ливо важливо для підприємств, які працюють в умовах швидких технологічних змін та глобальної конкуренції.

Abstract. The article examines the peculiarities of applying Agile methodology to improve digital communications in enterprises. The main principles and methods of Agile, including Scrum, Kanban, and Lean, are analyzed, highlighting their contribution to enhancing the flexibility of communication processes, reducing bureaucratic barriers, and strengthening team collaboration. A comparison of traditional and agile approaches to digital communication management is conducted, allowing the identification of key advantages of Agile in modern conditions. A case study of the company «SoftServe» is analyzed separately, demonstrating its successful implementation of Agile to optimize internal and external communications. It is concluded that the application of Agile in digital communications promotes rapid adaptation to market changes, increases customer engagement, and improves the efficiency of communication management processes.

Keywords: Agile, digital communications, project management, agile methodologies, customer interaction, adaptation.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Ковальчук Н., Комарова К. Гнучкі підходи в управління командами. *Економіка та суспільство*. 2023. № 47. DOI: 10.32782/2524-0072/2023-47-20.

2. Якубенко І. М. Agile-менеджмент, як дієве управління проектами для цілеспрямованих команд. *Економіка. Менеджмент. Бізнес*. 2017. № 4(22). С. 167–172.

3. Що таке Agile і як його застосувати в бізнесі. *Brainrain.* 01.01.2025. URL: https://brainrain.com.ua/uk/chto-takoe-agile-ua/ (дата звернення: 26.02.2025).

4. Впровадження Agile-методологій для ефективного Product менеджменту. *London Product Academy.* 02.07.2025. URL: https://www.londonproduct.academy/post/vprovadzhennya-agile-metodologiy-dlya-efektivnogo-product-menedzhmentu (дата звернення: 26.02.2025).

5. Аналіз традиційного та гнучкого підходів до створення програмного забезпечення в динамічних умовах / Ю. Кордунова, О. Смотр, І. Кокотко, Р. Малець. *Інформаційні технології управління.* 2021. 7 с.

6. Як працює SoftServe – одна з найбільших українських IT-компаній. *Vector.* 14.01.2022 URL: https://vctr.media/ua/yak-praczyuye-softserve-117161/ (дата звернення: 27.02.2025).

УДК 004.032.26:004.056

ПОПЕРЕДЖЕННЯ КОМП'ЮТЕРНОЇ АТАКИ ТИПУ «MAN IN THE MIDDLE», ЩО ЗДІЙСНЮЄТЬСЯ ЗА ДОПОМОГОЮ ГЕНЕРАТИВНОГО ШТУЧНОГО ІНТЕЛЕКТУ

М. А. Ласкавчук, Л. В. Загоруйко

Анотація. У дослідженні розглянуто комп'ютерну атаку типу «Man in the Middle», наведено її основні методи реалізації та потенційні загрози. Особливу увагу приділено ролі генеративного штучного інтелекту, який дає змогу навіть користувачам із мінімальними знаннями у сфері кібербезпеки здійснювати подібні атаки. Запропоновано підхід до виявлення та попередження атак за допомогою системи запобігання вторгненням, що підвищує рівень безпеки інформаційного середовища.

Ключові слова: комп'ютерна атака, людина посередині, кібератака, штучний інтелект, кібербезпека.

