УДК 004.056+004.8+316.6+343.9 DOI https://doi.org/10.35546/kntu2078-4481.2025.4.3.19

О. С. ПАРХОМЕНКО
магістрант
Сумський державний університет
ORCID: 0009-0004-7731-0274

В. В. КОВАЛЬ
кандидат фізико-математичних наук,
старший викладач кафедри кібербезпеки
Сумський державний університет
ORCID: 0000-0002-1593-5605

ЕВОЛЮЦІЯ ШАХРАЙСЬКОГО КОНТЕНТУ В УМОВАХ РОЗВИТКУ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА ШІ

Стаття присвячена аналізу трансформації шахрайського контенту під впливом швидкого розвитку генеративного штучного інтелекту та нових викликів для сучасної кібербезпеки. Показано, що публічно доступні й спеціалізовані ШІ-інструменти радикально змінили ландшафт кіберзлочинності. Зловмисники здатні створювати реалістичний синтетичний контент практично без витрат з мінімальними технічними навичками. Дослідження порівнює традиційні методи соціальної інженерії, коли фішингові повідомлення створювалися вручну й часто містили мовні помилки, із сучасними ШІ-підходами, які забезпечують масштабування атак без пропорційного зростання витрат, глибоку персоналізацію під конкретну жертву, адаптивність у реальному часі та повну автоматизацію всіх етапів шахрайської кампанії від аналізу викрадених даних до генерації контенту. Окремо виділено переваги ШІ для зловмисників: низька собівартість, висока реалістичність, залучення низькокваліфікованих виконавців, а також обмеження. Констатовано, що традиційні методи виявлення фейкового контенту втратили ефективність, а deepfake-технології створюють загрозу не лише індивідуальній безпеці, а й політичній стабільності та довірі до медіа. Запропоновано зміщення парадигми кіберзахисту: від реактивного пошуку відомих індикаторів до проактивного аналізу контексту, поведінкових аномалій, верифікації джерела ідентичності та використання спеціалізованих систем детекції синтетичного контенту. ШІ є одночасно потужним каталізатором зростання кіберзлочинності та ключовим інструментом протидії. Ефективна протидія можлива лише за умови інтегрованого міждисциплінарного підходу, який поєднує технічні інновації, підвищення цифрової грамотності населення, посилення законодавчого регулювання та міжнародну координацію.

Ключові слова: *штучний інтелект, соціальна інженерія, синтетичний контент, deepfake, кібербезпека, фішинг, шахрайство.*

O. S. PARKHOMENKO
Magister
Sumy State University
ORCID: 0009-0004-7731-0274

V. V. KOVAL
Candidate of Physical and Mathematical Sciences,
Senior Lecturer at the Department of Cybersecurity
Sumy State University
ORCID: 0000-0002-1593-5605

THE EVOLUTION OF FRAUDULENT CONTENT IN THE CONTEXT OF THE DEVELOPMENT OF INFORMATION TECHNOLOGY AND AI

The article is devoted to the analysis of the transformation of fraudulent content under the influence of the rapid development of generative artificial intelligence and new challenges for modern cybersecurity. It is shown that publicly available and specialized AI tools have radically changed the cybercrime landscape. Attackers are able to create realistic synthetic content at virtually no cost with minimal technical skills. Study compares traditional social engineering methods, when phishing messages were created manually and often contained language errors, with modern AI approaches that provide scaling of attacks without proportional increase in costs, deep personalization for

a specific victim, real-time adaptability and full automation of all stages of a fraudulent campaign from analysis of stolen data to content generation. Advantages of AI for attackers are highlighted: low cost, high realism, involvement of low-skilled performers, as well as limitations. It is stated that traditional methods of detecting fake content have lost their effectiveness, and deepfake technologies pose a threat not only to individual security, but also to political stability and trust in the media. A shift in the paradigm of cyber defense is proposed: from reactive search for known indicators to proactive analysis of the context, behavioral anomalies, verification of the source of identity and the use of specialized synthetic content detection systems. AI is both a powerful catalyst for the growth of cybercrime and a key tool for counteraction. Effective counteraction is possible only with an integrated interdisciplinary approach that combines technical innovations, increasing the digital literacy of the population, strengthening legislative regulation and international coordination.

