

УДК 811.111'42:81'23:81'27

DOI <https://doi.org/10.24919/2308-4863/104-23>

Анна МАРМУЛЯК,

orcid.org/0000-0002-7526-5850

доктор філософії,

викладач кафедри українознавства та міжкультурної комунікації

Львівського державного університету безпеки життєдіяльності

(Львів, Україна) *anua.marmulyak@gmail.com*

Христина ВЕРБИЦЬКА,

orcid.org/0000-0002-7951-0964

кандидат наук з соціальних комунікацій, доцент,

доцент кафедри українознавства та міжкультурної комунікації

Львівського державного університету безпеки життєдіяльності

(Львів, Україна) *khrystynav1004@gmail.com*

Тетяна ЛИПЧЕНКО,

orcid.org/0000-0003-0173-3372

старший викладач кафедри українознавства та міжкультурної комунікації

Львівського державного університету безпеки життєдіяльності

(Львів, Україна) *tetyanalypchenko@ukr.net*

СУГЕСТИВНИЙ ПОТЕНЦІАЛ АНГЛОМОВНОЇ КОМУНІКАЦІЇ У ЦИФРОВОМУ СЕРЕДОВИЩІ: ВЕРБАЛЬНИЙ РЕПРЕЗЕНТАНТ ТА ВИКЛИКИ ДЛЯ МОВНОЇ БЕЗПЕКИ

У статті досліджено сугестивну специфіку сучасного англомовного шахрайського дискурсу, який функціонує в межах віртуального простору. Глобалізація інформаційних потоків та перенесення бізнесової, фінансової та повсякденної комунікації в інтернет-мережу актуалізували вивчення нових деструктивних жанрів. Оскільки англійська мова є домінантним кодом міжнародної цифрової взаємодії, саме її текстовий простір стає основним майданчиком для реалізації фішинг-атак. Мова у цьому контексті розглядається не лише як засіб передачі дезінформації, а як складний інструмент впливу на когнітивну сферу адресата.

Дослідження зумовлене наявною суперечністю між високою технологічною захищеністю цифрових платформ та вразливістю «людського фактора», який зловмисники експлуатують за допомогою соціальної інженерії. Традиційні автоматизовані системи безпеки (спам-фільтри) фокусуються на технічних параметрах повідомлень, проте часто виявляються неефективними проти нових, лінгвістично адаптованих і згенерованих штучним інтелектом текстів. У зв'язку з цим постає проблема відсутності чітких лінгвістичних критеріїв диференціації маніпулятивного контенту, що створює прямі виклики для мовної безпеки користувачів, підриваючи їхню здатність вчасно розпізнавати комунікативні загрози.

Метою наукової праці є виявлення та класифікація мовних маркерів прихованого впливу, що виступають вербальними репрезентантами сугестивного потенціалу в англомовній комунікації у цифровому середовищі, задля обґрунтування засад мовної безпеки.

Для реалізації поставленої мети авторами було сформовано корпус англомовних фішингових повідомлень, які підлягали комплексному аналізу за допомогою методів лінгвопрагматики та критичного дискурс-аналізу. За результатами дослідження встановлено, що вербальний репрезентант сугестії системно виявляється на кількох мовних рівнях. Обґрунтовано лексико-семантичні стратегії штучного дефіциту часу, псевдоавторитету та залякування. На прагма-синтаксичному рівні виокремлено домінування пасивних конструкцій для імітації офіційних сповіщень та надмірне вживання імперативів. Особливу увагу приділено лінгвістичним аномаліям (помилкам нейтивовомовних авторів), які руйнують сугестивний ефект тексту. Доведено, що маркування цих елементів є основою лінгвістичного складника мовної безпеки в мережі. Практична цінність роботи полягає у можливості використання її висновків під час викладання курсів ділової англійської мови та медіаграмотності для студентів-філологів.

Ключові слова: сугестивний потенціал, англомовна комунікація, цифрове мовне середовище, вербальний репрезентант, мовна безпека, фішинг-дискурс, лінгвопрагматика.