Вступ. За інформацію Державної служби спеціального зв'язку та захисту інформації України, урядова команда реагування на комп'ютерні надзвичайні події CERT-UA, яка діє при Держспецзв'язку, у 2024 р. опрацювала 4 315 кіберінцидентів [1]. Це на 69,8 % більше, ніж роком раніше, коли кіберзлочинці атакували український кіберпростір 2 541 раз. Найпоширенішими типами інцидентів є розповсюдження шкідливого програмного забезпечення, фішинг, шкідливе підключення, компрометація облікового запису або системи. Метою зловмисників є викрадення чутливої інформації, а також знищення даних та інформаційних систем [1]. Існують різні методи проведення комп'ютерних атак, одним із таких методів є атака типу «людина посередині» (англ. *man in the middle,* далі – MITM). Наразі неможливо навести статистику збитків, що відбуваються саме від комп'ютерних атак типу MITM, оскільки кожен випадок атаки має свої унікальні характеристики та наслідки. Поширеність кіберзагроз у всіх сферах суспільного та державного життя, а також удосконалення методів їх реалізації, зокрема із застосуванням штучного інтелекту, актуалізують необхідність глибокого аналізу механізмів та сценаріїв кібератак. Це вимагає перегляду наявних стратегій і тактик протидії, а також пошуку нових підходів для підвищення ефективності кіберзахисту.

Відповідно до статті 1 Закону України «Про основні засади забезпечення кібербезпеки України» [2], кібератака (комп'ютерна атака) – це спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включно з інформаційно-комунікаційними технологіями, програмними, програмно-апаратними засобами, іншими технічними та технологічними засобами і обладнанням) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту.

Комп'ютерна атака типу MITM – це ситуація, коли суб'єкт використовує різні методики та технічні рішення, спрямовані на отримання доступу до трафіка та його декодування. Ця комп'ютерна атака реалізується із застосуванням алгоритмів перехоплення трафіка, що передається між двома кінцевими пристроями [3].

Атаки MITM можуть починатися з [3–4]:

– «отруєння» кешу протоколу дозволу адрес (ARP);
– підробка DNS;
– підміна IP-адреси;
– викрадення сеансу;
– перехоплення SSL;
– атаки на Wi-Fi;
– атаки Evil Twin;
– перехоплення електронної пошти;
– перехоплення Bluetooth.

На рис. 1 наведено, як відбувається атака MITM.

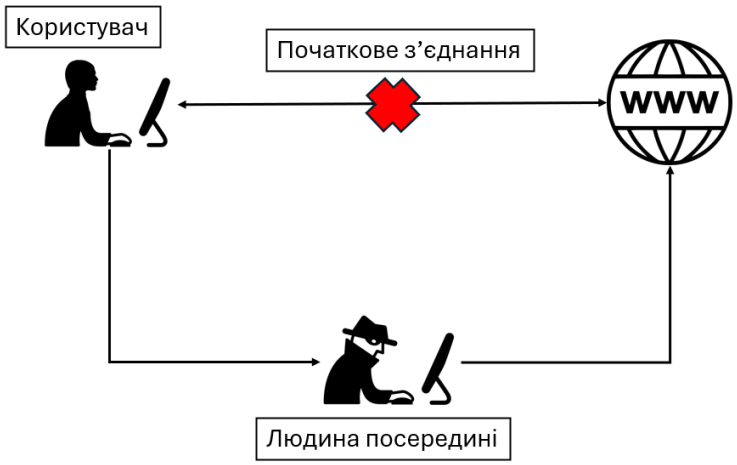

Рис. 1. Процес атаки MITM

Один із випадків таких атак відомий як динамічне підслуховування, під час якого зловмисники створюють незалежні асоціації з жертвами і впливають на комунікацію між користувачами, модифікуючи повідомлення між двома користувачами, щоб вплинути на довіру між ними. Зловмисник має можливість перехоплювати повідомлення між ними з метою їх модифікації. Більшість криптографічних угод включають у себе певну перевірку кінцевих точок, в основному для того, щоб протистояти MITM-атакам [4].

Класична MITM-атака проходить у два етапи.

Перший – перехоплення даних, коли злочинець інтегрується в середовище передачі даних. Далі за допомогою спуфінгу реалізує підміну IP-адрес, ARP10-повідомлень, сервера доменних імен тощо. Атаки MITM найчастіше використовують ARP-кеш, який являє собою локальний кеш із призначеними IP-адресами і зіставленими фізичними унікальними ідентифікаторами

пристроїв у мережі (MAC-адресами). Внаслідок цього реалізуються завдання отримання відомостей про структуру досліджуваної мережі та зіставлення локальних ідентифікаторів і універсальних ідентифікаторів мережі (MAC-адрес).

