УДК 303.4:004.056
DOI: https://doi.org/10.32782/business-navigator.81-47

Пенюк В.О.
кандидат економічних наук, доцент,
доцент кафедри менеджменту, маркетингу і міжнародної логістики
Чернівецький торговельно-економічний інститут
Державного торговельно-економічного університету

Peniuk Valeriia
Candidate of Economic Sciences, Docent,
Associate Professor at the Department of Management,
Marketing and International Logistics
Chernivtsi Trade And Economic Institute of
State University of Trade and Economics

КІБЕРБЕЗПЕКА ТА КОМУНІКАЦІЇ: СУЧАСНІ РЕАЛІЇ

CYBERSECURITY AND COMMUNICATIONS: MODERN REALITIES

Стаття присвячена дослідженню актуальності проблеми цифрових загроз в процесі здійснення комунікацій підприємств зі споживачами. Окреслено особливість поняття довіри споживача у цифровому середовищі та визначено складові довіри у цифровому середовищі. Визначено поняття та передумови кібезагроз у сучасному світі. Доведено чому кібербезпека це фундамент якісної комунікації та довготривалих стосунків із клієнтами в цифровому середовищі, і визначено результати такого впливу на довіру, лояльність і репутацію бренду/підприємства. Охарактеризовано поняття «ботоферма» і визначено його вплив в процесі використання інструментів маркетингу. Наведено приклади інформації, яка повинна бути захищеною при використанні різних видів каналів комунікацій зі споживачами/клієнтами. Визначено важливість захисту клієнтських баз даних в процесі збору, та окреслено чому формування баз даних це лише початковий етап цифрової безпеки.

Ключові слова: кібербезпека, комунікації, довіра, споживач, цифрове середовище.

The article is devoted to the study that cybersecurity and effective communication have become critically important components of the security and stable functioning of not only governmental structures, but also of business, education, and everyday life. Cybersecurity and communication are closely interconnected, as any exchange of information through digital channels requires protection. Almost daily, companies interact with and attempt to better understand their consumers – learning their personal data, preferences, purchasing frequency, and more – thereby actively collecting personal information. This article explores the relevance of digital threats in the context of business-to-consumer communication. It highlights the specific nature of consumer trust in the digital environment and outlines the components that constitute trust in this space. The concept and prerequisites of cyber threats in the modern world are defined. The study demonstrates why cybersecurity forms the foundation of high-quality communication and long-term relationships with clients in a digital setting, and shows how it influences trust, loyalty, and the reputation of a brand or enterprise. The concept of a "bot farm" is described, and it is recognized as a significant and dangerous threat to modern consumer communications. The article provides examples of the types of information that must be protected when using various communication channels with consumers and clients, including email marketing, social media surveys, messaging platforms, data collection via websites, chatbots, and more. It is emphasized that effective communication – even in the digital realm – enables the formation of a valuable asset: client databases. The article underlines the importance of protecting these databases during the data collection process and argues that database formation is only the initial stage of ensuring digital security. Additionally, the article emphasizes the need for continuous staff training and awareness to maintain robust cybersecurity practices and ensure secure, trustworthy communication with consumers. It stresses that cybersecurity is not a one-time implementation but an ongoing process that must evolve alongside emerging digital threats. Ultimately, the article advocates for a strategic and integrated approach to cybersecurity as a core element of effective digital communication and consumer relationship management.

Keywords: cybersecurity, communication, trust, consumer, digital environment.

Постановка проблеми. У реаліях сучасного цифрового середовища питання кібербезпеки та ефективної комунікації виходять на перший план як ключові чинники стабільності й безпеки в державному управлінні, бізнесі, освітніх установах та повсякденному житті громадян. Надійний захист інформації є основою будь-якої цифрової взаємодії, адже комунікація в онлайн-просторі неможлива без належного рівня безпеки.

Інформаційний обмін у цифрових каналах, таких як електронна пошта, соціальні мережі, месенджери чи корпоративні портали, вимагає постійного контролю за збереженням даних. Без належного захисту така комунікація стає вразливою до атак, що може призвести до витоку конфіденційної інформації, фінансових втрат і втрати репутації.

