

## ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В ПРОЦЕСІ РОЗВИТКУ ЦИФРОВОЇ КОМПЕТЕНТНОСТІ З ІНФОРМАЦІЙНОЇ БЕЗПЕКИ МАЙБУТНІХ УЧИТЕЛІВ ІНФОРМАТИКИ

**Анотація.** У статті розглядається використання штучного інтелекту для забезпечення інформаційної безпеки вчителями інформатики. Актуальність статті зумовлена широким поширенням застосування штучного інтелекту та затребуваністю використання актуальних та інноваційних ресурсів з інформаційної безпеки у процесі підготовки майбутніх учителів інформатики, що дасть можливість покращити рівень їхніх знань у цій галузі, а також ефективніше протидіяти загрозам інформаційної безпеки. Метою написання статті є дослідження можливостей застосування штучного інтелекту в процесі розвитку цифрової компетентності з інформаційної безпеки майбутніх учителів інформатики. Автор досліджує, які переваги та недоліки може мати використання ШІ в процесі розвитку цифрової компетентності з інформаційної безпеки майбутніх учителів інформатики. Серед основних переваг: використання чат-ботів для отримання певної інформації чи інструкцій, застосування ШІ для виявлення фішингу та інтернет шахрайств, використання спеціалізованих інструментів з застосуванням ШІ для автоматизації процесу сканування вразливостей шкільної мережі. Серед недоліків автор виділяє галюцинацію ШІ, зниження рівня критичного мислення у користувачів та збирання персональних даних. У статті описано реальні приклади використання штучного інтелекту в процесі розвитку цифрової компетентності з інформаційної безпеки майбутніх учителів інформатики. Автор також аналізує поняття “цифрова компетентність”, її складники в контексті підготовки майбутніх учителів інформатики, а також освітні програми спеціальності А4.09 “Середня освіта (Інформатика)” українських ЗВО щодо наявності відповідних компетенцій. Перспективами подальшого дослідження вбачаємо аналіз можливостей штучного інтелекту у процесі вивчення методів соціальної інженерії, а також можливості інтеграції інструментів ШІ в процесі розвитку цифрової компетентності з інформаційної безпеки майбутніх учителів інформатики.

**Ключові слова:** штучний інтелект, інформаційна безпека, штучний інтелект в інформаційній безпеці, цифрова компетентність, складники цифрової компетентності.

**Introduction.** The rapid development of artificial intelligence (AI) in recent years has significantly improved the lives of ordinary people. Not so long ago, the use of AI technologies was limited or almost inaccessible to ordinary users, but now this has changed dramatically. Its popularity has skyrocketed thanks to the emergence of powerful language models, including GPT-3, GPT-4o and DeepSeek, and its popularity is growing rapidly due to accessibility: now everyone can use chatbots, image generators, automatic text translators and other smart tools for free and from any device, be it a computer, smartphone or smartwatch. Today, technologies using artificial intelligence are widely used in various fields: from healthcare to the educational process. The information security industry is no exception. In the process of developing digital competence in information security of future computer science teachers, AI can be used in a variety of ways, from chatbots to special tools using artificial intelligence to perform certain activities. As O. Spirin and V. Oleksiuk note: “In the future, a modern teacher should be able to select AI systems to support learning at school and university” [19].

The relevance of the article is driven by the widespread adoption of artificial intelligence and the growing demand for up-to-date and innovative information security resources in the training of future computer science teachers. This approach will help enhance their knowledge in this field and strengthen their ability to effectively counter information security threats.

**Analysis of recent research and publications.** The digital competence of future computer science teachers has been studied by such Ukrainian scholars as V. Bykov, O. Ovcharuk, O. Spirin, L. Potapiuk, V. Oleksiuk, H. Henseruk, O. Pinchuk, N. Morze, and others. There is no such clear

interpretation of the concept of digital competence, which is used by most scientists. O. Spirin and O. Ovcharuk interpret it as the ability of an individual to confidently and thoroughly use digital technologies in such areas as professional activity and employment, education, leisure, and social activities, which are vital for participation in daily socio-economic life [18]. L. Potapyuk and I. Potapyuk note that: "Digital competence is the ability to use digital media and ICT, to understand and critically evaluate various aspects of digital media and media content, and to be able to communicate effectively in various contexts" [17]. Finnish scientists L. Ilomäki, A. Kantosalo and M. Lakkala claim that digital competence is based on basic ICT skills, that is, the use of computers to receive, evaluate, store, create, present and exchange information, as well as to communicate and participate in shared networks via the Internet. However, it includes not only digital skills, but also social and emotional aspects of using and understanding digital devices" [5].

