УДК 004.056:004.85

Є. А. Садовник

Т. Г. Кирилащук

ЯК ФІШИНГ ЕВОЛЮЦІОНУЄ В ЕПОХУ ШІ

Вінницький національний технічний університет

Анотація. *У роботі розглянуто проблему еволюції соціальної інженерії під впливом спеціалізованих ШІ моделей. Проведено аналіз потенційних наслідків таких атак, зокрема ризиків витоку конфіденційної інформації та фінансових втрат. Запропоновано ефективні методи захисту, що спрямовані на зменшення вразливостей і підвищення безпеки сучасних ІТ– систем.*

Ключові слова: штучний інтелект, фішинг, кібербезпека, автоматизація атак, соціальна інженерія, виявлення аномалій.

Abstract. *The paper considers the problem of the evolution of social engineering under the influence of specialized AI models. An analysis of the potential consequences of such attacks, in particular the risks of confidential information leaks and financial losses, is carried out. Effective protection methods are proposed, aimed at reducing vulnerabilities and improving the security of modern IT systems.*

Keywords: artificial intelligence, phishing, cybersecurity, attack automation, social engineering, anomaly detection.

Вступ

Впровадження та розвиток штучного інтелекту (ШІ) надає користувача та компаніям великі можливості – починаючи від автоматизації процесів до створення власних проєктів. Але попри це кібератаки зазнали суттєвих змін, особливо такий метод як фішинг. Фішинг – це зловмисна атака, під час якої шахраї видають себе за достовірні джерела з метою отримання цінної інформації [1]. Фішинг вже довгий час залишається найпоширенішим способом для кіберзлочинців через його простоту реалізації, а використання ШІ вивело цей метод на новий рівень. Завдяки штучному інтелекту атаки на конкретні цілі стали не тільки ефективнішими, але й менш помітними. Метою цієї роботи є дослідити механізми використання штучного інтелекту для автоматизації фішингових атак та оцінити ефективність сучасних ШІ у виявленні аномальних кіберзагроз.

Результати дослідження

Однією з ключових особливостей використання штучного інтелекту в сучасному фішингу є повна автоматизація атак. Раніше для проведення якісних фішингових кампаній потребувались значні людські ресурси, що робило процес фінансово затратним та повільним. З приходом ШІ цей процес пришвидшився в декілька разів, що надає зловмисникам можливості проводити масштабні операції з мінімальними витратами та зусиллями. Сьогодні хакери використовують спеціалізовані моделі, такі як WormGPT, що орієнтовані на створення переконливих фішингових листів без етичних обмежень, та FraudGPT, що дозволяє генерувати цілі шахрайські інфраструктури, включаючи підроблені платіжні системи та шкідливий код [2, 3]. Зараз штучний інтелект вміє не лише генерувати текст для спам-листів, але й здатен створювати фішингові вебсайти, які виглядають природньо та правдоподібно навіть для досвідченого користувача. Фішинговий сайт – це шахрайський вебресурс, який видає себе за офіційний онлайн-сервіс і використовується для отримання доступу до персональних або фінансових даних користувачів [4]. Основна мета такого ресурсу – змусити особу повірити, що вона перебуває на справжньому сайті, та

спонукати її до введення своєї конфіденційної інформації. Для досягнення кращого результату зловмисники застосовують такі інструменти як EvilGPT, що допомагають обійти спам-фільтри. Окрім того, ШІ автоматизує пошук та реєстрацію доменних імен з помилками (тайпсквотинг), написання яких дуже схоже на написання офіційних та правдивих сторінок. Це дозволяє надсилати листи через легітимні системи, де користувач може не помітити зайву літеру або розширення .org замість .com у домені [5]. Реальні приклади можуть підтвердити критичну небезпеку ШІ атак. Наприклад, у 2024 році світ сколихнула новина про масштабне шахрайство в Гонконзі, де зловмисники за допомогою ШІ-дипфейків відтворили образи керівництва компанії під час відеоконференції, що змусило співробітника переказати 25 мільйонів доларів на рахунки хакерів [6].