Anna MARMULYAK,

orcid.org/0000-0002-7526-5850

PhD,

Lecturer at the Department of Ukrainian Studies and Intercultural Communication

Lviv State University of Life Safety

(Lviv, Ukraine) anya.marmulyak@gmail.com

Khrystyna VERBYTSKA,

orcid.org/0000-0002-7951-0964

Candidate of Sciences in Social Communications, Associate Professor,

Associate Professor at the Department of Ukrainian Studies and Intercultural Communication

Lviv State University of Life Safety

(Lviv, Ukraine) khrystynav1004@gmail.com

Tetiana LYPCHENKO,

orcid.org/0000-0003-0173-3372

Senior Lecturer at the Department of Ukrainian Studies and Intercultural Communication

Lviv State University of Life Safety

(Lviv, Ukraine) tetyanalypchenko@ukr.net

SUGGESTIVE POTENTIAL OF ENGLISH-LANGUAGE COMMUNICATION IN THE DIGITAL ENVIRONMENT: VERBAL REPRESENTATIVE AND CHALLENGES TO LINGUISTIC SECURITY

The article examines the suggestive nature of contemporary English-language fraudulent discourse operating within the virtual space. The globalization of information flows and the migration of business, financial, and everyday communication to the Internet have made the study of new destructive genres a matter of current importance. As English is the dominant medium of international digital interaction, its textual space serves as the primary arena for phishing attacks. In this context, language is viewed not merely as a vehicle for disseminating disinformation, but as a sophisticated tool for influencing the recipient's cognitive processes.

The study is prompted by the existing contradiction between the high level of technological security of digital platforms and the vulnerability of the «human factor,» which malicious actors exploit through social engineering. Traditional automated security systems (spam filters) focus on the technical parameters of messages, yet they often prove ineffective against new, linguistically adapted, and AI-generated texts. This gives rise to the problem of a lack of clear linguistic criteria for distinguishing manipulative content, which poses direct challenges to users' linguistic security by undermining their ability to timely recognize communicative threats.

The aim of this research is to identify and classify linguistic markers of covert influence—which serve as verbal representations of suggestive potential in English-language digital communication—in order to substantiate the principles of linguistic security.

To achieve the stated objective, the authors compiled a corpus of English-language phishing messages, which were subjected to a comprehensive analysis using methods of linguopragmatics and critical discourse analysis. The study results reveal that the verbal representation of suggestion manifests systematically across several linguistic levels. The lexical-semantic strategies of artificial time pressure, pseudo-authority, and intimidation are substantiated. At the pragma-syntactic level, the dominance of passive constructions—used to simulate official notifications—and the excessive use of imperatives are identified. Particular attention is paid to linguistic anomalies (errors made by non-native speakers) that undermine the text's suggestive effect. It has been demonstrated that the marking of these elements forms the basis of the linguistic component of online language security. The practical value of the study lies in the potential to apply its findings when teaching Business English and media literacy courses to philology students.

Key words: *suggestive potential, English-language communication, digital linguistic environment, verbal representative, linguistic security, phishing discourse, linguopragmatics.*

Постановка проблеми. Стрімка еволюція глобального інформаційного суспільства та інтенсифікація цифрових процесів призвели до трансформації традиційних мовленнєвих жанрів та появи нових форм деструктивного впливу в мережі. В умовах сучасних гібридних загроз інформаційна безпека держави та індивіда безпосеред-

ньо залежить від стійкості особистості до мовних маніпуляцій у віртуальному просторі. Одним із найнебезпечніших проявів такого деструктивного впливу є фішинг – технологія соціальної інженерії, що реалізується через текстові повідомлення в інтернеті. Ефективність подібних кібератак базується не лише на технічних алгоритмах, а й на

тонкому знанні психології адресата, що кодується через конкретні мовні одиниці. Оскільки англійська мова є домінуючим кодом у міжнародному бізнесі та IT-індустрії, дослідження її сугестивного потенціалу в шахрайському дискурсі набуває сьогодні особливого значення. Захист користувачів від таких загроз виходить за межі суто технічних рішень і безпосередньо апелює до концепту мовної безпеки – здатності людини ідентифікувати та нейтралізувати приховані маніпулятивні коди в текстах. Відтак, виникла потреба науково описати та класифікувати вербальний репрезентант шахрайських намірів в англomовній комунікації у цифровому середовищі для розробки ефективних критеріїв мовної медіагігієни.