Based on the analysis of the works of domestic and foreign scientists, it can be concluded that digital competence – is a system of certain skills and abilities in using digital technologies, without which life in a modern digital society would be very difficult and dangerous, as it also forms the ability to responsibly and safely interact with information technologies and other users, critically evaluate digital content, and ensure the protection of one's own data in the online environment.

When it comes to the digital competence of future computer science teachers, the rapid development of digital technologies requires them to be able to adapt accordingly and master the necessary digital tools to perform educational and professional tasks. In the current era, it is not enough to own only certain individual applications and services, there is a need to be able to use them to organize the learning process, including combining them with each other. This will make the process of learning new knowledge more interesting and will also improve the effectiveness of such learning. "Digital competence combines knowledge and skills to use digital technologies to organize the educational process, to critically evaluate information resources for the appropriateness of their use in future professional activities, and to apply technological innovations," emphasizes H. Henseruk [9]. Digital competence is particularly important for future computer science teachers, as they are responsible for developing relevant digital skills in students. This makes it necessary not only to confidently work with digital tools, but also to be aware of the risks associated with their use, in particular with regard to information security.

Programming is one of the key components of the digital competence of future computer science teachers. Since any digital tool is written using a certain programming language, computer science teachers must know the advantages and disadvantages of the main ones, as well as understand which programming language to use and for what purpose, have the skills to write code using basic languages, and know their syntax. In addition, it is necessary for them to be able to analyze algorithms, their effectiveness, compare different approaches to solving the same problem and choose the optimal solutions. The ability to program is included in almost all educational and professional programs (EPP) of the specialty A4.09 "Secondary Education (Informatics)" at Ukrainian higher education institutions. For example, at the Volodymyr Vynnychenko Central Ukrainian State University, a computer science teacher must have: "the ability to develop, research, and implement algorithms for solving computer science problems in programming languages. The ability to form students' knowledge of the basics of programming and algorithmic thinking" [16]. Also important for future computer science teachers is the ability to understand current programming trends, in particular regarding the development of AI, web programming, mobile application development, and the use of popular frameworks.

The next, no less important, component of the digital competence of a modern computer science teacher is working with operating systems (OS) and computer networks. This constitutes a significant part of the work of these specialists, as they are usually responsible for setting up both their own workplace and the workplaces of students at school. The digital competence component includes understanding the architecture of the OS, knowledge of the principles of file system organization, as well as the skills to perform basic OS administration actions, in particular, creating and managing user accounts, configuring access, installing and updating programs, changing system settings, and creating backups. According to the educational and professional program "Secondary Education

(Informatics)” in specialty A4.09 of Rivne State Humanitarian University, a future computer science teacher must have: “The ability to organize computational processes in information systems, taking into account the architecture, configuration, and functioning of operating systems” [14]. As for computer networks, it is necessary for future computer science teachers to understand their structure, principles of construction and operation. In particular, they should know the differences in the operation of local area networks (LAN), wide area networks (WAN) and wireless networks, know the basic network topologies and methods of their implementation, have a general understanding of the main network protocols, for example, TCP/IP, HTTP, FTP, understand what they are designed for and how they work. According to the educational and professional program “Secondary Education (Informatics, Mathematics, Fundamentals of STEM Education)” in specialty A4.09 of the Ternopil V. Hnatyuk National Pedagogical University, future teachers of computer science must be able to: “set up and administer computer networks, including educational computer networks, determine the methodology for finding an effective technical solution” [15]. It is also important for them to know how network devices work, such as routers, switches, modems, and access points, and to understand how these devices provide interaction between individual network elements.