Key words: *artificial intelligence, social engineering, synthetic content, deepfake, cybersecurity, phishing, fraud.*

Постановка проблеми

Розвиток генеративного штучного інтелекту (ШІ) докорінно змінює ландшафт шахрайського контенту. Так, за даними Федерального бюро розслідувань США (FBI), кіберзлочинці активно застосовують публічно доступні та спеціальні ШІ-інструменти для організації високотаргетованих фішингових кампаній і шахрайських дзвінків із клонуванням голосів чи обличь [1]. ШІ дозволяє зловмисникам створювати переконливі повідомлення з бездоганною граматикою та видимою персоналізацією, що суттєво підвищує ймовірність успішної атаки.

У зв'язку з цим стає очевидною гостра проблема – традиційні методи виявлення фейкового контенту перестають бути достатньо ефективними.

Зростання масштабів шахрайства підтверджують і інші експертні дані: неурядові дослідження вказують, що злочинці «інтегрують ШІ на всіх етапах своєї діяльності», зокрема для створення фальшивих особистостей і аналізу викрадених даних. Отже, необхідно дослідити, як розвиток ШІ вплинув на еволюцію шахрайського контенту та які нові виклики це створює для кібербезпеки [2].

Аналіз останніх досліджень і публікацій

Сучасна література фокусується на різних аспектах впливу ШІ на дезінформацію та шахрайство. У роботі [3] відзначають, що deepfake-відео й інший мультимедійний фальшивий контент стають серйозною суспільною проблемою. За їхнім звітом, «зловмисники використовують технології deepfake для поширення фальшивої інформації (зображень, відео та аудіо)», що загрожує політиці, безпеці та приватності. Дослідники виділяють основні виклики у виявленні таких матеріалів, зокрема брак якісних тренувальних даних і швидку еволюцію методів підробки.

У роботі [4] підкреслюють, що генеративний ШІ «піднімає фейкові новини на новий рівень»: нині можливо «масово автоматизувати створення великої кількості високоякісних адресованих фейкових новин». Автори відзначають, що генеративні моделі створюють реалістичний мультимедійний контент «майже безкоштовно», що суттєво ускладнює відрізнення реального від штучного.

Ще один напрям – вплив ШІ на фішингові атаки. У роботі [5] зазначають, що з появою генеративних моделей фішинг став «експоненційно небезпечнішим». Їхній аналіз свідчить, що інструменти ШІ посилюють соціальну інженерію: цей висновок корелює із звітом Всесвітнього економічного форуму, де зазначено, що можливості emerging-технологій (зокрема генерувального ШІ) значно посилюють фішинг і суміжні загрози.

Автори [6] провели хронологічний огляд кіберзлочинів і підкреслили тенденцію збільшення шкоди: за даними IC3 у США, у 2024 році отримано 859 тис. повідомлень про кіберзлочини із загальними втратами $16 млрд (на 33% більше, ніж у 2023). Автори зауважують, що «поки технології розвиваються, так само зростають пов'язані з ними атаки, такі як AI-атаки та deepfake».

Аналіз сучасних досліджень дозволяє констатувати: сучасна наукова спільнота фіксує зростаючі масштаб і складність шахрайства за рахунок ШІ та потребує розробки новітніх, інколи кардинально інших, інструментів для протидії (наприклад, нові методи детекції deepfake).

Формулювання мети дослідження

Метою дослідження є аналіз трансформації шахрайського контенту під впливом розвитку генеративних технологій штучного інтелекту, виявлення особливостей особливо у соціальній інженерії, а також спроба визначення нових викликів для кібербезпеки, пов'язаних із поширенням синтетичного контенту.

Для досягнення виділимо основні дослідити еволюцію методів створення шахрайського матеріалу, класифікувати види контенту, що генерується ШІ, оцінити переваги та недоліки його використання з боку зловмисників, а також окреслити напрями удосконалення механізмів протидії.

Викладення основного матеріалу дослідження

На основі проведених аналізів наукових публікацій [7-8] та сучасних досліджень [9-10] можна виділити кілька ключових аспектів впливу штучного інтелекту на еволюцію шахрайського контенту, а саме: історичні методи соціальної інженерії, трансформація атак із появою ШІ–технологій, особливості контенту, що ним створюється, а також переваги й недоліки його використання з позиції зловмисників.

1. Традиційні методи створення шахрайського контенту

До появи технологій штучного інтелекту соціальна інженерія базувалася здебільшого на ручній роботі та психологічних техніках впливу. Підготовка фішингових повідомлень, підроблених документів чи візуальних матеріалів вимагала часу та певних навичок. Обмежений доступ до технічних засобів та характерні мовні або стилістичні помилки часто давали змогу розпізнати обман як користувачам, так і системам захисту.