Аналіз досліджень. Фундамент для вивчення сугестивного та маніпулятивного потенціалу тексту закладено в класичних працях із критичного дискурс-аналізу Т. ван Дейком (Dijk, 2008: 11), Н. Фейркліфом (Fairclough, 1995: 12), Р. Блакаром (Blakar, 1979: 9) та теорії мовленнєвих актів Дж. Остіном (Austin, 1962: 8), Дж. Серльем (Searle, 1979: 14), де мова трактується як інструмент модифікації поведінки адресата. У вітчизняній лінгвістиці прагматичний і сугестивний складники комунікації активно розробляли Г. Почепцов (Почепцов, 2000: 4), С. Жаботинська (Жаботинська, 2005: 2) та Ф. Бацевич (Бацевич, 2004: 1). Специфіка комунікації у цифровому середовищі та еволюція інтернет-жанрів перебувають у центрі уваги сучасних медіалінгвістів, зокрема, концепція комп'ютерно-опосередкованого дискурсу описана С. Геррінгом (Herring, 2004: 13). Питання інформаційної та мовної безпеки в умовах новітніх віртуальних загроз порушуються у працях Л. Масенко (Масенко, 1999: 3) та О. Сербенської (Сербська, 2011: 6). Водночас у роботах провідних англівстів О. Селіванової (Селіванова, 2008: 5), І. Шевченко (Шевченко, 2002: 7) детально описано лінгвокогнітивні та прагматичні константи сучасного англomовного ділового й корпоративного дискурсів. Окремий пласт закордонних розвідок останніх років присвячено кіберлінгвістиці та лінгвістичній експертизі шахрайських текстів М. Култхардом, Т. Грантом (Coulthard, 2010: 10). Попри потужну теоретичну базу сугестивної лінгвістики, вербальний репрезентант англomовного фішингу як специфічного деструктивного жанру залишається малодослідженим. Більшість існуючих праць із кібербезпеки мають суто технічний характер і концентруються на архітектурі спам-фільтрів чи машинному навчанні. Лінгвістичний вимір мовної безпеки користувачів у віртуальному просторі часто розглядається науковцями

лише дотично, без прив'язки до лінгвопрагматичних маркерів конкретної мови. У сучасних філологічних студіях практично відсутні праці, які б системно описували мовні пастки фішинг-повідомлень, побудованих за канонами Business English. Також потребує глибшого теоретичного осмислення когнітивний механізм сприйняття штучно створених сугестивних тригерів терміновості та псевдоавторитету. Недостатньо вивченим залишається й аспект лінгвістичних аномалій у текстах кібершахраїв, які виступають маркерами деструкції сугестивного впливу. Таким чином, фрагментарність лінгвістичних описів англomовного шахрайського дискурсу та практична потреба у розробці критеріїв мовної безпеки зумовлюють вибір вектора нашого дослідження.

Метою статті є комплексний лінгвопрагматичний аналіз та систематизація вербальних маркерів сугестивного потенціалу в англomовній комунікації у цифровому середовищі на матеріалі фішингових повідомлень. На основі виявлених мовних маркерів та стратегій штучного впливу планується окреслити ключові виклики мовної безпеки користувачів та обґрунтувати гуманітарні засади їхньої цифрової гігієни.

Виклад основного матеріалу. Дослідження вербального репрезентанта сугестивного потенціалу деструктивної англomовної комунікації у цифровому середовищі здійснювалося на основі сформованого нами корпусу, який містить 50 автентичних фішингових повідомлень (електронних листів та SMS-сповіщень), що імітують офіційну кореспонденцію провідних світових брендів (*PayPal, Netflix, Amazon, FedEx, Google*). Лінгвопрагматичний та дискурсивний аналіз матеріалу дозволив структурувати вербальні засоби навіювання та виклики мовної безпеки за трьома взаємопов'язаними рівнями: лексико-семантичним, прагма-синтаксичним та рівнем лінгвістичних аномалій.