One of the most relevant components of a computer science teacher's digital competence today is information security. With the increasing integration of technologies into educational institutions, there is a growing need for the ability to ensure the protection of digital information of the participants in the educational process and the educational environment. This is precisely what computer science teachers are responsible for, so it is essential for them to have up-to-date and practical knowledge of information security. Future computer science teachers must have knowledge of various types of threats they and their students may encounter when using digital technologies, including malicious software such as viruses, ransomware, adware and spyware; in addition, they need to possess knowledge of social engineering, its methods and techniques that cybercriminals may employ. Thus, according to the educational and professional program “Secondary Education (Informatics)” in the specialty A4.09 at Lutsk National Technical University, future computer science teachers are required to have: “the ability to implement a set of measures aimed at ensuring information security, and the ability to develop school students’ skills for safe work in a computer network” [13]. and according to the educational and professional program “Secondary Education (Informatics)” in specialty 014.09 of Zaporizhzhia National University, they must be able to: “Ensure information protection and security in local and global networks” [12]. In addition to ensuring their own information security and educational environment, future informatics teachers should also teach their students to effectively recognize dangerous situations in the process of using digital technologies, as well as how to act in order not to become victims of cybercriminals and ensure their own reliable protection in the online environment [11].

**The purpose of the article** is to study the possibilities of using artificial intelligence in the process of developing digital competence in information security of future computer science teachers. The tasks of the article include:

1. Analysis of the advantages of using artificial intelligence in the process of developing digital competence in information security of future computer science teacher;
2. Analysis of the threats of using artificial intelligence in the process of developing digital competence in information security of future computer science teachers;
3. Research into real cases of the application of using artificial intelligence in the process of developing digital competence in information security of future computer science teachers.

**Presentation of the main research material. Advantages of using artificial intelligence in the process of developing digital competence in information security of future computer science teachers.** Using chatbots to obtain certain information is an effective approach to developing digital competence in information security among future computer science teachers. R. Hodhod, S. Wang and S. Khan emphasize that “intelligent systems can play an important role in accelerating the formation of cybersecurity skills by helping teachers develop teaching materials and programs” [4]. Chatbots contribute to the development of this competence by helping to quickly find relevant materials, simulate real dangerous situations, and develop and improve skills in recognizing

vulnerabilities and threats. Their interactivity allows learning at a convenient time and in an accessible format, which contributes to a deeper understanding of current needs in the field of information security.

The use of artificial intelligence can be effective in detecting and preventing phishing and online fraud. Artificial intelligence systems, leveraging large collections of phishing emails and documented fraud schemes, can detect subtle cues that are typically unnoticed by humans but may indicate potential security threats. For instance, artificial intelligence can identify anomalies in email metadata, including atypical sending patterns or inconsistencies between the displayed sender name and the actual email address. As Indian scientist R. Chokkappagari notes: "Over time, artificial intelligence is getting better at learning new phishing techniques, making it the most effective tool in recognizing cybercriminal attacks that are constantly evolving" [2]. AI quite accurately identifies and marks suspicious actions, phishing attempts, and its constant development in this field makes it an indispensable tool now.

Using specialized tools with artificial intelligence can automate the process of scanning school network vulnerabilities, making it easier to fix security flaws. This is very similar to what cybercriminals would do to find vulnerabilities. Through continuous network monitoring, AI can pinpoint vulnerabilities and assign priorities according to their potential effect, facilitating effective issue resolution. Ongoing evaluation allows for real-time oversight of vulnerabilities, narrowing the scope for cybercriminals to exploit system weaknesses. S. Pala, in his article "Study to Develop AI Models for Early Detection of Network Vulnerabilities" notes: "Artificial intelligence models can effectively process large volumes of network traffic data and provide timely notifications of cybersecurity incidents, ensuring rapid response and mitigation measures" [8]. The real advantage here is speed, as AI can find vulnerabilities, assess them, and fix them considerably more quickly than a person is able to perform manually.

**Threats of using artificial intelligence in the process of developing digital competence in information security of future computer science teachers.** With all the advantages of using AI for information security training, it is worth highlighting the threats that this use can cause. Among the main ones are AI hallucination, a decrease in the level of critical thinking, and the collection of personal data. Let's consider them in more detail.

The AI hallucination deserves special attention, especially when it comes to the need to receive truthful and precise information. Hallucination in AI is a phenomenon that emerges when receiving non-specific or vaguely formulated requests, in this case, AI can generate text that at first glance seems logical and plausible, but in reality, it will be untrustworthy or fictional. This phenomenon arises due to the limitations of the model's algorithms, because AI does not work with real knowledge, but with probabilistic models that select the most suitable word chains. AI hallucination significantly affects the reputation of generative models, so developers are actively trying to fix this to make it impossible or at least minimize the likelihood of generating fabricated information. H. Alkaissi and S. McFarlane point out: "To overcome and mitigate artificial hallucinations in chatbots, it is important to ensure that the system is properly trained and tested using a diverse and representative dataset. In addition, the use of hallucination monitoring and detection methods, such as human scoring, can help to address this issue" [1].