З кожним роком кібератаки стають дедалі витонченішими, а кіберзлочинці активно використовують соціальну інженерію, фішингові повідомлення, бот-мережі та інші інструменти для втручання у цифрові зв'язки. Це підвищує потребу у впровадженні новітніх технологій захисту, зокрема двофакторної автентифікації, шифрування даних і постійного моніторингу мережевої активності.

Особливо актуальною кібербезпека стає для компаній, які будують комунікацію зі своїми клієнтами. Збір персональних даних споживачів, аналіз їхньої поведінки та створення клієнтських баз формує важливий цифровий актив. Але без гарантій захисту цієї інформації бізнес ризикує втратити довіру клієнтів і зіштовхнутися з серйозними правовими наслідками.

Аналіз останніх досліджень та публікацій. Проблемами менеджменту кібербезпеки в системі лояльності покупців займались Ю. Королюк та В. Чичун [7], які вважають, що це, перш за все, побудова ефективної динамічної системи оцінки ризиків кіберзагроз та вчасний моніторинг таких ризиків дозволить встановлювати рівні прийнятної безпеки для підприємства, забезпечувати їх дотримання, приймаючи рішення за наявних ресурсів та управлінських інструментів.

Організаційно-правові основи інформаційної безпеки вивчав Б. Кормич [6], який вважає, що інформаційна безпека є складовою національної безпеки та є одним із багатьох інтересів держави і не може розглядатись як стан захищеності національних інтересів. Вплив ботоферм на кібербезпеку підприємства досліджував А. Юшков [14], в результаті чого пропонує розробити законодавчі зміни щодо вдосконалення санкцій за поширення дезінформації, налагодити проактивне інформування суспільства через соціальні мережі щодо позиції України з питань, які потенційно можуть стати загрозливими, а також вважає, що потрібна активізація діяльності, спрямована на нейтралізацію впливу дезінформації та маніпуляцій, впровадження швидкого та проактивного реагування на ключові теми, у межах яких поширюють фейки та пропаганду.

Соціотехнічному аспекту інформаційної та кібербезпеки присвятили свої праці В. Бурячок, В. Толубко, В Хорошко та С. Толюпа [5], та визначили, що кіберпростір і кібербезпека – головні ознаки нової інформаційної цивілізації. Але недостатньо вивченим залишається проблема формування безпечного цифрового середовища в процесі здійснення комунікацій споживача/клієнта з підприємством, що реалізує товар або послугу.

Формулювання завдання дослідження. Метою статті є визначення взаємозв'язку понять кібербезпека та комунікації в процесі здійснення комунікацій споживача/клієнта з підприємством, що реалізує товар або послугу. Для досягнення поставленої мети визначено наступні завдання:

– визначити поняття довіри в процесі комунікацій споживача з підприємством за допомогою цифрових інструментів та визначити її складові;

– довести чому фундаментом якісної комунікації та довготривалих стосунків із клієнтами в цифровому середовищі є кібербезпека;

– навести приклади інформації, яка повинна бути захищеною при використанні різних видів каналів комунікацій споживача/клієнта з підприємством, що реалізує товар або послугу.

Виклад основного матеріалу дослідження. Інформаційні потреби людства сьогодні створюють нове культурне цифрове середовище [9], де і сучасні підприємства активно вдаються до змін та впроваджують нові способи контакту зі споживачем. Майже кожного дня компанії контактують та намагаються вивчити свого споживача, зібрати їх особисті дані, вивчити уподобання, частоту покупок тощо, тому активно проводять збір персональної інформації споживача. Якщо цільова аудиторія впевнена у захисті інформації та особистих даних це підсилює відчуття «довіри» до продукту чи послуги, і формує впевненість у якості комунікацій з нею.