1. Лексико-семантичний рівень: вербалізація тригерів та емоційного тиску.

На лексичному рівні сугестивний потенціал реалізується через систему слів-тригерів, спрямованих на відключення раціонального аналізу ситуації адресатом шляхом апеляції до базових емоцій (страху, паніки, бажання вигоди). Дослідження дозволило виокремити три домінантні лексико-семантичні стратегії: стратегія штучного дефіциту часу завдяки навіювальному ефекту базується на звуженні часових меж для ухвалення рішення. У корпусі дослідження це вербалізується через поєднання ад'єктивів високої інтенсивності та конкретних часових обмежень: «*Urgent action*

required: Your account has been flagged. Please verify your identity within 24 hours to prevent permanent suspension»; «Immediate response necessary. Failure to log in now will result in instant deactivation of your services». Лексеми *urgent, immediate, instant* функціонують як прагматичні маркери невідкладності, а словосполучення *permanent suspension* або *frozen funds* лексикалізують загрозу безповоротності негативних наслідків, блокуючи критичне мислення людини. Стратегія легітимізації та псевдоавторитету: для присиплення пильності адресата шахраї активно експлуатують номінативні моделі офіційно-ділового стилю (*Business English*). Сугестія досягається шляхом використання складних іменникових конструкцій, що імітують інституційний статус: *«Dear Customer, Our Advanced Cyber Security Division has detected a suspicious login attempt»; «This notice is issued by the Global Billing and Verification Team».* Використання маркерів *Advanced Cyber Security Division* чи *Global Billing Team* створює в когнітивній системі користувача помилковий фрейм легітимності. Лексеми *detected, suspicious, unauthorized* запозичені з реального ІТ-дискурсу, що посилює ілюзію офіційності. Стратегія залякування та загрози втрати експлуатує психологічне прагнення людини уникати збитків: *«We noticed unusual activity on your card. To avoid financial penalty, update your tax information».* Лексичні одиниці з негативною конотацією (*unusual activity, penalty, security breach*) діють як сугестивні подразники, змушуючи користувача фокусуватися виключно на усуненні уявної небезпеки.

2. Прагма-синтаксичний рівень: іллокутивна сила та синтаксичне маскування: на синтаксичному рівні вербальним репрезентантом сугестії виступає специфічна архітектоніка речень, яка маскує справжні інтенції автора та максимізує спонукальний ефект. У цьому зрізі виокремлено такі прагматичні константи: домінування пасивного стану. У класичній англomовній бізнес-комунікації пасивний стан використовується для дистанціювання та об'єктивності. Фішинг-дискурс інструменталізує цю граматичну категорію для зняття персональної відповідальності та надання тексту «роботизованого» вигляду системного повідомлення: *«Your account has been locked due to several failed attempts. Access is temporarily denied until verification is completed».* Синтаксичні структури *has been locked, is denied* усувають реального суб'єкта дії, створюючи ілюзію об'єктивного автоматизованого процесу. Це пригнічує критичне запитання адресата про те, хто саме надсилає повідомлення, що є прямим викликом для мовної безпеки. Висока кон-

центрація імперативних конструкцій. Після психологічної підготовки адресата за допомогою залякування, текст миттєво пропонує єдиний «рятувальний» алгоритм дій через директивні мовленнєві акти: *«Click here to log in. Update your billing data immediately. Do not ignore this notification».* Наказові дієслова *click, update, download* мають високу іллокутивну силу. Вони функціонують як безальтернативні команди, що спонукають до автоматичного виконання фізичної дії (кліку на шкідливе посилання).

3. Рівень лінгвістичних аномалій як деструктор сугестивного впливу: найбільш значущим викликом та водночас інструментом забезпечення мовної безпеки у цифровому просторі є аналіз мовних девіацій. Оскільки значна частина фішингових кампаній розробляється суб'єктами, які не є носіями англійської мови або генерується автоматизованими перекладачами без належної прагматичної адаптації, тексти містять яскраві лінгвістичні аномалії.

