0	10	3	8	18	19	8	12	18	19	7	4	3	14	18	7	4	18
К Л Ю Ч		С	И	Р	Н	Е	Р	С	И	Р	Н	Е	Р	С	И	Р	Н	Е	Р	С	И	Р	Н	Е	Р	С
		2	8	15	7	4	17	2	8	15	7	4	17	2	8	15	7	4	17	2	8	15	7	4	17	2
И Т О Г		В	Р	Т	Н	С	Ж	В	И	З	К	М	Ж	В	Q	В	З	Х	Y	Г	Л	Д	З	Л	В	U
		21	15	19	13	18	9	21	8	25	10	12	9	21	16	1	25	23	24	6	11	3	25	11	21	20

Таким образом, процесс шифрования исходного текста можно условно представить следующим образом: 1) выбор отрывка из исходного текста; 2) отбор ключевого слова из открытого текста, которое в случае несовпадения исходного количества символов расширяется до необходимого объема путем повторения самого себя по принципу репризы; 3) изменение ключевого слова путем замены каждого отдельного символа согласно данным таблицы Виженера, где новый искомым буквенный знак будет находиться на пересечении «двух осей», где буквы исходного слова отслеживаются по вертикали, а элементы ключа – по горизонтали, или будет вычисляться математически по формуле  $N = (S_n + K_n)$ , где  $S$  – это порядковый номер каждой буквы исходной фразы,  $K$  – порядковый номер элемента ключа,  $n$  – число алфавитных символов в языке кодирования [9].

При этом, параметр  $N$  должен быть меньше или равен  $n$ ; если же сумма  $S$  и  $K$  превышает  $n$ , то отсчет необходимо начать «с нуля» – из первоначально полученной суммы вычитается показатель количества символов в алфавите, а получившееся число используется для дальнейших расчётов.

Так, например, в приведенном выше примере буквы 'М' с порядковым номером 12 и 'Р' номером 15, соответственно, заменяются на В (1) – необходимо отметить, что речь идет о кодировании с использованием средств английского алфавита, состоящего из 26 символов, что в рамках положений классической математики позволяет нам говорить о вычислительных операциях по модулю 26 (mod26). где букве 'А' присвоен порядковый

номер 0. Графически данные преобразования можно представить следующим образом:

$$\left. \begin{array}{l} 12 + 15 = 27 \\ 27 > 26 \end{array} \right\} \rightarrow 27 - 26 = 1$$

Появление телеграфа как продукта третьей информационной революции стало предтечей эпохи средств массовой коммуникации. В связи с этим методы шифрования тоже должны были соответствовать требованиям времени. Отдельно следует выделить предложенный еще в XIX веке метод «блокнотного шифрования», отличавшегося особенной устойчивостью благодаря «повышению» уровня безопасности путем использования одно-разового случайного «ключа», число символов которого изначально равнялось длине входящего сообщения. Подобная вспомогательная «фраза» переводится в последовательность натуральных чисел, где каждая буква сначала меняется на свой порядковый номер в алфавите.

Затем полученный «числовой ключ» суммируют с аналогичным цифровым форматом выражения транслируемой фразы, происходит так называемое сложение единиц шифрования по рассматриваемому модулю, полученный результат снова «переводят» в буквенную форму. Подобный процесс «симметричного наложения» числовой последовательности также принято называть гаммированием [8].

В приведенном ниже примере фраза «Глокая куздра кудрячит бокренка» гаммируется по mod33 и на выходе превращается в шифр ЫПУБЖЩ АСИРЕТ ЁРУЫПЛЛ ШЫЩШАЯЯВ (табл. 2).

Таблица 2

Блокнотный шифр.

Table 2

One-Time Pad.

ДАННО	Г	Л	О	К	А	Я	К	У	З	Д	Р	А				
	3	12	15	11	0	32	11	20	8	4	17	0				
КЛЮЧ	Щ	Д	Е	Ц	Ж	Ъ	Х	Ю	Б	М	Ф	Т				
	26	4	5	23	7	27	22	31	1	13	21	19				
ИТОГ	Ь	П	У	Б	Ж	Щ	А	С	И	Р	Е	Т				
	29	16	20	1	7	26	0	18	9	17	5	19				

Таким образом, шифрование начинает трансформироваться из чисто лингвистического явления в комплексное гибридное междисциплинарное образование, находящееся на стыке таких наук, как языкознание и математика, к которым потом присоединилась информатика.