Проте штучний інтелект виступає не лише інструментом нападу, а й ключовим елементом сучасного захисту, здатним виявляти приховані аномалії та блокувати загрози ще на етапі їх виникнення. Організації активно використовують системи Cyber AI, такі як Darktrace, для моніторингу мережевої активності та виявлення відхилень у поведінці користувачів – від нетипових спроб авторизації до підозрілої маршрутизації вхідної пошти [7]. Платформи такі як Abnormal Security аналізують соціальний граф компанії, блокуючи шкідливі повідомлення ще до моменту взаємодії з адресатом, що дає змогу виявити високоякісні підробки, які за грамотністю майже не відрізняються від справжніх звернень [8]. Кіберзагрози постійно еволюціонують, тому недостатньо покладатися виключно на технологічні засоби. Важливо, щоб кожен співробітник розумів, як уникати фішингу та соціальної інженерії. Компанії повинні регулярно проводити тренінги, використовуючи інструменти адаптивної симуляції атак, на кшталт KnowBe4. Подібні платформи використовують ШІ для створення індивідуальних сценаріїв перевірки працівників, базуючись на їхніх попередніх діях, що допомагає персоналу на практиці навчитися розпізнавати реальні загрози [9].

Висновки

Використання штучного інтелекту в фішингових атаках призвело до трансформації кіберзагроз, зробивши їх масовими, автоматизованими та надзвичайно переконливими для користувачів. Спеціалізовані інструменти, такі як WormGPT та FraudGPT, а також використання дипфейків і автоматизованого тайпсквотингу, дозволяють зловмисникам обходити звичайні методи перевірки. В той же час штучний інтелект стає основою сучасного захисту, забезпечуючи захист через моніторинг аномалій та аналіз контексту комунікацій. Хоча ШІ і допомагає автоматизувати захист, але людський фактор залишається ключовою ланкою безпеки. Адаптивні тренінги та симуляції дозволяє мінімізувати ризики соціальної інженерії.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Фішинг – що це таке? *Fenix Industry*. URL: https://fnx.com.ua/ua/articles/publications/25 (дата звертання 08.03.2026).
2. WormGPT: The New Bait in Phishing and BEC Attacks. *blackpoint*. URL: https://blackpointcyber.com/blog/wormgpt-new-bait-phishing-bec-attacks/ (дата звернення: 08.03.2026).
3. FraudGPT: The Villain Avatar of ChatGPT. *Netenrich*. URL: https://netenrich.com/blog/fraudgpt-the-villain-avatar-of-chatgpt (дата звернення: 08.03.2026).
4. Фішингові сайти: як розпізнати загрозу та захистити свої платежі. *PROIT*. URL: https://proit.ua/fishinghovi-saiti-iak-rozpiznati-zaghrozu-ta-zakhistiti-svoyi-platiezhi/ (дата звернення: 08.03.2026).
5. The cyber threat of Typosquatting and how to strengthen your online security. *MasterBase*. URL: https://masterbase.com/en/the-cyber-threat-of-typosquatting-and-how-to-strengthen-your-online-security/masterbase/ (дата звернення: 08.03.2026).
6. British engineering giant Arup revealed as $25 million deepfake scam victim. *CNN*. URL: https://edition.cnn.com/2024/05/16/tech/arup-deepfake-scam-loss-hong-kong-intl-hnk (дата звернення: 08.03.2026).
7. Darktrace Launches Enterprise Immune System Version 4. *DarkTrace*. URL: https://www.darktrace.com/news/darktrace-launches-enterprise-immune-system-version-4 (дата звернення: 08.03.2026).
8. Abnormal Security Product Privacy Guide. *Abnormal*. URL: https://files.abnormalsecurity.com/production/files/Abnormal_Security_Product-Privacy-Guide_v3.pdf?dm=1697492767 (дата звернення: 08.03.2026).
9. 2025 Phishing By Industry Benchmarking Report. *Knowbe4*. URL: https://www.knowbe4.com/resources/reports/phishing-by-industry-benchmarking-report (дата звернення: 08.03.2026).

Садовник Євгеній Анатолійович – студент групи 1БС-24б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, email: sadovnikevgenii@gmail.com

Кирилащук Тетяна Геннадіївна – доцент кафедри захисту інформації, Вінницький національний технічний університет, Вінниця, email: tan099838@vntu.edu.ua

Sadovnyk Yevhenii A. – student of 1BS-24b group, Faculty of Information Technology and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email: sadovnikevgenii@gmail.com

Kyrylaschuk Tetiana G. – Associate Professor, Department of Information Security, Vinnytsia National Technical University, Vinnytsia, email: tan099838@vntu.edu.ua