Educational materials created using AI hallucinations may contain inaccurate, distorted, or nonexistent information, which creates a risk of forming incorrect knowledge and misunderstandings among the students. This is especially dangerous in the field of information security, where accuracy and reliability are critically important. Therefore, it is necessary to take a critical attitude to the materials generated by AI and check their authenticity using reliable sources.

Another threat of using AI in the process of developing digital competence in information security for future computer science teachers is the reduction of the level of critical thinking, which is a cognitive skill for analyzing and assessing the reliability of information and making informed decisions depending on the situation. An important characteristic of critical thinking is that it includes not only science but also has relevance in daily life. As L. Zhelyazkova notes: "The development of critical thinking is a very important aspect not only in education, but also in everyday life" [10]. The

daily use of technologies that greatly facilitate and speed up the search for necessary information, in particular AI, can lead to its passive consumption. When acquiring new knowledge is reduced to writing prompt and getting results, without analysis and independent research of the topic, with in-depth study of additional information resources or scientific papers on practical applications. Such actions significantly weaken mental activity and negatively affect the level of critical thinking.

In the context of information security, this poses a serious threat to future computer science teachers, because critical thinking is one of the foundations of their pedagogical activity in this field. Since they not only process new information, but also teach students to analyze new data, structure theoretical knowledge, make informed choices, and act effectively in accordance with the emerging situation or threat.

One of the most pressing threats of using AI in the process of developing digital competence in information security is the collection of personal data. D. Lang and J. Pillet emphasize: “Each of us leaves “traces” that constitute a certain amount of collected data, which are most often processed and transmitted without our knowledge” [7]. It is not always obvious what data can be collected, so most AI models have a privacy policy that outlines the data that can be collected. For example, the Chinese DeepSeek model, which gained widespread popularity earlier this year, is not as secure as it seems. As L. Columbus notes: “DeepSeek programs and services collect user data (names, email addresses, queries, passwords) and store them on Chinese servers, were authorities, according to Chinese data laws, can access them” [3].

Future computer science teachers should be aware that, in addition to the data that is listed in the privacy policy, any other data entered or accessed by AI may be stored. And this can later be processed and used for various purposes, from optimizing services, advertising, or even cases of cyber fraud. This is relevant in an educational environment where students, and often teachers, have a limited understanding of what their data is being collected and do not have sufficient skills and knowledge to ensure that it is protected.

**Examples of the use of artificial intelligence in the process of developing digital competence in information security of future computer science teachers.** Let's consider real examples of the use of AI in the process of developing digital competence in information security. First of all, this is the use of chatbots to obtain certain information or instructions. When interacting with them, it is important to be able to formulate clear and specific requests, as the reliability and accuracy of the answers may depend on this. “The quality of prompts significantly influences the efficacy of AI models, with well-structured prompts improving response accuracy from 85% to 98%”, – emphasize N. Kulkarni and P. Tupsakhare [6].

As shown in Figure 1, there was an explicit request for Gemini to write instructions on how to enable two-factor authentication for Gmail. The result is a clear instruction that includes precise steps with an order of action, as well as alternative ones that need to be performed depending on the user's choice. Following the sequence of actions of this instruction will make it possible to complete the necessary task, and its clarity and brevity allows it to be used effectively as a basis for creating educational materials on information security for students in computer science classes.

In Figure 2, we see the list of phishing email checks generated in ChatGPT. It includes checks from the sender to the content, in particular, it checks that the sender's domain is correct, that the email does not contain suspicious links, does not ask for personal information, and does not require the user's immediate action. Modern email services, in particular Gmail, have their own mechanism for detecting phishing in received emails, which bases its work, in particular, on AI, but due to the active development of cyberfraud methods, this does not always help identify it. Therefore, this checklist is one of the effective protection methods, and it can also be used as a basis for educational recommendations for students in computer science classes.

Let's consider another example of the use of AI in the process of developing digital competence in information security for future computer science teachers. This is checking the safety of opening links. A variety of services offer this capability. Consider CheckPhish.ai, a digital service driven by artificial intelligence to detect phishing and fraudulent links and analyze suspicious emails.

Write instructions on how to enable two-factor authentication in Gmail.