Ввиду этого в начале XX века появилась отдельная «ветвь» криптографии – математическая криптография как самостоятельная междисциплинарная область знания, в основе которой лежат статистика, абстрактная алгебра, высшая арифметика и теория вероятностей, которые в совокупности позволяют создать контролируемую систему кодирования данных, которая будет отличаться своей целостностью и устойчивостью к внешнему несанкционированному доступу [7]. Одним из ярких примеров использования данного метода кодирования является код 'Enigma'.

Специально созданная шифровальная машина «Энигма» технически упрощала процесс кодирования информации, при этом значительно снижала шансы случайного подбора ключа в связи с уникальностью используемого «ключа», который, согласно инструкции, подлежал ежедневной замене. После ввода «слова дня» электромеханическая

роторная машина в случайном порядке видоизменяла выборочный отрезок исходного текста согласно шифру Цезаря, постоянно меняя алгоритм кодирования посредством постоянного вращения алфавитных колец. При этом, в качестве дополнительной меры защиты проводилось повторное кодирование, которое позволяло избежать появления коллизии – замены символа на самого себя, а также производилась дополнительная замена отдельных букв в рамках случайной выборки [13].

Попробуем самостоятельно смоделировать процесс шифрования слова 'Entscheidungsschwierigkeiten' согласно вышеперечисленным принципам работы шифровальной машины.

Согласно стандартам настройки 1941 сдвиг роторов «III – II – I» будет проводиться слева направо через начальное положение **B-L-A**. Дополнительные вводные: 1) параметры настройки коммутатора **A-D B-R C-L E-T F-W G-Z H-K I-J M-X N-Y**; 2) код рефлектора **UKW-B** [10].

Рассмотрим алгоритм кодирования первых 10 букв (табл. 3):

Таблица 3

Модель работы шифровальной машины Энигма.

Table 3

An example of the Enigma machine's encryption process.

Символ I	Ротор	Сдвиг	Сигнал	Символ II
E	B-L-A	A → B	E → T → K	K
N	B-L-B	B → C	N → Y → F	F
T	B-L-C	C → D	T → E → M	M
S	B-L-D	D → E	S → S → R	R
C	B-L-E	E → F	C → L → W	W
H	B-L-F	F → G	H → K → X	X
E	B-L-G	G → H	E → T → P	P
I	B-L-H	H → I	I → J → Z	Z
D	B-L-I	I → J	D → D → Q	Q
U	B-L-J	J → K	U → U → G	G

В результате загаданное нами слово 'Entscheidungsschwierigkeiten' на выходе приобретает следующий вид: KFMRW XPZQG VSEAN IDOBV YTLCHF HSW.

Единственным слабым звеном системы, благодаря которому ее, в первую очередь, и получилось «взломать», это набор повторяющихся в тексте слов и выражений, которые машина не могла самостоятельно «перефразировать»; следовательно, зная контекст протекания коммуникации в полученном тексте и используя сравнительно-сопоставительный метод и метод подбора, возможно найти ключевое слово, которое позволит расшифровать остальную часть сообщения.

Таким образом, лингвистическое шифрование текста ставит своей целью изучение закодированного определенным образом сообщения с целью выявления «спрятанной» информации путем обнаружения специального «ключа» для «взлома» исходного кода.

Важно отметить, что работа с подобной системой «шифрования» долгое время была возможна только в рамках функционирования каждой отдельной языковой системы, т.е. и коммуникатор, и реципиент принадлежат к одной лингвокультуре и обладают одинаковым и/или схожим уровнем сформированности языковой и коммуникативной компетенций, так как трансформация исходного текста происходит с изменением синтаксической и грамматической формы оригинала, а также с привлечением как математических, так и национально-культурных кодов [11].