2. Вплив розвитку ШІ на шахрайські кампанії

Поширення ШІ радикально змінило підхід до створення шахрайського контенту. Вони здатні аналізувати великі обсяги даних, навчатися на них і генерувати новий матеріал, що виглядає реалістично. Завдяки цьому зловмисники отримали змогу проводити атаки на значно ширшому масштабі та з меншими ресурсними витратами.

3. Контент, що застосовується у шахрайстві

Розвиток ШІ дозволив створювати різні види контенту, що активно використовується у шахрайстві:

- текстові матеріали;
- зображення, аудіо та відео;
- шкідливе програмне забезпечення.

Ключовою характеристикою такого контенту є правдоподібність, яка у багатьох випадках перевищує можливості людини виявити підробку без спеціальних засобів.

4. Переваги та недоліки ШІ з точки зору зловмисників

Використання ШІ у шахрайстві надає значні переваги порівняно з традиційними методами, хоча водночас має й певні обмеження.

Переваги:

- масштабування атак майже без додаткових витрат;
- висока персоналізація та психологічний вплив;
- автоматизація процесів соціальної інженерії;
- адаптивність під жертву в режимі реального часу.

Недоліки:

- залежність від тренувальних даних: помилки або артефакти можуть викривати підробку;
- складність контролю над генерацією та ризик «відхиленої поведінки» моделей;
- потреба у технічній інфраструктурі та певних знаннях для навчання систем.

Таке співвідношення переваг і недоліків формує нову проблему – можливість залучення нефахових зловмисників до проведення складних або масштабних атак.

5. Вплив на сучасну кібербезпеку

Факт застосування ШІ у соціальній інженерії зумовлює структурні зміни у сфері захисту. Атаки стають динамічними, коригуються на основі реакції жертви та можуть точково імітувати її середовище. Це ускладнює процес розпізнавання обману як на технічному, так і на психологічному рівні.

У відповідь на нові загрози фокус кіберзахисту зміщується від пошуку ознак фальсифікації у повідомленні до комплексної оцінки контексту та поведінкових факторів, включно із:

- перевіркою достовірності джерела ідентичності;
- аналізом поведінкових аномалій у комунікації;
- використанням систем виявлення синтетичних даних.

Таким чином, протидія шахрайському контенту, створеному за допомогою ШІ, потребує інтеграції технічних рішень із підготовкою користувачів, посиленням правового регулювання та міжнародної співпраці.

Висновки

Поява та швидкий розвиток штучного інтелекту призвели до суттєвих змін у сфері кіберзлочинності. Якщо традиційні шахрайські схеми ґрунтувалися на ручній роботі та мали помітні ознаки підробки, то сучасні інструменти дозволяють створювати реалістичний контент із персоналізацією під конкретну жертву. Це значно знижує ймовірність розпізнавання шахрайства кінцевим користувачем та збільшує ефективність соціальної інженерії.

У таких умовах ключовим стає переорієнтування стратегій кіберзахисту: від реагування на відомі індикатори атаки – до виявлення поведінкових та контекстуальних аномалій, застосування систем детекції синтетичного контенту, багатофакторної верифікації та посилення інформаційної грамотності користувачів. Штучний інтелект є водночас чинником підвищення загроз і важливим інструментом протидії їм, що потребує інтегрованого та міждисциплінарного підходу до забезпечення інформаційної безпеки.

Список використаної літератури

1. FBI San Francisco: FBI Warns of Increasing Threat of Cyber Criminals Utilizing Artificial Intelligence [Electronic resource]. Access mode: https://www.fbi.gov/contact-us/field-offices/sanfrancisco/news/fbi-warns-of-increasing-threat-of-cyber-criminals-utilizing-artificial-intelligence (last access: 06.11.2025). Title from the screen.

2. Arafah, M., Karadsheh, L., Aburub, F., & Alhariri, S. AI-Powered Social Engineering and Impersonation Attacks. In A. Almomani & M. Alauthman (Eds.). *Examining Cybersecurity Risks Produced by Generative AI, IGI Global Scientific Publishing*, 2025. P. 123-142. DOI: https://doi.org/10.4018/979-8-3373-0832-6.ch006.

3. Kaur A., Noori Hoshyar A., Saikrishna V., Firmin S., Xia, F Deepfake video detection: challenges and opportunities *Artificial Intelligence Review*. 2024. Vol. 57, N. 6. DOI: https://doi.org/10.1007/s10462-024-10810-6.

4. Loth A., Kappes M., Pahl M.-O. Blessing or curse? A survey on the impact of generative AI on fake news. *arXiv.org*, 2024 [Online]. Available: http://arxiv.org/abs/2404.03021v1.