To enable two-factor authentication (2FA), also known as 2-Step Verification, for your Gmail account, follow these instructions:

1. **Go to your Google Account Security page:**

- Open your web browser and navigate to: <https://myaccount.google.com/security>
- Sign in with your Gmail address and password if you haven't already.

2. **Find "2-Step Verification":**

- On the "Security" page, scroll down to the "How you sign in to Google" section.
- Look for "2-Step Verification" and click on it.

3. **Get Started:**

- You'll likely see a blue "GET STARTED" button. Click on it.
- You may be prompted to re-enter your Google password for security reasons.

4. **Choose your second step:**

- Google will usually suggest using "Google Prompts" as the primary second step. This sends a notification to your signed-in Android phone or iPhone (with the Gmail app or Google app installed). This is generally the easiest and most secure method.
- **If you want to use Google Prompts:**
  - Make sure the correct phone is listed. If not, you might need to add it or use a different method.
  - Click "CONTINUE".
  - You'll be asked to test it. On your phone, look for the Google prompt and tap "Yes" to confirm it's you.
  - Once confirmed, click "TURN ON" on your computer.
- **If you prefer other options or want backups (recommended):**
  - Below the Google Prompts section, you'll see "Add more second steps to verify it's you."
  - **Backup codes:** Click "Set up" next to "Backup codes." These are one-time codes you can print or save, useful if you lose your phone. Generate them and keep them in a safe place.
  - **Authenticator app:** Click "Set up" next to "Authenticator app." This uses an app like Google Authenticator or Authy to generate time-sensitive codes. Scan the QR code with your authenticator app and enter the code displayed in the app to verify.
  - **Security Key:** (More advanced) If you have a physical security key, you can set this up for the strongest protection.
  - **Voice or text message (SMS):** While available, Google promotes Google Prompts as more secure. If you choose this, you'll enter your phone number, and Google will send a code via SMS to verify.

5. **Turn On 2-Step Verification:**

- After setting up your preferred second steps (at least one is required), click the "TURN ON" button (if you haven't already done so after testing Google Prompts).

**Important Notes:**

- **App Passwords:** If you use older email clients (like Microsoft Outlook, Mozilla Thunderbird)

Запитайте Gemini



Deep Research



Canvas



Зображення



Fig 1. Instructions for enabling two-factor authentication in Gmail

Write a checklist to verify that an email is not a phishing attempt

Here's a checklist to verify that an email is not a phishing attempt — useful for both personal and professional use:

### ✓ Email Phishing Verification Checklist

#### 1. Sender Verification

- ☐ Is the sender's email address correct and familiar?
- ☐ Does the domain match the organization it claims to be from (e.g., @paypal.com, not @paypal.com)?
- ☐ Hovered over the sender's address to check for mismatched or suspicious domains?

#### 2. Salutation and Language

- ☐ Does the email use your real name instead of generic terms like "Dear user" or "Valued customer"?
- ☐ Is the language free of grammar mistakes, odd phrasing, or urgency ("Act now!", "You must click immediately!")?
- ☐ Does the tone match past communications from this sender?

#### 3. Links and Attachments

- ☐ Hovered over all links — do the URLs match the expected destinations (e.g., <https://www.apple.com> and not <http://apple-login.security-alert.biz>)?
- ☐ Are you expecting any attachments? If not, **don't open** them.
- ☐ Do the links lead to secure (https://) and official websites?

#### 4. Request Content

- ☐ Is the email asking for personal info, passwords, or financial details? Legitimate companies **never** do this via email.
- ☐ Is there a sense of urgency or threat (e.g., "Your account will be suspended in 24 hours")?
- ☐ Are you being asked to bypass normal procedures (e.g., use a personal email or click on a form)?

#### 5. Visual Clues

- ☐ Are the branding, logo, and design consistent with the real organization's usual format?
- ☐ Are there any misspelled brand names or low-quality graphics?
- ☐ Is the footer complete with contact info and company details?

#### 6. Technical Check (Optional but Recommended)

- ☐ Checked the email header for SPF, DKIM, or DMARC pass (available in most email clients)?
- ☐ Reported or flagged the email in your system if suspicious?
- ☐ Consulted IT or a security team if unsure?



