Міністерство освіти і науки України

Харківський національний університет радіоелектроніки

Кафедра комп'ютерно-інтегрованих технологій, автоматизації, робототехніки та безпекової інженерії

I Всеукраїнська конференція «Інтелектуальні технології цивільної безпеки та робототехнічні системи аварійно-рятувальних робіт»

I All-Ukrainian Conference “Intelligent Civil Safety Technologies and Robotic Systems for Emergency and Rescue Operations”

ICSTRO

2026

I All-Ukrainian Conference

February 12 - 13, 2026

Kharkiv

УДК: 005:004.896:62-65:338.3

Інтелектуальні технології цивільної безпеки та робототехнічні системи аварійно-рятувальних робіт 2026: матеріали І-ої Всеукраїнська конференція, Харків, 12-13 лютого 2026 р.: тези доповідей / [редкол. І.Ш. Невлюдов (відповідальний редактор)].-Харків: [електронний друк], 2026. – 192 с.

У збірник включені тези доповідей, які присвячені сучасним тенденціям розвитку технологій та засобів моделювання, прогнозування та управління ризиками у сфері цивільної безпеки; техногенна та виробнича безпека: технічні засоби, оцінка ризиків, експертиза; інтелектуальні та робототехнічні системи аварійно-рятувальних робіт; кіберфізичні системи, інформаційна безпека та цифровий захист виробництв; інформаційно-комунікаційні технології в системах управління та моніторингу надзвичайних ситуацій; сталий розвиток, екологічна безпека та соціальна відповідальність у сфері цивільної безпеки; інтелектуальні системи прийняття рішень у сфері цивільного захисту.

Intelligent Civil Safety Technologies and Robotic Systems for Emergency and Rescue Operations 2026: Proceedings of I st All-Ukrainian Conference, Kharkiv, February 12 - 13, 2026: Thesises of Reports / [Ed. I.Sh. Nevlyudov (chief editor).] .- Kharkiv .: [electronic version], 2026. - 192 p.

The collection includes the thesises of reports on devoted to current trends in the development of technologies and tools for modeling, forecasting, and risk management in the field of civil safety; industrial and technological safety, including technical means, risk assessment, and expert evaluation; intelligent and robotic systems for emergency and rescue operations; cyber-physical systems, information security, and digital protection of industrial facilities; information and communication technologies in emergency management and monitoring systems; sustainable development, environmental safety, and social responsibility in the field of civil safety; and intelligent decision-support systems in civil protection.

Харківський національний університет радіоелектроніки
Кременчуцький національний університет імені Михайла Остроградського
Національний університет «Запорізька політехніка»
Національний університет «Львівська політехніка»
Державне підприємство «Південний державний проектно-конструкторський та науково-дослідний інститут авіаційної промисловості»
Головне управління ДСНС України у Харківській області

Всеукраїнська конференція «Інтелектуальні технології цивільної безпеки та робототехнічні системи аварійно-рятувальних робіт» (ICSTRO-2026)

All-Ukrainian Conference “Intelligent Civil Safety Technologies and Robotic Systems for Emergency and Rescue Operations” (ICSTRO-2026)

ЗМІСТ

ANALYSIS OF THE EFFECTIVENESS AND CYBERSECURITY RISKS OF THE GITHUB COPILOT TOOL

I. Dvoinikova, S. Sotnik
Kharkiv National University of Radio Electronics
Ukraine, 61166, Kharkiv, Nauky av., 14
E-mail: indira.dvoinikova@nure.ua

***Annotation*:** The work analyzes the impact of artificial intelligence-based tools, particularly GitHub Copilot, on the modern software development industry. It examines the results of experimental studies that confirm a significant increase in developer productivity (up to 55.8%) and contribute to the democratization of professional skills. Special attention is given to cybersecurity risks: it has been found that generative models, when trained on open repositories, often reproduce vulnerabilities and outdated coding practices. The necessity of transforming the role of the programmer is justified, shifting the focus from writing code to its thorough auditing and prompt engineering, which is critical for the safe realization of the economic potential of AI assistants.

Key words: artificial intelligence, GitHub Copilot, software development, cybersecurity, work productivity.

