AZƏRBAYCAN RESPUBLİKASI
DÖVLƏT TƏHLÜKƏSİZLİYİ XİDMƏTİNİN
HEYDƏR ƏLİYEV adına AKADEMİYASI

Ümummilli Lider Heydər Əliyevin anadan olmasının 102-ci ildönümünə və «Konstitusiya və Suverenlik İli»nə həsr olunmuş «Heydər Əliyevin dövlət təhlükəsizliyi siyasəti: tarixi nailiyyətlər və müasir çağırışlar» mövzusunda respublika elmi-praktik konfransının

M A T E R İ A L L A R I

II cild

07 may 2025-ci il

**“Heydər Əliyevin dövlət təhlükəsizliyi siyasəti:
tarixi nailiyyətlər və müasir çağırışlar”
adlı respublika elmi-praktik konfransının təşkilat komitəsi:**

Komitə sədri:	general-mayor	Elşad Nəsirov

Komitə sədrinin müavinləri:

h.e.n., dosent,	polkovnik	Azər İsmayılov
	general-leytenant	İsmayıl Əkbərov
	polkovnik	Tahir Haqverdi

Komitə üzvləri:

iqt.ü.f.d.,	polkovnik	Elçin Əliyev
	polkovnik	İlkin Əhmədov
tex.e.n., dosent,	polkovnik	Ziyafət Əmirov
	polkovnik	Neyman Rəsulov
ped.ü.f.d.,	polkovnik-leytenant	Rəna İsmayılova
	polkovnik-leytenant	Aydın Mirzəyev
	mayor	Vəfa Camalova

© DTX-nin Heydər Əliyev adına Akademiyası, 2025

д.ф.п.ф. Амина Сафарзаде
Азербайджанский Университет Языков
e-mail: *amina.safarzade@mail.ru*

ЛИНГВИСТИЧЕСКИЕ АСПЕКТЫ ШИФРОВАНИЯ И СКРЫТОЙ ПЕРЕДАЧИ ДАННЫХ В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Резюме

Статья посвящена изучению взаимосвязи лингвистики и информационной безопасности. Рассматриваются преимущества применения морфологического, синтаксического и семантического анализа для шифрования и скрытой передачи данных. Также исследуется влияние многозначности выражений и культурных контекстов на криптографические процессы. Подчёркивается потенциал технологий NLP и искусственного интеллекта для повышения эффективности шифрования и маскировки информации. На основе литературы отмечается необходимость разработки методов, адаптированных для различных языков. В области стеганографии использование лингвистических средств обеспечивает надёжную маскировку данных. Исследования показывают, что интеграция лингвистики и технологий позволяет достичь нового уровня безопасности. В итоге подчёркивается значимость лингвистических аспектов в развитии современных систем безопасности.

Ключевые слова: *шифрование, лингвистика, информационная безопасность, NLP, стеганография.*

Əminə Səfərzadə
Azərbaycan Dillər Universiteti
filologiya üzrə fəlsəfə doktoru

İNFORMASİYA TƏHLÜKƏSİZLİYİNDƏ ŞİFRELƏNMƏNİN VƏ GİZLİ MƏLUMATLARIN KEÇİRİLMƏSİNİN LİNQVİSTİK ASPEKTLƏRİ

Xülasə

Bu məqalədə dilçilik və informasiya təhlükəsizliyi arasındakı əlaqələr geniş şəkildə araşdırılır. Şifrləmə və məlumatların gizli ötürülməsi üçün morfoloji, sintaktik və semantik analizlərin tətbiqinin üstünlükləri vurğulanır. Məqalə həmçinin çoxmənalı ifadələrin və mədəni kontekstlərin kriptoqrafik proseslərə təsirini öyrənir. NLP və süni intellekt texnologiyalarının şifrləmə və məlumatların maskalanmasında effektivliyini artırma imkanları araşdırılır. Ədəbiyyatlar əsasında, fərqli dillər üçün uyğunlaşdırılmış metodların inkişaf etdirilməsi zərurəti qeyd olunur. Steqanoqrafiya sahəsində dilçilik vasitələrinin istifadəsi məlumatların etibarlı maskalanmasını təmin edir. Tədqiqatlar göstərir ki, dilçilik və texnologiyaların inteqrasiyası yeni təhlükəsizlik səviyyəsinə çatmağa imkan verir. Nəticədə, müasir təhlükəsizlik sistemlərinin inkişafında dilçilik aspektlərinin vacibliyi bir daha vurğulanır.