5. Jabir R., Le J., Nguyen C. Phishing Attacks in the Age of Generative Artificial Intelligence: A Systematic Review of Human Factors. *AI*. 2025. Vol. 6, N. 8. P. 174. DOI: https://doi.org/10.3390/ai6080174.

6. Abdullah M., Nawaz M. M., Saleem B., Zahra M., Ashfaq E., Muhammad Z. Evolution Cybercrime–Key Trends, Cybersecurity Threats, and Mitigation Strategies from Historical Data. *Analytics*. 2025. Vol. 4, N. 3. P. 25. DOI: https://doi.org/10.3390/analytics4030025.

7. Suela L. C. Online Fraud Exposed: Tactics and Strategies of Cyber Scammers. *Interantional journal of scientific research in engineering and management*. 2024. Vol. 08, N. 04. P. 1–5. DOI: https://doi.org/10.55041/ijsrem31604.

8. Carter E. The anatomy of written scam communications: An empirical analysis. *Crime, Media, Culture: An International Journal*. 2015. Vol. 11, №. 2. P. 89–103. DOI: https://doi.org/10.1177/1741659015572310.

9. Górka M. Manipulation techniques of cyber fraudsters using the example of phishing attempts for private content. *Przegląd Policyjny*. 2023. Vol. 150, N. 2. P. 207–220. DOI: https://doi.org/10.5604/01.3001.0053.8540.

10. Oroșanu M., Alexandru M. Cybercrime: A New Challenge of Criminality in the Digital Age. In *International Conference on Cybersecurity and Cybercrime*, 2024, Vol. 11, P. 115-121, DOI:https://doi.org/10.19107/CYBERCON.2024.16.

References

1. FBI San Francisco: FBI Warns of Increasing Threat of Cyber Criminals Utilizing Artificial Intelligence [Electronic resource]. Access mode: https://www.fbi.gov/contact-us/field-offices/sanfrancisco/news/fbi-warns-of-increasing-threat-of-cyber-criminals-utilizing-artificial-intelligence (last access: 06.11.2025). Title from the screen.

2. Arafah, M., Karadsheh, L., Aburub, F., & Alhariri, S. (2025). AI-Powered Social Engineering and Impersonation Attacks. In A. Almomani & M. Alauthman (Eds.), *Examining Cybersecurity Risks Produced by Generative AI*, 123-142. IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3373-0832-6.ch006.

3. Kaur A., Noori Hoshyar A., Saikrishna V., Firmin S., Xia F. (2024). Deepfake video detection: challenges and opportunities. *Artificial Intelligence Review*, 57(6). https://doi.org/10.1007/s10462-024-10810-6.

4. Loth A., Kappes M., Pahl M.-O. (2024) Blessing or curse? A survey on the impact of generative AI on fake news. *arXiv.org* [Online]. Available: http://arxiv.org/abs/2404.03021v1.

5. Jabir R., Le J., Nguyen C. (2025). Phishing Attacks in the Age of Generative Artificial Intelligence: A Systematic Review of Human Factors. *AI*, 6(8), 174. https://doi.org/10.3390/ai6080174.

6. Abdullah M., Nawaz M. M., Saleem B., Zahra M., Ashfaq E., Muhammad, Z. (2025). Evolution Cybercrime–Key Trends, Cybersecurity Threats, and Mitigation Strategies from Historical Data. *Analytics*, 4(3), 25. https://doi.org/10.3390/analytics4030025

7. Suela, L. C. (2024). Online Fraud Exposed: Tactics and Strategies of Cyber Scammers. *Interantional journal of scientific research in engineering and management*, 08(04), 1–5. https://doi.org/10.55041/ijsrem31604.

8. Carter E. (2015). The anatomy of written scam communications: An empirical analysis. *Crime, Media, Culture: An International Journal*, 11(2), 89–103. https://doi.org/10.1177/1741659015572310.

9. Górka M. (2023). Manipulation techniques of cyber fraudsters using the example of phishing attempts for private content. *Przegląd Policyjny*, 150(2), 207–220. https://doi.org/10.5604/01.3001.0053.8540.

10. Oroșanu M., Alexandru M. (2024). Cybercrime: A New Challenge of Criminality in the Digital Age. In *International Conference on Cybersecurity and Cybercrime*, Vol. 11, 115-121, https://doi.org/10.19107/CYBERCON.2024.16.

Дата першого надходження рукопису до видання: 22.11.2025
Дата прийнятого до друку рукопису після рецензування: 19.12.2025
Дата публікації: 31.12.2025