Другий етап – дешифрація, отримання доступу до зашифрованих даних. Оскільки існує велике розмаїття методик проведення атаки та методик протидії, однією з яких є аналіз вихідного коду (як встановлюваних застосунків, так і дослідження переданих даних у межах «пісочниці» на віртуальній машині та без наявності виходу у відкриту мережу). Такий аналіз може здійснюватися вручну фахівцем або за допомогою рішень, створених на основі навченого за відповідним напрямом ШІ.

Ще один випадок – атака типу «людина в браузері». Це особливий підтип MITM-атаки, що відбувається на кінцевій точці зв'язку [5]. В основі «людина в браузері» лежить ідея розміщення шкідливого прозорого браузера між браузером жертви та вебсервером, до якого жертва звертається для отримання послуги (наприклад, банківської послуги, соціальної мережі тощо). Метою атаки є перехоплення, запис і маніпулювання будь-яким обміном даними між жертвою і постачальником послуг [18–19]. На рис. 2 наведено атаку «людина в браузері».

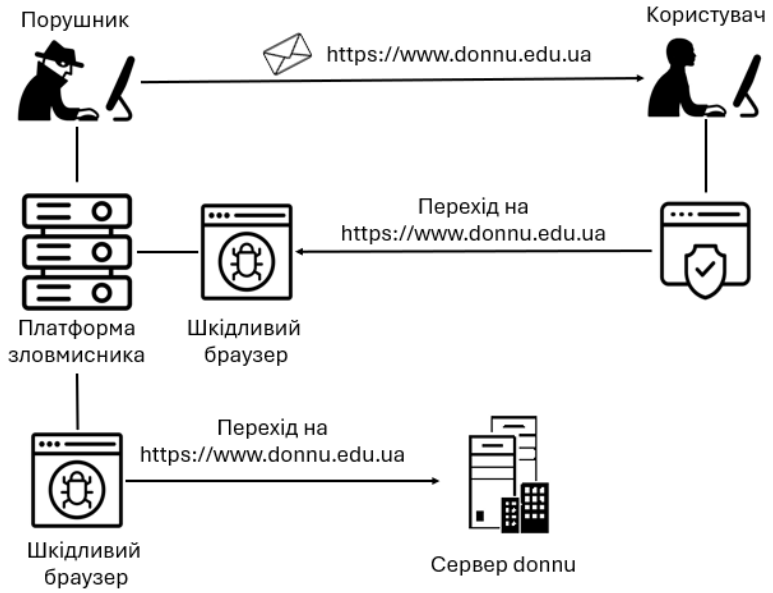

Рис. 2. Атака «людина в браузері»

– Порушник: комп'ютерний злочинець, метою якого є порушення приватності жертви, а також конфіденційності, цілісності та доступності даних, якими обмінюються дві кінцеві точки. Зловмисник встановлює і контролює шкідливий сервер, який слугує прозорим веббраузером для кінцевого користувача [6].

– Користувач: потерпілий, який за допомогою фішингових методів отримує доступ до шкідливого сервера (на якому розміщений прозорий веббраузер), налаштованого зловмисником, і починає користуватися вебдодатком [6].

– Ціль: вебдодаток, здатний надавати конфіденційні та/або цінні послуги (наприклад, банківські послуги, поштові сервіси тощо), доступ до яких здійснюється за допомогою механізму автентифікації [6].