АНАЛІЗ ЕФЕКТИВНОСТІ ТА РИЗИКІВ КІБЕРБЕЗПЕКИ ІНСТРУМЕНТУ GITHUB COPILOT

І. Є. Двойнікова, С. В. Сотник
Харківський національний університет радіоелектроніки,
Україна, 61166, Харків, пр. Науки 14
E-mail: indira.dvoinikova@nure.ua

***Анотація*:** У роботі проаналізовано вплив інструментів на базі штучного інтелекту, зокрема GitHub Copilot, на сучасну індустрію розробки програмного забезпечення. Розглянуто результати експериментальних досліджень, що підтверджують суттєве зростання продуктивності праці розробників (до 55,8 %) та сприяють демократизації професійних навичок. Особливу увагу приділено ризикам, пов'язаним із кібербезпекою: виявлено, що генеративні моделі, навчаючись на відкритих репозиторіях, часто відтворюють вразливості та застарілі практики кодування. Обґрунтовано необхідність трансформації ролі програміста, де фокус зміщується з написання коду на його ретельний аудит та інженерію запитів, що є критичним для безпечної реалізації економічного потенціалу ШІ-асистентів.

***Ключові слова*:** штучний інтелект, GitHub Copilot, розробка програмного забезпечення, кібербезпека, продуктивність праці.

Artificial intelligence (AI) is rapidly transforming the software development industry, offering tools that promise a revolutionary increase in work efficiency [1-9]. The most well-known representative of this wave is GitHub Copilot (Fig. 1) – an «AI pair programmer» that generates code in real time based on context. However, along with the unprecedented speed of code writing comes new challenges related to the security and quality of software products. The implementation of such tools fundamentally changes the workflow: from impressive productivity metrics to hidden risks that require programmers to adopt a new mindset and constant vigilance. This transformation is part of a broader trend of development automation, which is evolving alongside AI, gradually delegating not only routine tasks but also increasingly complex intellectual ones [10-15].

The aim of this work is a comprehensive analysis of the effectiveness of GitHub Copilot in terms of improving developer productivity and assessing the associated cybersecurity risks arising from the use of generative AI.

Studies involving developers [16, 17] demonstrate the impressive impact of AI on work speed. In a controlled experiment where participants were tasked with creating an HTTP server in JavaScript, the group using GitHub Copilot completed the task 55,8 % faster than the control group working without AI assistance. This result is not only statistically but also practically significant, indicating a tremendous potential for time savings in the industry.

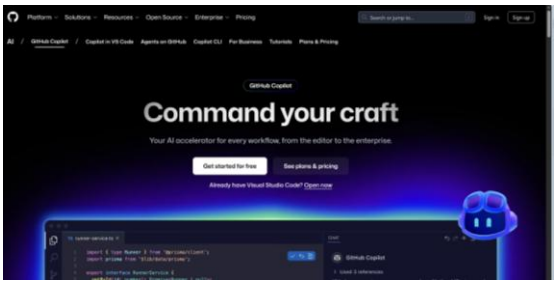

Figure 1 – GitHub Copilot Start Page

Artificial intelligence acts as a kind of «leveler» of professional skills. Analysis showed that the greatest benefit from using assistants is gained by developers with less programming experience, older specialists, and those who spend many hours a day coding. This indicates that AI tools can help lower the barrier to entry into the profession and support career transitions. Notably, developers themselves tend to underestimate the impact of the technology on their performance: participants in the experiment subjectively estimated their productivity increase at an average of 35 %, while actual metrics exceeded 55 % [17].

Despite the obvious advantages in speed, the quality of generated code from a cybersecurity perspective raises serious concerns. Since large language models, such as Codex (which powers Copilot), are trained on massive datasets of open-source code from GitHub, they pick up not only effective solutions but also bugs, vulnerabilities, and bad practices present in public repositories.

Systematic security research has revealed alarming statistics: in high-risk scenarios (from the MITRE Top 25 Common Weakness Enumeration), approximately 40 % of the code suggestions made by Copilot contained vulnerabilities.

Among the most common problems with Copilot were SQL injections, buffer overflow vulnerabilities, and the use of hard-coded credentials. What is particularly dangerous is that the AI often suggests vulnerable code as the «best option» with a high level of confidence, which can mislead less experienced developers. The model also tends to reproduce outdated practices, such as recommending weak hashing algorithms like MD5 simply because they are frequently found in the old code it was trained on.

The widespread adoption of AI assistants is changing the very essence of a programmer's work. The focus is shifting from directly writing code to auditing and reviewing machine suggestions. Researchers emphasize the need to «stay awake at the keyboard», as blind trust in autocomplete carries significant risks.