Згідно тлумачного словника «довіра» – ставлення до кого-небудь, що виникає на основі віри в чиюсь правоту, чесність, щирість тощо [11]. Т.Кричевська визначає довіру як відношення до економічних суб'єктів і інститутів, що виражає міру впевненості у відповідності їх поведінки уявленням про образ цієї поведінки без актуалізації основ відшкодування витрат та еквівалентності [8]. Довіру визначають як суб'єкт-суб'єктні або суб'єкт-об'єктні відносини у рамках економічної системи на основі впевненості, що інша сторона виконає всі покладені на неї функції та обов'язки, буде діяти згідно з певними установленими нормами, а результат такої співпраці принесе деякий економічний, соціальний або моральний ефект для кожної з сторін [10].

Якщо взяти до уваги, що цифрове середовище – середовище, що охоплює інформаційно-комунікаційні технології, включаючи Інтернет, мобільні та пов'язані з ними технології та пристрої, а також цифрові мережі, бази даних, контент та послуги, використовується для взаємодії з іншими користувачами та доступу й публікації створеного контенту [12], то можна зробити власне визначення поняття довіри споживача в цифровому середовищі.

Довіра в цифровому середовищі – це впевненість користувача у надійності, чесності та передбачуваності дій інших учасників цифрової взаємодії (зокрема, онлайн-сервісів, платформ, контенту і користувачів), що ґрунтується на дотриманні етичних норм, правових стандартів і технічних гарантій безпеки, і сприяє формуванню стабільних інформаційних, економічних чи соціальних відносин.

Складові безпеки довіри в цифровому середовищі охоплюють кілька ключових аспектів, які забезпечують користувачам впевненість у надійності взаємодії, захисті їхніх даних та добросовісності учасників онлайн-комунікації (таблиця 1).

Одна з головних небезпек у цифровому просторі, те, що стопорить веденню якісної комунікації з споживачами – це кібернебезпека (кіберзагроза) – одна з найбільших проблем, з якими сьогодні стикається бізнес (атаки на резервні копії, відмова в обслуговуванні, злом паролів, використання номеру мобільного телефону тощо). У країнах Європи, продовж п'яти років кількість жертв від кібератак зросла з 28% до 80%. Саме тому запроваджуються заходи з кібербез-

Таблиця 1

Основні складові довіри в цифровому середовищі

Складові	Опис/характеристика
Технічна безпека	• Захист даних (Data Protection): шифрування, автентифікація, брандмауери, антивіруси. • Безпечне зберігання та передача інформації: використання HTTPS, VPN, надійних серверів. • Оновлення систем та виправлення вразливостей: регулярне технічне обслуговування
Приватність та конфіденційність	• Політики конфіденційності: прозоре інформування користувача про збір і використання даних. • Контроль над особистими даними: можливість налаштувати рівень відкритості особистої інформації. • Згода користувача: використання персональних даних лише після явного дозволу
Юридична та етична надійність	• Відповідність законодавству: дотримання норм GDPR, українського закону «Про захист персональних даних» та інших актів. • Дотримання етичних стандартів: чесна комунікація, відсутність маніпуляцій, прозорість у діях
Прозорість	• Доступ до інформації: чітке пояснення умов користування, цінової політики, прав та обов'язків. • Відкритість щодо змін: інформування користувачів про зміни в політиці чи роботі сервісу
Надійність та репутація	• Відгуки та рейтинги: соціальний доказ довіри з боку інших користувачів. • Репутація бренду чи платформи: історія роботи, сертифікації, партнерства.
Користувацький досвід	• Зрозумілий інтерфейс: легкість у користуванні, доступність інформації. • Підтримка користувачів: оперативна технічна допомога, підтримка у вирішенні питань

Джерело: сформовано автором

пеки – практичної діяльності, спрямованої на захист комп'ютерних систем, корпоративних мереж та особистих даних від кібератак.

Кібербезпека охоплює весь комплекс заходів – починаючи з керування паролями до інструментів безпеки на основі штучного інтелекту та машинного навчання. Кібербезпека дає змогу надійно захищати транзакції, переглядати контент та безпечно спілкуватись онлайн [4]. Дотримуючись суворої політики кібербезпеки, будь-яка організація чи то заклад може уникнути витоку даних, несанкціонованого доступу та інших серйозних загроз.