Наступні кроки описують техніку атаки «людина в браузері» [6]:

а) порушник створює підроблене гіперпосилання, що вказує на шкідливий сервер. Посилання надсилається жертві, яку за допомогою фішингових методів заманюють натиснути на нього та пройти автентифікацію у вебдодатка;

б) натиснувши на шкідливе гіперпосилання у власному браузері, користувач мимоволі підключається до шкідливого сервера, де знаходиться прозорий веббраузер разом з низкою програм (наприклад, вебпроксі, сніффер, кейлоггер, надбудови тощо), які зловмисник використовує для перехоплення, запису та маніпулювання даними, якими обмінюються жертва та цільова вебпрограма;

в) шкідливий сервер отримує доступ до цільового вебдодатка (наприклад, банківського додатка, соціальної мережі тощо) через шкідливий веббраузер абсолютно прозорим способом. На цьому етапі користувач зможе використовувати всі функціональні можливості цільового додатка (плюс ті, які тепер може запропонувати зловмисний сервер). Усі операції жертви тепер можуть бути перехоплені, а отже, записані і використані зловмисником для маніпуляцій. Наприклад, порушник зможе перехопити облікові дані, надані жертвою в якійсь формі автентифікації, незалежно від того, які протоколи безпеки налаштовані у вебдодатку. Жертва зможе користуватися всіма функціями додатка за допомогою браузера, який, без її відома, підключений до шкідливого сервера.

Найпростіший спосіб здійснити атаку – це скористатися штучним інтелектом. На рис. 3 наведено те, як штучний інтелект пропонує здійснити цю атаку.

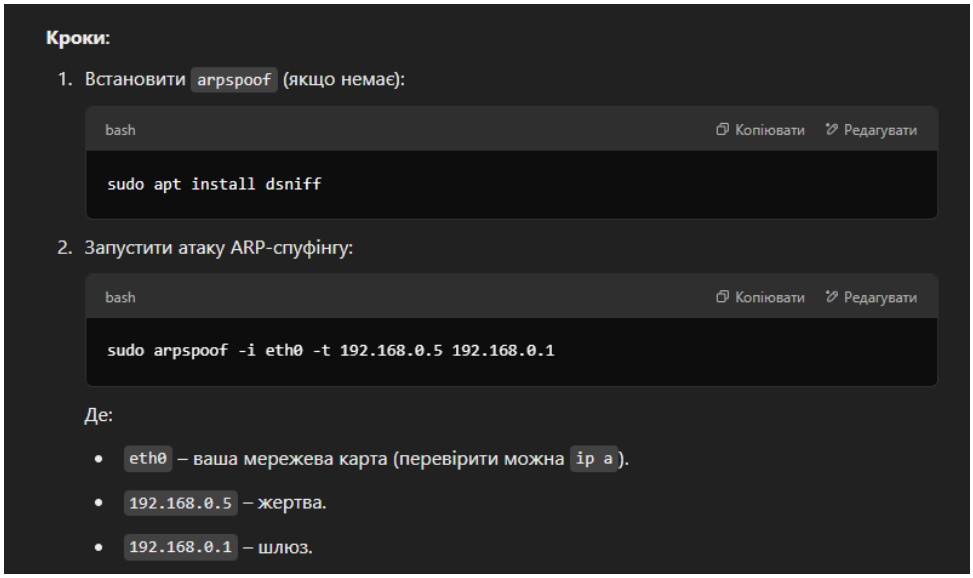

Рис. 3. Підміна ARP-пакетів

Застосування цієї атаки наведено на рис. 4.