The ability to correctly formulate context and queries for the system becomes critically important. Experiments have shown that even minor, semantically insignificant changes in comments can drastically affect the safety of the output. For example, a simple replacement of the word «remove» with «delete» in a comment, or adding false labels indicating that a vulnerability has been fixed, sometimes prompted the AI to generate even more dangerous code. Additionally, the AI's effectiveness heavily depends on the popularity of the programming language. While Copilot performs well with Python or JavaScript, in specialized areas such as hardware description using Verilog, it often generates syntactically incorrect or functionally flawed code due to a smaller volume of training data.

The transformation of the workflow requires developers to develop new competencies and critical thinking skills. The traditional model of learning programming, which focused on memorizing syntax and writing each line of code independently, is giving way to a new paradigm in which the programmer acts as both an architect and a reviewer. This involves a deep understanding of secure coding principles, the ability to quickly identify potential vulnerabilities, and the skill to communicate effectively with AI systems through comments and context. Paradoxically, to work productively with an AI assistant, a developer needs an even higher level of

expertise than in traditional programming, as they must critically evaluate every suggestion made by the machine.

The changes also affect teamwork and code review processes. AI-generated code often looks syntactically flawless and adheres to commonly accepted style conventions, which can create a misleading sense of quality during peer reviews. Development teams need to adapt their quality control processes, paying attention not only to logic and functionality but also to hidden security vulnerabilities that AI may have subtly integrated into the code. This requires the implementation of additional static analysis tools and automated security testing as a mandatory part of the development pipeline.

Tools like GitHub Copilot have significant economic potential. Extrapolating the observed productivity growth to the level of a national economy (for example, the U.S., where developers generate about 2 % of GDP) suggests enormous cost savings and a positive impact on GDP. Users also highly value such tools: those who had the opportunity to work with Copilot expressed a willingness to pay a much higher monthly price for it compared to those who only saw a demo version. However, to safely realize this potential, the industry needs new approaches to training developers and improving the models themselves in order to minimize the risk of replicating past mistakes.

Analysis of the GitHub Copilot tool demonstrates its controversial and transformational role in modern software development. On the one hand, the AI assistant has proven its ability to be a powerful catalyst for productivity; on the other hand, it has turned out to be a source of systemic cybersecurity risks. The main challenge of GitHub Copilot is the inherent tendency of generative models to reproduce vulnerabilities. The fact that approximately 40 % of code suggestions in high-risk scenarios contain flaws from the MITRE CWE Top 25 list (such as SQL injections, buffer overflows, and the use of weak encryption algorithms) transforms the AI assistant from a helper into a potential vector for the mass distribution of dangerous practices. Particularly dangerous is the psychological aspect – the system's high confidence in its suggestions, which can mislead even experienced developers. To safely realize the potential of GitHub Copilot, systemic changes are necessary: at the developer level – constant vigilance, i.e., developing skills for critical analysis of generated code and formulating effective contextual prompts; at the team level – adapting code review processes to focus on searching for hidden vulnerabilities, not just syntactic errors. The integration of specialized static and dynamic application security testing (SAST/DAST) tools into Continuous Integration / Continuous Delivery (CI/CD) pipelines is mandatory. The economic efficiency lies in GitHub Copilot's ability to increase the speed of developers' task completion, which opens economic potential for the industry. The tool acts as a «social leveler», providing the greatest value to developers with less experience, thereby lowering barriers to entry into the profession and promoting career mobility.

Thus, GitHub Copilot is not a panacea, but rather a powerful yet double-edged tool. Its economic benefits can only be fully realized by overcoming cybersecurity risks through improving developers' skills, enhancing the models themselves, and deeply transforming software development culture. The future belongs not to those who write code faster, but to those who can most effectively manage and control its creation by artificial intelligence.

REFERENCES

1. Nevludov, I. Sh. & et al. Application of artificial intelligence in additive manufacturing (3D printing). Information Technologies and Automation – 2025 / Proceedings of the XVIII International Scientific and Practical Conference. Odessa, October 30-31, 2025. – Odessa, ONUT Publishing House, 2025. PP. 1006-1009.

2. Marunich, R.V. & et al.. Features of IoT application in the security sector. «Computer-integrated technologies, automation and robotics» CITAR-2025, 2025. PP. 80-84.