Протягом лише одного місяця після запровадження воєнного стану кількість кібератак на державні установи та бізнес в Україні зросла майже втричі порівняно з аналогічним періодом 2021 року, і як результат навчили підприємства реагувати на кіберзагрози та запроваджувати дієві інструменти кіберзахисту в систему управління підприємством [7, с.47]. За даними Держспецзв'язку, більшість цих атак не досягли успіху та не завдали шкоди критично важливій інформаційній інфраструктурі. Найчастіше хакери націлюються на державні й місцеві органи влади, структури безпеки та оборони, приватні компанії різного профілю, фінансовий сектор, телекомунікаційну інфраструктуру, ІТ-компанії, засоби масової інформації, а також на ресурси, що документують воєнні злочини росії в Україні. У перші півтора місяці війни понад половину кіберзагроз становили спроби збору даних або розповсюдження вірусного програмного забезпечення. За даними звіту Microsoft за 2021 рік, Україна входила до числа головних мішеней кібератак у світі – майже 20% глобальних загроз спрямовувалися саме на неї, поступаючись лише США [3] .

Одним із масштабних кібератак на велику клієнтську базу була атака кібератака на «Київстар» у грудні 2023 року [2]. В результаті, без зв'язку опинилися близько 24 млн абонентів, мережу повністю вимкнули, хакерам вдалося знищити 40% інфраструктури. Хоча, як запевняє компанія, що витоку клієнтських даних не було, інвестування фінансів в кібербезпеку компанії все ж здійснювалось.

Не менш важливою та небезпечною загрозою перед сучасними комунікаціям з споживачами є робота так званих «ботоферм». Як зазначає А.Юшков [14], ботоферми – це компанії, які масово створюють несправжніх користувачів соцмереж і від їхнього імені пишуть тисячі коментарів. Якщо не брати до уваги глобальні небезпеки на рівні країни, можемо відзначити, що часто для підвищення іміджу та привабливості компанії чи продукту використовуються роботу ботоферм і у торгівлі чи сервісі. Імітують лайки у соціальних мережах, коментують про рівень наданих послуг чи якості товару, просувають думки у маси. Тож, споживачі у свою чергу або вдаються до такого впливу і здійснюють покупку, або розуміють, що варто спробувати інший продукт та зробити власні висновки. Така практика зменшує рівень довіри до компаній та погіршують відносини зі споживачами.

Кібербезпека – це фундамент якісної комунікації та довготривалих стосунків із клієнтами в цифровому середовищі, адже вона безпосередньо впливає на довіру, лояльність і репутацію бренду/підприємства. Ось чому:

1. Захист персональних даних – основа довіри. Клієнти надають компаніям доступ до своїх персональних даних (контакти, платіжні реквізити, історія покупок тощо). Якщо ці дані потрапляють до зловмисників через слабкі місця в системі, це призводить до втрати довіри, відтоку клієнтів і юридичних наслідків. Надійна кібербезпека гарантує, що дані захищені, а компанія заслуговує на довіру.

2. Репутаційна стабільність. Навіть один витік даних або кібератака можуть нанести величезної

шкоди репутації бізнесу. Клієнти неохоче співпрацюють із тими, хто не може гарантувати безпеку. Системний підхід до кіберзахисту формує стійку позитивну репутацію бренду як надійного партнера.

3. Підвищення лояльності. Коли користувачі впевнені у безпеці сервісу, вони частіше повертаються, більше витрачають і охочіше рекомендують іншим. Лояльність базується не лише на продукті, а й на відчутті захищеності під час взаємодії з брендом.

4. Конкурентна перевага. У світі, де кіберзагрози постійно зростають, компанії, що інвестують у кібербезпеку, виділяються на фоні конкурентів. Безпека стає частиною ціннісної пропозиції та брендингу.

5. Відповідність законодавству. Компанії, що дотримуються вимог щодо захисту даних (GDPR, українські норми тощо), демонструють свою відповідальність і повагу до прав клієнтів, що також сприяє зміцненню довіри.