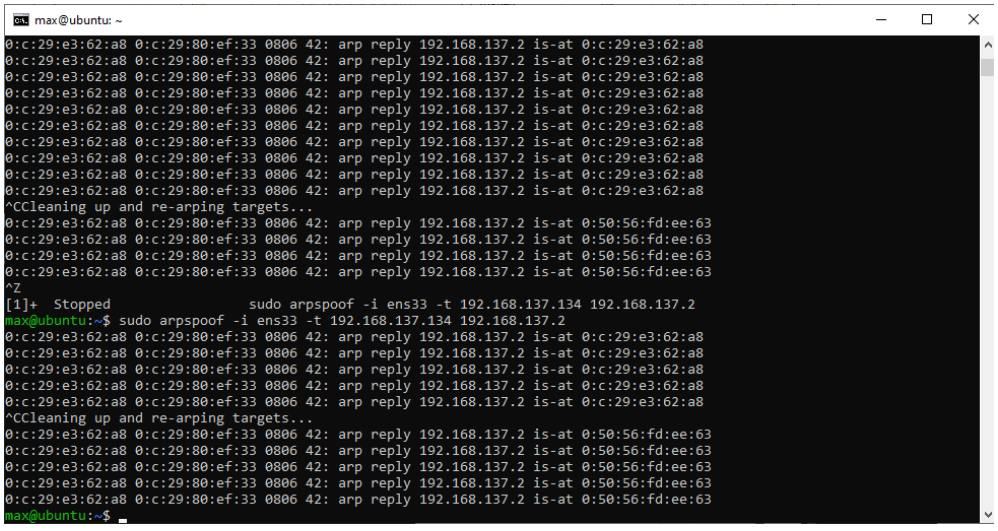

Рис. 4. Застосування підміни ARP-пакетів

Для попередження цієї атаки буде використовуватися Snort IPS – провідна система запобігання вторгненням з відкритим вихідним кодом [7]. Snort IPS використовує низку правил, які допомагають визначити зловмисну мережеву активність, і на основі цих правил знаходить пакети, які їм відповідають, та генерує сповіщення для користувачів [7].

Для розблокування правил відстеження підміни ARP-пакетів був змінений конфігураційний файл (рис. 5).

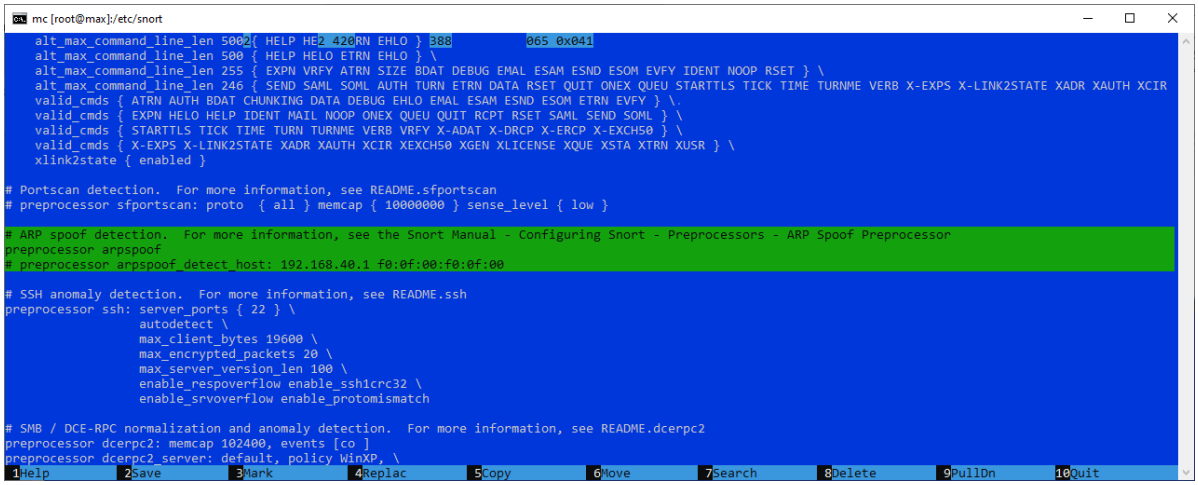

Рис. 5. Конфігураційний файл Snort

Результат попередження підміни ARP-пакетів наведено на рис. 6.