3. Sotnik, S. & et al.. Evaluating relational database scaling strategies in web engineering. International Conference on Advanced Trends In Radioelectronics and Infocommunications (ATRIC-2025) (May 21–22, 2025), Lviv Polytechnic Publishing House, Lviv, Ukraine, 2025. PP. 224-228.

4. Marunich, R.V., Sotnik, S.V. Modern IoT technologies for creating automated access systems. Sustainable smart cities and communities: business and innovation solutions 2025: Proceedings of I st I International Conference, Kharkiv, April 21, 2025: Thesises of Reports, 2025. PP. 38-39.

5. Yechevskyi, A., & et al.. Analysis of the data collection process about products at different stages of production. Manufacturing & Mechatronic Systems 2025: Proceedings of IX st International Conference, Kharkiv, October 25-26, 2025: Thesises of Reports, 2025. PP. 38-41.

6. Levenets, I. O. & et al. The role of artificial intelligence in optimizing information retrieval systems. Information Technologies and Automation – 2025 / Proceedings of the XVIII International Scientific and Practical Conference. Odessa, October 30-31, 2025. – Odessa, ONUT Publishing House, 2025. PP. 975-977.

7. Rudenko, M. & et al. Overview of approaches to scaling relational databases in development and adaptation of web applications. Сучасні проблеми і досягнення в галузі радіотехніки, телекомунікацій та інформаційних технологій: Тези доповідей XII Міжнародної науково-практичної конференції (10-12 грудня 2024 р., м. Запоріжжя). [Електронний ресурс] /Електрон. дані. – Запоріжжя: НУ «Запорізька політехніка», 2024. PP. 398-402.

8. Khalimonov, Y. I. & et al. Integration of IoT into security systems: opportunities and risks. Комп'ютерно-інтегровані технології автоматизації технологічних процесів на транспорті та у виробництві : матеріали всеукр. наук.-практ. конф. здобувачів вищ. освіти і молодих учених, 20 листоп. 2024 р., 2024. PP. 117-121.

9. Sotnik, S. V. & et al.. Analysis of collecting data process on products at different stages of production. Стан, досягнення та перспективи інформаційних систем і технологій / Матеріали XXIV Всеукраїнської науково-технічної конференції молодих вчених, аспірантів та студентів. Одеса, 18-19 квітня 2024 р. - Одеса, Видавництво ОНТУ, 2024 р., 2024. PP. 84-86.

10. Achkan, M. S. & et al.. Integration of cloud technologies into modern SCADA systems: prospects and challenges. «Computer-integrated technologies, automation and robotics» CITAR-2025, 2025. PP. 26-29.

11. Konieva, A. & et al.. Main trends in the development of automated image processing systems. «Computer-integrated technologies, automation and robotics» CITAR-2025, 2025. PP. 68-72

12. Shrubkovskyi, Y. V. & et al.. Development of a structural scheme for automatic dosing of liquid components. Період трансформаційних процесів в світовій науці: задачі та виклики: збірник наукових праць з матеріалами V Міжнародної наукової конференції, м. Кропивницький, 6 червня, 2025 р. / Міжнародний центр наукових досліджень. – Вінниця: ТОВ «УКРЛОГОС Груп, 2025. PP. 242-246.

13. Sotnik S. V. Analysis of Personal Information Security Issues in Peacetime and Wartime. International Journal of Academic Engineering Research (IJAER), 2024, PP. 108-113.

14. Hubar, A.Y., Sotnik, S.V. Impact of automation and CALS technologies on human factor in production. The 5th International scientific and practical conference "Perspectives of contemporary science: theory and practice" (June 24-26, 2024) SPC "Sci?conf.com.ua", Lviv, Ukraine, 2024. PP. 243-249.

15. Tverdokhlib, A., Sotnik, S. Intelligent tools for optimizing information and search engines. Manufacturing & Mechatronic Systems 2024: Proceedings of VIII st International Conference, Kharkiv, October 25-26, 2024, PP. 28-31.

16. Pearce, H. & et al.. Asleep at the keyboard? assessing the security of github copilot's code contributions. Communications of the ACM, 2025. PP 96-105.

17. Peng, S., Kalliamvakou, E., Cihon, P., Demirer, M. The impact of ai on developer productivity: Evidence from github copilot. arXiv preprint arXiv:2302.06590, 2023. PP.1-19. Article ID arXiv.2302.06590, https://doi.org/10.48550/arXiv.2302.06590.