Нами виявлено та класифіковано порушення мовної норми, а саме аномалії категорії визначеності/невизначеності: *«We detected a suspicious activity in your account»* (іменник *activity* у цьому контексті функціонує як незлічуваний, використання неозначеного артикля є помилкою). *«Please click on Ø link below to restore the access»* (пропуск артикля перед конкретним посиланням та надлишкове вживання означеного артикля перед абстрактним іменником *access*). Порушення лексичної сполучуваності: *«Please make the necessary steps»* замість нормативного для *Business English* *«take steps / take measures».* *«Your password was made invalid»* замість конвенційного *«became invalid / was rendered invalid».* Синтаксичні та пунктуаційні зсуви: порушення жорсткого англійського порядку слів, нетипові для офіційного стилю знаки оклику або хаотичне використання великих літер всередині речення: *«For security reasons is required your instant confirmation!».* Для мовної особистості з високим рівнем лінгвістичної компетенції саме ці вербальні аномалії виступають маркерами деструкції сугестивного впливу. Вони руйнують створений шахраями фрейм «офіційного інституційного повідомлення», сигналізуючи про небезпеку і виступаючи внутрішнім тригером мовної безпеки користувача.

Висновки. У статті здійснено комплексне лінгвістичне дослідження деструктивного шахрайського дискурсу в інтернет-середовищі, що дозволило сформулювати теоретичні та практичні підсумки.

Обґрунтовано, що вербальний репрезентант сугестивного потенціалу в англomовній комунікації у цифровому середовищі (на матеріалі фішингу) є складною багаторівневою системою мовних засобів, спрямованих на модифікацію поведінки адресата шляхом пригнічення його раціонального критичного мислення та присипляння пильності. На лексико-семантичному рівні виокремлено та класифіковано три домінантні стратегії сугесії: штучного дефіциту часу, псевдоавторитету та залякування. Вербальними маркерами цих стратегій виступають емоційно-інтенсифіковані ад'єктиви, часові обмежувачі та специфічні іменникові конструкції. На прагма-синтаксичному рівні встановлено, що іллокутивна сила повідомлень має приховано-директивний характер. Сугестивний ефект посилюється через домінування конструкцій пасивного стану, які усувають реального суб'єкта дії та імітують об'єктивні роботизовані

сповіщення системи безпеки, а також через високу концентрацію імперативів, які спонукають користувача до негайного виконання фізичної дії. Доведено, що ключовим інструментом забезпечення мовної кібербезпеки особистості є ідентифікація лінгвістичних аномалій (девіацій артиклів, прийменників, лексичної сполучуваності та синтаксичного порядку слів), які виникають внаслідок генерації текстів авторами-неносіями мови чи автоматичними перекладачами. Ці аномалії виступають деструкторами сугестивного впливу, руйнують ілюзію легітимності повідомлення та сигналізують користувачеві про небезпеку.