Як вважає І.Чирак [13, с.15], сьогодні існує безліч варіантів як просувати товар чи послугу та/або комунікувати з цільовою аудиторією. Наприклад, розсилати інформацію електронною поштою, проводити опитування у соціальних мережах, месенджерах, збирати інформацію на власному сайті, в чат-ботах тощо. А тому особливо важливо захисти персональні дані та повідомлення зі споживачами (табл. 2).

Ефективна комунікація, навіть у цифровому світі, дає можливість сформувати певний актив – бази даних клієнтів, що зберігають критично важливу інформацію: персональні дані користувачів, історії транзакцій, логістичні операції, бізнес-аналітику тощо. Вони є не лише джерелом операційної ефективності, а й основою формування довіри між компанією та клієнтами, партнерами, суспільством загалом.

Безпека баз даних охоплює заходи, інструменти та політики для захисту баз даних від неавторизованого доступу користувачів, зловживань, крадіжок або втрат. Сюди входить контроль доступу до бази даних, захист даних всередині бази даних, а також захист даних під час їх переміщення або доступу до них. Ефективні стандарти безпеки баз даних захищають цінні інформаційні активи організації, що, своєю чергою, допомагає зберегти довіру клієнтів та уникнути фінансових і репутаційних збитків, спричинених витоком даних. Однак підприємствам потрібно пам'ятати, що заходи, спрямовані на максимізацію безпеки даних, часто розчаровують користувачів і перешкоджають їхній продуктивності. Це може призвести до того, що користувачі почнуть обходити заходи безпеки, що в кінцевому підсумку зашкодить безпеці.

Наприклад, вимога складних і часто змінюваних паролів допомагає захистити акаунти від компрометації, але може також дратувати користувачів, що призводить до небезпечних практик, таких як повторне використання паролів або їх запис. Щоб уникнути цих проблем, організаціям потрібно збалансувати заходи безпеки баз даних з впливом на взаємодію з користувачами [1].

Таблиця 2

Приклади інформації яка повинна бути захищеною при використанні різних видів каналів комунікацій

Канал комунікації	Приклад використання	Що повинно бути захищено
Електронна пошта	Розсилка новин, підтвердження замовлень, підтримка клієнтів	Адреси клієнтів
		Вміст листів
		Сервери поштових систем
Месенджери (Viber, WhatsApp, Telegram)	Спілкування з клієнтом у реальному часі	Переписка
		Доступ до акаунтів
		Вкладення та файли
Телефонні дзвінки	Гаряча лінія, консультації, служба підтримки	Номери телефонів
		Записи дзвінків
		VoIP-інфраструктура
Онлайн-чати / чат-боти	Живий чат з консультантом на сайті	Дані користувача (ІПН, адреси, запити)
		Історія повідомлень
		Особисті дані
		API-з'єднання з CRM або базами даних
Соціальні мережі (Facebook, Instagram)	Повідомлення, коментарі, реклама	Дані акаунтів
		Повідомлення
		Фотографії
Платформи електронної комерції	Повідомлення в облікових записах користувача	Дані про замовлення
		Платіжна інформація
		Історія покупок
Розсилки SMS та push-сповіщення	Акції, сповіщення про замовлення	Телефонні номери
		Контент повідомлень
		Канали доставки
Відеоконференції (Zoom, Meet)	Онлайн-презентації, вебінари, підтримка	Доступ до конференцій
		Записи
		Посилання з доступом

Джерело: сформовано автором

Висновки. Якщо підприємство обирає цифрові канали для просування своєї продукції, важливою стратегічною складовою його діяльності має стати забезпечення кібербезпеки комунікацій зі споживачами. Формування та наповнення баз даних клієнтів становить лише початковий етап цифрової безпеки. Значно більш критичним є безперервний контроль за станом інформаційної системи та вжиття заходів щодо запобігання витоку конфіденційних даних. У сучасних умовах це є одним із ключових пріоритетів для керівництва підприємств, які прагнуть зберегти довіру споживачів, забезпечити стабільність бізнес-процесів і відповідати вимогам цифрової доби. Лише за умови системного підходу до кіберзахисту можна гарантувати безпечну та ефективну взаємодію з клієнтами у цифровому середовищі.