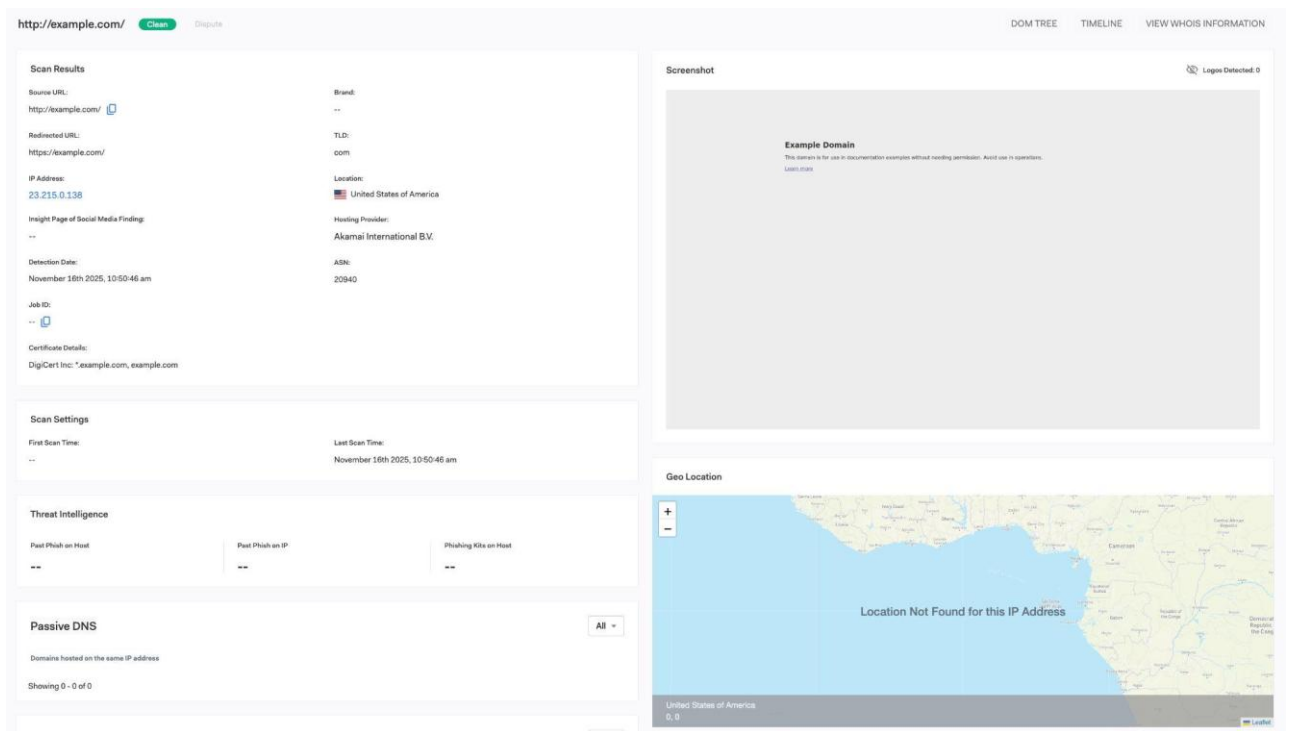
Ask anything

+ Tools



ChatGPT can make mistakes. Check important info.

Fig. 2. Checklist for checking a received email for phishing content



*Fig. 3. Checking a link for safety using CheckPhish.ai*

Figure 3 shows the result of this online service, which contains information about the site's SSL certificates, hosting details, a screenshot of the display, and an assessment of whether the link is malicious. If the link is dangerous, this service determines the type of threat, for example, whether it is phishing, malware, another type of fraud, etc. This tool also analyzes page content, domain structure, logos, and other signs of threats, and the use of AI and improvements through machine learning enables it to detect new types of threats.

**Conclusions.** The development of AI and its capabilities make it an indispensable tool in people's modern lives. The prevalence and popularity of its use have increased significantly recently, which is due to its accessibility and the fact that AI is increasingly associated with increased efficiency and progress. Its uses are diverse, from individual use in everyday life to large-scale implementation in business, education, and medicine. AI also plays an important role in the information security industry.

The use of artificial intelligence has gained significant application in the process of developing various digital competencies of future computer science teachers, in particular, in programming, configuring operating systems and computer networks, or ensuring information security. The use of AI for the development of digital competence in information security of future computer science teachers has both advantages and certain disadvantages. On the one hand, AI makes it possible to quickly obtain the necessary information and instructions, effectively identify and prevent social engineering methods, such as phishing, and conduct automated scans of network vulnerabilities. On the other hand, the use of AI also has disadvantages, such as hallucination, deterioration of the level of critical thinking in those who use it, and problems with the collection of personal data. It is also important that AI technologies can be used by cybercriminals to develop more advanced and potent cyber threats.