Увеличение числа кросс-культурных контактов вывело процесс кодирования на новый уровень, повысив устойчивость нового сообщения ко взлому благодаря использованию двух и более опорных языков, что хорошо видно при изучении истории становления современных методов шифро-

вания – симметричное (AES, 3DES, RC2, WAKE) и асимметричное шифрование (RSA, DSA, Elgamal), системы шифрования с открытым и закрытым ключами, алгоритмы хеширования, где на начальном этапе была особенно важна межкультурная коммуникативная компетенция разработчиков, так как необходимо было создать универсальный алгоритм действий, который бы подходил для работы с различными языками в рабочей паре «ЯВ<sub>1</sub>–ЯК–Я1» и «ЯВ<sub>1</sub>–ЯК–Я2», где ЯВ<sub>1</sub>– язык ввода, ЯК – язык кодирования, Я1– результат на языке ввода, Я2– результат на новом языке, что позволило бы преодолеть «верхнюю границу возможности использования одного и того же ключа шифрования без утечки информации» [8].

### Выводы

В условиях повсеместной цифровизации коммуникативных процессов лингвистическое шифрование как элемент межкультурной коммуникации становится ключевым фактором для обеспечения конфиденциальности и целостности информации.

За последние две тысячи лет методы шифрования эволюционировали от простых моноалфавитных систем, таких как шифр Цезаря, до сложных полиалфавитных алгоритмов – квадрат Виженера, блокнотное шифрование и др. Диахронический анализ положений перечисленных алгоритмов кодирования подчеркнул значимость криптографии как междисциплинарного явления, находящегося на стыке лингвистики, математики и информатики.

Отдельно отмечается необходимость унификации процессов шифрования, которые могли бы применяться для работы с разноразличными данными, что делает лингвистическое шифрование как самостоятельную область языкознания перспективным направлением для изучения.

### Список источников

1. Аксенова Н.С., Епифанцева Н.Г., Жирова И.Г. Интертекстуальность как лингвистический феномен межкультурного диалога: (на материале сакрально-мистических текстов). Москва: Издат. Дом "Академия Естествознания", 2018. 96 с.
2. Арзиев А.Т., Шаназаров Б. Криптографический метод шифрования и дешифрования информации на основе алгоритма машины Энигма // Universum: технические науки. 2024. № 4 (121). С. 33 – 35.
3. Бабаш А.В. Гузовс Р., Касаткин С.В., Прохоров А.Н., Слимов Н.А. Расширение границ применения методов дешифрования шифра Виженера // Вопросы кибербезопасности. 2019. № 5 (33). С. 42 – 50.
4. Березина Я.Н. Дешифрование текста как аспект прикладной лингвистики // Инновационные аспекты развития науки и техники. 2020. № 2. С. 110 – 113.
5. Жирова И.Г. Роль и место интерсубъективной интерпретации текста в теории и практике перевода // Язык. Культура. Перевод: сб. материалов IV Междунар. науч. конф.: к 80-летию со дня рождения д-ра филол. наук, проф. Р.Р. Чайковского, Магадан, 30 сент. 2019 г. / Северо-Восточный гос. ун-т. Магадан: ООО "Научно-инновационный центр", 2019. С. 109 – 119.
6. Здор С.Е. Кодированная информация: От первых природных кодов до искусственного интеллекта. Москва : Лиبرоком, 2012. 168 с.