Список використаних джерел:

1. 13 найкращих практик для безпеки баз даних. *Corewin: веб-сайт.* URL: https://corewin.ua/blog/what-is-database-security/ (дата звернення: 23.07.2025).
2. Якою була атака хакерів на «Київстар» та як відновлювалась компанія. *DOU.ua*: веб-сайт. URL: https://dou.ua/lenta/news/kyivstar-cyber-attack-restoration/ (дата звернення: 23.07.2025).
3. Кіберзахист компанії в умовах війни перемагають сучасні технології. *Kyivstar Hub*: веб-сайт. URL: https://hub.kyivstar.ua/articles/kiberzahyst-kompaniyi-v-umovah-vijny-peremagayut-suchasni-tehnologiyi (дата звернення: 23.07.2025).
4. Основи кібербезпеки для бізнесу. *Westelecom*: веб-сайт. URL: https://westelecom.ua/blog/osnovy-kiberbezopasnosti-dla-biznesa (дата звернення: 23.07.2025).
5. Бурячок В. Л., Толубко В. Б., Хорошко В. О., Толюпа С. В. Інформаційна та кібербезпека: соціотехнічний аспект: підручник. Львів : «Магнолія 2006». 2024. 320 с.
6. Кормич Б. А. Інформаційна безпека: організаційно-правові основи: навчальний посібник. Київ : Кондор, 2004. 384 с.
7. Королюк Ю. Г., Чичун В. А. Менеджмент кібербезпеки в системі лояльності покупців. *Вісник Чернівецького торговельно-економічного інституту. Економічні науки.* 2023. №4 (92). С. 39–53. DOI: https://doi.org/10.34025/2310-8185-2023-4.92.03
8. Логіко-історичний аналіз довіри в контексті соціально-економічних відносин. URL: https://etet.org.ua/docs/ET_09_3_05_uk.pdf (дата звернення: 23.07.2025).
9. Пенюк В. О. Вплив інтернет-технологій на комунікативну культуру суспільства. *Міжнародний науковий журнал «Інтернаука". Серія: "Економічні науки».* 2023. № 6. DOI: https://doi.org/10.25313/2520-2294-2023-6-8979
10. Турчин Л. Є. Сутність поняття «довіра» як економічної категорії. *Ефективна економіка.* 2012. № 5. URL: http://www.economy.nayka.com.ua/?op=1&z=1173 (дата звернення: 23.07.2025).
11. Тлумачний словник. *Словник.ua:* веб-сайт. URL: https://slovnyk.ua/ (дата звернення: 23.07.2025).
12. Цифрове освітнє середовище педагога НУШ. *Всеосвіта:* веб-сайт. URL: https://vseosvita.ua/library/tsyfrove-osvitnie-seredovyshche-pedahoha-nush-teoretychnyi-keis-matematychna-haluz-825681.html (дата звернення: 23.07.2025).
13. Чирак І. М. Економіка соціальних медіа: навчальний посібник. Тернопіль : ЗУНУ. 2023. 300 с.
14. Юшков А. Г. Загрозливі тенденції використання ботоферм на шкоду державним інтересам України: Механізми запобігання та протидії. *Інформація і Право.* 2021. № 3(38). С. 90–98. DOI: https://doi.org/10.37750/2616-6798.2021.3(38).243812

References:

1. 13 naikrashchykh praktyk dlia bezpeky baz danykh [13 best practices for database security]. Available at: https://corewin.ua/blog/what-is-database-security/ (accessed July 23, 2025).
2. Yakoiu bula ataka khakeriv na "Kyivstar" ta yak vidnovliuvalas kompaniia [What was the hacker attack on Kyivstar and how was the company restored?]. Available at: https://dou.ua/lenta/news/kyivstar-cyber-attack-restoration/ (accessed July 23, 2025).
3. Kiberzakhyst kompanii v umovakh viiny peremahaiut suchasni tekhnolohii [Modern technologies are winning over a company's cyber defense in wartime]. Available at: https://hub.kyivstar.ua/articles/kiberzahyst-kompaniyi-v-umovah-vijny-peremagayut-suchasni-tehnologiyi (accessed July 23, 2025).
4. Osnovy kiberbezpeky dlia biznesu [Cybersecurity basics for business]. Available at: https://westelecom.ua/blog/osnovy-kiberbezopasnosti-dla-biznesa (accessed July 23, 2025).
5. Buriachok V. L., Tolubko V. B., Khoroshko V. O., Toliupa, S. V. (2024). *Informatsiina ta kiberbezpeka: sotsiotekhnichnyi aspekt: pidruchnyk* [Information and cybersecurity: sociotechnical aspect: textbook]. Lviv : «Mahnoliia 2006», 320 p. (in Ukrainian).
6. Kormych B. A. (2004). *Informatsiina bezpeka: orhanizatsiino-pravovi osnovy: navchalnyi posibnyk* [Information security: organizational and legal foundations: textbook]. Kyiv : Kondor, 384 p. (in Ukrainian).
7. Koroliuk Yu. H., Chychun V. A. (2023). Menedzhment kiberbezpeky v systemi loialnosti pokuptsiv [Cybersecurity management in the system of customer loyalty]. *Visnyk Chernivetskoho torhovelno-ekonomichnoho instytutu. Ekonomichni nauky – Bulletin of the Chernivtsi Institute of Trade and Economics. Economic Sciences.* Vol. №4 (92). pp. 39–53. DOI: https://doi.org/10.34025/2310-8185-2023-4.92.03
8. Lohiko-istorychnyi analiz doviry v konteksti sotsialno-ekonomichnykh vidnosyn [Logical-historical analysis of trust in the context of socio-economic relations]. Available at: https://etet.org.ua/docs/ET_09_3_05_uk.pdf (accessed July 23, 2025).
9. Peniuk V. O. (2023). Vplyv internet-tekhnolohii na komunikatyvnu kulturu suspilstva [The impact of Internet technologies on the communicative culture of society]. *Mizhnarodnyi naukovyi zhurnal "Internauka", Seriia: "Ekonomichni nauky" – International scientific journal "Internauka". Series: "Economic Sciences».* Vol. 6. DOI: https://doi.org/10.25313/2520-2294-2023-6-8979. Available at: https://www.inter-nauka.com/issues/economic2023/6/8979 (accessed July 23, 2025).
10. Turchyn L. Ye. (2012). Sutnist poniattia «dovira» yak ekonomichnoi katehorii [The essence of the concept of "trust" as an economic category]. *Efektyvna ekonomika – Effective Economy*. Vol. 5. Available at: http://www.economy.nayka.com.ua/?op=1&z=1173 (accessed July 23, 2025).

11. Tlumachnyi slovnyk [Explanatory dictionary]. Available at: https://slovnyk.ua/ (accessed July 23, 2025).
12. Tsyfrove osvitnie seredovyshche pedahoha NUSh [Digital educational environment of the NUS teacher]. Available at: https://vseosvita.ua/library/tsyfrove-osvitnie-seredovyshche-pedahoha-nush-teoretychnyi-keis-matematychna-haluz-825681.html (accessed July 23, 2025).
13. Chyrak I. M. (2023). *Ekonomika sotsialnykh media*: *navchalnyi posibnyk* [The economics of social media: textbook]. Ternopil: ZUNU. 330 p. (In Ukraininan).
14. Iushkov A. H. (2021). Zahrozlyvi tendentsii vykorystannia botoferm na shkodu derzhavnym interesam Ukrainy: Mekhanizmy zapobihannia ta protydii [Threatening trends in the use of bot farms to the detriment of the state interests of Ukraine: Prevention and countermeasure mechanisms]. *Informatsiia i Pravo – Information and Law.* Vol. 3(38), pp. 90–98. DOI: https://doi.org/10.37750/2616-6798.2021.3(38).243812