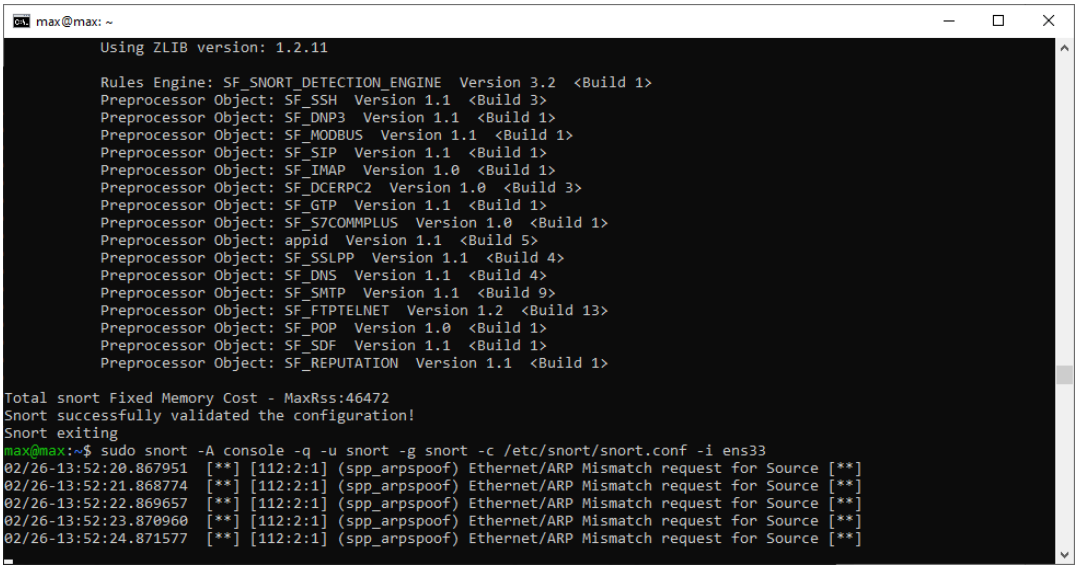

Рис. 6. Попередження атаки

Висновки. Під час дослідження було проаналізовано комп'ютерну атаку «Man in the Middle», розглянуто її різновиди та основні методи реалізації. Особливу увагу приділено використанню генеративного штучного інтелекту, який значно спрощує здійснення подібних атак, навіть для осіб із мінімальними знаннями у сфері кібербезпеки. На основі проведеного аналізу запропоновано підхід до виявлення та попередження таких атак за допомогою системи запобігання вторгненням, що сприяє підвищенню рівня інформаційної безпеки.

Abstract. The study examines the Man in the Middle computer attack, describes its main methods of implementation and potential threats. Particular attention is paid to the role of generative artificial intelligence, which allows even users with minimal knowledge of cybersecurity to carry out such attacks. An approach to detecting and preventing attacks using an intrusion prevention system is proposed, which increases the level of security of the information environment.

Keywords: computer attack, man in the middle, cyberattack, artificial intelligence, cybersecurity.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. CERT-UA минулого року опрацювала 4315 кіберінцидентів. 08.01.2025. URL: https://cip.gov.ua/ua/news/cert-ua-minulogo-roku-opracyuvala-4315-kiberincidentiv

2. Закон України «Про основні засади забезпечення кібербезпеки України», 2017, № 45. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

3. Man in the Middle Attacks: Analysis, Motivation and Prevention / D. Javeed, U. Mohammed Badamasi, C. O. Ndubuisi, F. Soomro, M. Asif. *International Journal of Computer Networks and Communications Security.* Vol. 8, № 7, July 2020. P. 52–58.