Açar sözlər: *şifrləmə, dilçilik, məlumat təhlükəsizliyi, NLP, staqanografiya.*

Amina Safarzade
Azerbaijan University of Languages
Doctor of Philosophy in philology

LINGUISTIC ASPECTS OF ENCRYPTION AND TRANSMISSION OF CLASSIFIED DATA IN INFORMATION SECURITY

Summary

This article focuses on the relationship between linguistics and information security. It examines the advantages of applying morphological, syntactic, and semantic analysis for encryption and covert data transmission. The impact of linguistic ambiguity and cultural contexts on cryptographic processes is also explored. The potential of NLP technologies and artificial intelligence to enhance the efficiency of encryption and data masking is emphasized. Based on the literature, the necessity of developing methods adapted for different languages is highlighted. In steganography, the use of linguistic tools

ensures reliable data masking. Research demonstrates that the integration of linguistics and technology enables a new level of security. Ultimately, the significance of linguistic aspects in the advancement of modern security systems is underscored.
Key words: *encryption, linguistics, information security, NLP, steganography.*

Информационная безопасность является одной из ключевых сфер современной науки и технологий, направленной на защиту данных от несанкционированного доступа. Одним из важнейших компонентов этой области являются шифрование и скрытая передача данных, обеспечивающие конфиденциальность и целостность информации. Современные криптографические методы всё чаще интегрируют лингвистические подходы, позволяющие учитывать особенности языка и текста. Лингвистика изучает структуру языка, что делает её незаменимым инструментом для создания устойчивых алгоритмов защиты данных. Использование лингвистических моделей позволяет не только повышать стойкость шифров, но и разрабатывать методы анализа и обнаружения угроз, таких как стеганография или скрытые коммуникации. Помимо этого, лингвистические исследования способствуют адаптации алгоритмов шифрования к особенностям различных языков, что особенно важно в условиях глобализации. В данной статье рассматриваются ключевые аспекты интеграции лингвистики в криптографию и стеганографию, а также вызовы, связанные с межъязыковыми и культурными различиями.

1. Лингвистика в криптографии

1.1. Частотный анализ как основа

Частотный анализ является базовым методом, используемым для дешифрования сообщений, зашифрованных простыми алгоритмами, например, шифром Цезаря или моноалфавитными шифрами. В английском языке, например, буква "e" встречается чаще других, что позволяет быстро определить ключ шифрования. В азербайджанском языке частота букв, таких как "a" и "e", также является характерной, что должно учитываться при разработке адаптивных алгоритмов шифрования [5].

1.2. Роль морфологии и синтаксиса

Морфологические особенности языка влияют на сложность взлома шифров. Например, агглютинативные языки, такие как азербайджанский, содержат сложные словообразовательные структуры, которые могут затруднить применение универсальных алгоритмов дешифрования. В таких случаях использование специальных лингвистических моделей повышает эффективность шифрования [6, с. 78].

1.3. Семантическое шифрование

Семантические алгоритмы используют контекст и значение слов для кодирования информации. Например, сообщение «покупай золото» может быть зашифровано через подбор синонимов или переформулировку как «приобрети драгоценности», что затрудняет его автоматическое обнаружение [10, с. 45].

2. Лингвистические аспекты стеганографии

2.1. Методы скрытия информации

Текстовая стеганография использует перестановки слов, синонимичные замены, а также изменения в пунктуации для сокрытия данных. Например, в тексте "Я люблю математику" можно закодировать сообщение, переставив слова: "Математику люблю я". Такой подход требует анализа грамматики, чтобы текст оставался естественным [7, с. 123].