7. Коржик В.И., Яковлев В.А., Изотов Б.В., Старостин В.С., Буйневич М.В. Прогресс в теории прикладной криптографии: обзор и некоторые новые результаты. Часть 1. Ключевая криптография // Труды учебных заведений связи. 2024. № 4. С. 126 – 141.
8. Коржик В.И., Яковлев В.А., Старостин В.С., Буйневич М.В. Прогресс в теории прикладной криптографии: обзор и некоторые новые результаты. Ч. 2. Бесключевая криптография // Труды учебных заведений связи. 2024. № 6. С. 79 – 98.
9. Тахиров Б.Н. Алгоритмы шифрования и их свойства // Universum: технические науки. 2021. № 11-1 (92). С. 66 – 68.
10. Шолин И.М. Чубырь Н.О. Алгоритм переносной шифровальной машины Энигма // Форум молодых ученых. 2018. № 10 (26). С. 1352 – 1356.
11. Harris R. Signs of Writing. London : Routledge, 1996. 208 p.
12. Kahn, D. The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet. New York : Scribner, 1996. 1200 p.
13. Криптоанализ «Энигмы» [Электронный ресурс]. URL: <https://habr.com/ru/articles/269519/> (дата обращения: 12.02.2025)
14. Путешествие от шифра Цезаря до RSA. Прикладная теория чисел [Электронный ресурс]. URL: <https://habr.com/ru/articles/757558/> (дата обращения: 12.02.2025)
15. Статистические техники криптоанализа [Электронный ресурс]. URL: <https://habr.com/ru/articles/533974/> (дата обращения: 12.02.2025)

### References

1. Aksenova N.S., Epifantseva N.G., Zhirova I.G. Intertextuality as a linguistic phenomenon of intercultural dialogue: (based on sacred and mystical texts). Moscow: Publishing House "Academy of Natural Sciences", 2018. 96 p.
2. Arziev A.T., Shanazarov B. Cryptographic method of encryption and decryption of information based on the Enigma machine algorithm. Universum: technical sciences. 2024. No. 4 (121). P. 33 – 35.
3. Babash A.V., Guzovs R., Kasatkin S.V., Prokhorov A.N., Slimov N.A. Expanding the boundaries of application of Vigenere cipher decryption methods. Cybersecurity Issues. 2019. No. 5 (33). P. 42 – 50.
4. Berezina Ya.N. Text decoding as an aspect of applied linguistics. Innovative aspects of science and technology development. 2020. No. 2. P. 110 – 113.
5. Zhirova I.G. The role and place of intersubjective interpretation of the text in the theory and practice of translation. Language. Culture. Translation: collection of materials of the IV Int. scientific conf.: dedicated to the 80th anniversary of the birth of Doctor of Philological Sciences, Professor R.R. Tchaikovsky, Magadan, September 30, 2019. North-Eastern State University. Magadan: Scientific and Innovation Center LLC, 2019. P. 109 – 119.
6. Zdor S.E. Coded information: From the first natural codes to artificial intelligence. Moscow: Librokom, 2012. 168 p.
7. Korzhik V.I., Yakovlev V.A., Izotov B.V., Starostin V.S., Buinevich M.V. Progress in the theory of applied cryptography: a review and some new results. Part 1. Key cryptography. Transactions of educational institutions of communication. 2024. No. 4. P. 126 – 141.
8. Korzhik V.I., Yakovlev V.A., Starostin V.S., Buinevich M.V. Progress in the theory of applied cryptography: a review and some new results. Part 2. Keyless cryptography. Transactions of educational institutions of communication. 2024. No. 6. P. 79 – 98.
9. Takhirov B.N. Encryption algorithms and their properties. Universum: technical sciences. 2021. No. 11-1 (92). P. 66 – 68.
10. Sholin I.M. Chubyr N.O. Algorithm of the portable encryption machine Enigma. Forum of young scientists. 2018. No. 10 (26). P. 1352 – 1356.
11. Harris R. Signs of Writing. London : Routledge, 1996. 208 p.
12. Kahn, D. The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet. New York : Scribner, 1996. 1200 p.
13. Cryptanalysis of "Enigma" [Electronic resource]. URL: <https://habr.com/ru/articles/269519/> (date of access: 12.02.2025)
14. Journey from the Caesar Cipher to RSA. Applied Number Theory [Electronic resource]. URL: <https://habr.com/ru/articles/757558/> (date of access: 12.02.2025)
15. Statistical Cryptanalysis Techniques [Electronic resource]. URL: <https://habr.com/ru/articles/533974/> (date of access: 12.02.2025)

### **Информация об авторе**

**Носова В.Д.**, аспирант, Государственный университет просвещения; преподаватель, Университет мировых цивилизаций

© Носова В.Д., 2025