4. Security risks from the modern man-in-the-middle attacks, January 2025 URL: https://www.meste.org/mest/MEST_Najava/XXV_Cekerevac.pdf

5. Man-in-the-browser attacks against IoT devices: a study of smart homes, April 2021 URL: https://www.researchgate.net/profile/Samuli-Laato/publication/350907813_Man-in-the-Browser_Attacks_Against_IoT_Devices_A_Study_of_Smart_Homes/links/607d30b3881fa114b4111176/Man-in-the-Browser-Attacks-Against-IoT-Devices-A-Study-of-Smart-Homes.pdf

6. Browser-in-the-Middle (BitM) attack, April 2021 URL: https://link.springer.com/content/pdf/10.1007/s10207-021-00548-5.pdf

7. What is Snort? URL: https://www.snort.org/

УДК 004:005:51

ЗАСТОСУВАННЯ ПОЛІНОМА ЛАГРАНЖА ДЛЯ ІНТЕРПОЛЯЦІЇ ОБСЯГУ ЕЛЕКТРОННОЇ ТОРГІВЛІ У СФЕРІ ІНФОРМАЦІЙНИХ ПОСЛУГ

В. О. Лисак, Н. А. Потапова

Анотація. У статті досліджено тенденції розвитку електронної торгівлі у сфері комп'ютерного програмування та надання інформаційних послуг. Проведено аналіз статистичних даних щодо частки підприємств, які здійснюють онлайн-продажі, та обсягів реалізованої продукції через вебсайти. Для оцінки показників використано інтерполяційний поліном Лагранжа. Отримані результати дають змогу оцінити можливості застосування методів обчислень під час оцінкизмін у сфері цифрової економіки.

Ключові слова: методи обчислень, інтерполяція, поліном Лагранжа, електронна торгівля, інформаційні послуги.

Вступ. В умовах цифрової трансформації економіки все більшого значення набуває розвиток електронної торгівлі, яка виступає важливим індикатором рівня впровадження інформаційних технологій у різні сектори бізнесу. Аналіз тенденцій розвитку електронної комерції дає змогу оцінити динаміку цифровізації підприємств та прогнозувати подальші зміни в цій сфері. Особливу увагу привертає аналіз показників електронної торгівлі в галузі комп'ютерного програмування та надання інформаційних послуг, оскільки ця сфера безпосередньо впливає на розвиток галузі інформаційних технологій.

Останніми роками спостерігається зростання використання цифрових платформ у різних сферах ведення бізнесу, що впливає на його організацію та способи комунікації з клієнтами. Зокрема, підприємства все активніше впроваджують онлайн-продажі через власні вебсайти, що дає змогу розширювати клієнтську базу та збільшувати обсяги реалізованої продукції. Частка електронної торгівлі у загальному обсязі продажів варіюється залежно від специфіки галузі та рівня технологічної готовності підприємств. Для сфери комп'ютерного програмування та надання інформаційних послуг характерний високий рівень інтеграції цифрових інструментів, що сприяє активному використанню електронної комерції.

Аналіз останніх досліджень [1; 2] свідчить про важливість оцінки показників розвитку електронної торгівлі з метою формування ефективних рішень у бізнес-стратегії. Різні математичні моделі використовуються для оцінки змін показників, що дає змогу підприємствам більш ефективно планувати свою діяльність. Водночас необхідність проведення аналітичних розрахунків моделей динаміки залишається актуальною проблемою, оскільки вони дають змогу визначити характеристики нелінійності процесів.

Для побудови моделей динаміки доцільним є використання методів обчислень, зокрема методів інтерполяції [3]. Одним із таких підходів є визначення інтерполяційного полінома Лагранжа, який дає змогу моделювати динаміку змін на основі наявних статистичних даних.

Метою статті є дослідження використання інтерполяційного полінома Лагранжа для оцінки динаміки показників електронної торгівлі у сфері комп'ютерного програмування та надання інформаційних послуг на основі статистичних даних за 2020–2023 рр. У дослідженні буде розглянуто основні тенденції електронної торгівлі у зазначеній галузі, проведено аналіз можливостей використання методів обчислень для інтерполяції даних та оцінено точність отриманих результатів.

Основна частина. Теоретичною основою розрахунку інтерполяційного полінома Лагранжа, що використовується для прогнозної оцінки в електронній торгівлі та сфері інформаційних