2.2. Алгоритмы на основе грамматики

Один из инновационных методов скрытия данных — использование грамматических изменений. Например, активный залог в предложении "Сотрудники

завершили проект" может быть заменён на пассивный: "Проект был завершён сотрудниками". Это позволяет скрывать данные на уровне синтаксической структуры [1].

2.3. Скрытие данных в многозначных словах

Некоторые языки, такие как русский и азербайджанский, богаты словами с несколькими значениями. Это открывает новые возможности для шифрования и стеганографии. Например, слово "ключ" может обозначать как "инструмент", так и "шифровальную последовательность". Подобная многозначность усложняет анализ текста злоумышленниками [4].

3. Проблемы и вызовы

3.1. Межъязыковые особенности

При разработке универсальных криптографических решений возникает проблема адаптации алгоритмов к разным языковым системам. Например, в английском языке фиксированный порядок слов (SVO) упрощает анализ, тогда как в русском и азербайджанском языках порядок слов свободный, что требует дополнительных ресурсов для обработки [8, с. 89].

3.2. Использование диалектов

Диалектные различия в языке также являются вызовом для алгоритмов шифрования. Например, различия между литературным азербайджанским языком и его региональными диалектами могут использоваться для создания уникальных ключей шифрования, но требуют значительных затрат на разработку адаптивных моделей [2].

3.3. Учет культурного контекста

Лингвистика тесно связана с культурой. Шифрование сообщений, содержащих культурные или исторические термины, должно учитывать их значения в конкретной культуре. Это особенно важно для предотвращения ложных интерпретаций при анализе текста [9].

4. Применение искусственного интеллекта

4.1. NLP в криптографии

Обработка естественного языка (NLP) активно используется для анализа больших объемов текстов, что позволяет разрабатывать сложные алгоритмы шифрования. Например, нейронные сети могут быть обучены на корпусах текстов для предсказания вероятных замен символов или слов [3].

4.2. Генерация скрытых текстов

С помощью языковых моделей, таких как GPT, можно автоматически генерировать тексты, содержащие скрытые сообщения. Такие модели используются для создания естественных текстов, которые содержат зашифрованную информацию, оставаясь при этом читаемыми [11].

Лингвистические аспекты шифрования и скрытой передачи данных предоставляют уникальные возможности для совершенствования методов информационной безопасности. Использование морфологических, синтаксических и семантических анализов позволяет разрабатывать алгоритмы, устойчивые к современным угрозам. Однако сложность языковых структур и многозначность слов остаются значительными вызовами, требующими междисциплинарного подхода. Применение методов обработки естественного языка (NLP) и искусственного интеллекта открывает перспективы автоматизации и улучшения шифровальных процессов. Адаптация алгоритмов к культурным и языковым особенностям повышает их применимость в глобальном масштабе. В дальнейшем потребуется более глубокая интеграция лингвистических моделей с современными технологиями, чтобы справляться с новыми угрозами. Таким образом, взаимодействие лингвистики и информационных технологий продолжает оставаться важным направлением в области безопасности и защиты данных.

Список литературы:

1. Алиев К. Адаптация алгоритмов шифрования для азербайджанского языка. Баку: Элм, 2022.
2. Ахмедов Э. Диалекты и криптография. Баку: Элм, 2023.
3. Громов С. Искусственный интеллект в обработке текста. М.: Альфа, 2022.
4. Жуков В. Лингвистика в информационной безопасности. М.: Логос, 2018.
5. Иванов А. Введение в криптографию. М.: Наука, 2021.
6. Петров Б. Методы частотного анализа. СПб.: Питер, 2019.
7. Brown R. Steganography and NLP Applications. New York: Wiley, 2021.
8. Carter M. Grammar-based Cryptography. Berlin: De Gruyter, 2020.
9. Lee K. Cultural Context in Cryptographic Algorithms. Tokyo: Kuroda, 2021.
10. Smith J. Semantic Encryption in Modern Security. London: Springer, 2020.
11. Wang T. Neural Networks in Steganography. Beijing: SinoTech, 2021.