Перспективи подальших розвідок у цьому напрямі полягають у дослідженні трансформації сугестивних стратегій під впливом генеративного штучного інтелекту, а також у розробці лінгвістичних критеріїв для автоматизованих систем моніторингу цифрових загроз.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бацевич Ф. Основи комунікативної лінгвістики : підручник. Київ : Академія, 2004. 344 с.
2. Жаботинська С. Концептуальний аналіз тексту: фреймові мережі. *Вісник Черкаського університету. Серія: Філологічні науки*. 2005. Вип. 72. С. 48–56.
3. Масенко Л. Мова і політика. Київ : Соняшник, 1999. 100 с.
4. Почепцов Г. Сучасні комунікативні технології. Київ : Альтерпрес, 2000. 304 с.
5. Селіванова О. Сучасна лінгвістика: напрями та проблеми : підручник. Полтава : Довкілля-К, 2008. 711 с.
6. Сербенська О. Культура усного мовлення. Практичний курс : навч. посіб. Київ : Центр учбової літератури, 2011. 140 с.
7. Шевченко І. Історична динаміка англomовного дискурсу: когнітивно-прагматичний аспект. *Вісник Харківського національного університету імені В. Н. Каразіна*. 2002. № 532. С. 45–52.
8. Austin J. *How to Do Things With Words*. Oxford : Oxford University Press, 1962. 168 p.
9. Blakar R. *Language as an Instrument of Social Power. Context and Communication*. London : Academic Press, 1979. P. 131–151.
10. Coulthard M., Grant T. *Routledge Handbook of Forensic Linguistics*. London : Routledge, 2010. 672 p.
11. Dijk T. *Discourse and Power*. London : Palgrave Macmillan, 2008. 320 p.
12. Fairclough N. *Critical Discourse Analysis: The Critical Study of Language*. London : Longman, 1995. 265 p.
13. Herring S. *Computer-Mediated Discourse Analysis: An Approach to Researching Online Behavior. Designing for Virtual Communities in the Service of Learning*. New York : Cambridge University Press, 2004. P. 338–376.
14. Searle J. *Expression and Meaning: Studies in the Theory of Speech Acts*. Cambridge : Cambridge University Press, 1979. 187 p.

REFERENCES

1. Batsevych F. (2004) *Osnovy komunikatyvnoi linhvistyky*. [Fundamentals of Communicative Linguistics] Pidruchnyk Kyiv, Akademiia, 344. [in Ukrainian].
2. Zhabotynska, S. (2005) *Kontseptualnyi analiz tekstu: freimovi merezhi* [Conceptual analysis of the text: frame networks]. *Visnyk Cherkaskoho Universytetu. Seriya: Filolohichni Nauky* 72. 48–56. [in Ukrainian].
3. Masenko L. (1999). *Mova i polityka*. [Language and Politics]. Kyiv, Soniashnyk, 100. [in Ukrainian].
4. Pocheptsov H. (2000) *Suchasni komunikatyvni tekhnolohii*. [Modern communication technologies]. Kyiv, Alterpres, 304. [in Ukrainian].
5. Selivanova O. (2008) *Suchasna linhvistyka: napriamy ta problemy* [Contemporary linguistics: direct and problematic].: pidruchnyk. Poltava, Dovkillia-K, 711. [in Ukrainian].
6. Serbenska O. (2011) *Kultura usnogo movlennia. Praktychnyi kurs : navch. posib*. [Oral culture. Practical course]. Kyiv, tsentr uchbovoi literatury, 140. [in Ukrainian].
7. Shevchenko I. (2002) *Istorychna dynamika anhlomovnoho dyskursu: kohnityvno-prahmatychnyi aspekt*. [Historical dynamics of the ankhlo discourse: a cognitive-pragmatic aspect]. *Visnyk Kharkivskoho natsionalnoho universytetu imeni V. N. Karazina* № 532. 45–52. [in Ukrainian].
8. Austin J. (1962) *How to Do Things With Words*. Oxford : Oxford University Press, 168.

9. Blakar R. (1979) Language as an Instrument of Social Power. Context and Communication. London : Academic Press, 131–151.
10. Coulthard M., Grant T. (2010) Routledge Handbook of Forensic Linguistics. London : Routledge, 672.
11. Dijk T. (2008) Discourse and Power. London : Palgrave Macmillan, 320.
12. Fairclough N. (1995) Critical Discourse Analysis: The Critical Study of Language. London : Longman, 265.
13. Herring S. (2004) Computer-Mediated Discourse Analysis: An Approach to Researching Online Behavior. Designing for Virtual Communities in the Service of Learning. New York : Cambridge University Press, 338–376.
14. Searle J. (1979) Expression and Meaning: Studies in the Theory of Speech Acts. Cambridge : Cambridge University Press, 187.

Дата першого надходження статті до видання: 17.09.2026

Дата прийняття статті до друку після рецензування: 09.10.2026

Дата публікації (оприлюднення) статті: 30.10.2026

Стаття поширюється на умовах
ліцензії відкритого доступу (CC BY 4.0)