As artificial intelligence and attack methods continue to evolve, it is crucial for computer science teachers, school staff, and students to stay informed about new threats and realize that one cannot rely on unconditional trust or mechanically use AI without analyzing the information received and applying critical thinking.

The prospects for further research lie in analyzing the potential of artificial intelligence in the study of social engineering methods, as well as exploring the possibilities of integrating AI tools into the process of developing digital competence in information security of future computer science teachers.

### Список використаних джерел:

- [1] Alkaissi H., McFarlane S. Artificial hallucinations in ChatGPT: implications in scientific writing. Cureus 15.2 (2023). URL: <https://assets.cureus.com/uploads/editorial/pdf/138667/20230219-28928-6kcyip.pdf>
- [2] Chokkappagari R. How AI Detects Phishing Scams. Insights2Techinfo, pp.1. 2024. URL: <https://insights2techinfo.com/how-ai-detects-phishing-scams/>
- [3] Columbus L. DeepSeek AI's AI Breakthrough: A Bold Innovation or a Serious Data Privacy Risk? LinkedIn, 2025. URL: [https://www.linkedin.com/posts/louiscolumbus\\_is-deepseek-really-sending-data-to-china-activity-7289771690425827331-6sBR](https://www.linkedin.com/posts/louiscolumbus_is-deepseek-really-sending-data-to-china-activity-7289771690425827331-6sBR)
- [4] Hodhod R., Wang S., Khan S. Cybersecurity curriculum development using ai and decision support expert system. International Journal of Computer Theory and Engineering 10.4 (2018): 111. URL: [https://www.researchgate.net/profile/Rania-Hodhod/publication/330320538\\_Cybersecurity\\_Curriculum\\_Development\\_Using\\_AI\\_and\\_Decision\\_Support\\_Expert\\_System/links/5c5dc101a6fdccb608b0be80/Cybersecurity-Curriculum-Development-Using-AI-and-Decision-Support-Expert-System.pdf](https://www.researchgate.net/profile/Rania-Hodhod/publication/330320538_Cybersecurity_Curriculum_Development_Using_AI_and_Decision_Support_Expert_System/links/5c5dc101a6fdccb608b0be80/Cybersecurity-Curriculum-Development-Using-AI-and-Decision-Support-Expert-System.pdf)
- [5] Ilomäki L., Kantosalo A., Lakkala M. "What is digital competence." Linked portal (2011): 1-12. URL: [https://digitalcompetenceforum.wordpress.com/wp-content/uploads/2011/05/digital\\_competence\\_definition1.pdf](https://digitalcompetenceforum.wordpress.com/wp-content/uploads/2011/05/digital_competence_definition1.pdf)
- [6] Kulkarni N., Tupsakhare P. Crafting effective prompts: enhancing ai performance through structured input design. Journal of recent trends in computer science and engineering (JRTCSE) 12.5 (2024): 1-10. URL: [https://www.researchgate.net/profile/Preeti-Tupsakhare/publication/385591891\\_Crafting\\_Effective\\_Prompts\\_Enhancing\\_AI\\_Performance\\_through\\_Structured\\_Input\\_Design/links/672bd21edb208342deeced9/Crafting-Effective-Prompts-Enhancing-AI-Performance-through-Structured-Input-Design.pdf](https://www.researchgate.net/profile/Preeti-Tupsakhare/publication/385591891_Crafting_Effective_Prompts_Enhancing_AI_Performance_through_Structured_Input_Design/links/672bd21edb208342deeced9/Crafting-Effective-Prompts-Enhancing-AI-Performance-through-Structured-Input-Design.pdf)
- [7] Lang D., Pillet J. Informing and Communications Technology Threats: Personal Data and User Behaviour. Communications of the IBIMA (2011). URL: <https://pdfs.semanticscholar.org/a2a2/0826ce9f6366fe968f897bede80ebfd6a6b0.pdf>
- [8] Pala S. Study to Develop AI Models for Early Detection of Network Vulnerabilities. International Journal of Enhanced Research in Science, Technology & Engineering ISSN: 2319-7463. URL: [https://www.researchgate.net/profile/Sravan-Pala/publication/380712170\\_Study\\_to\\_Develop\\_AI\\_Models\\_for\\_Early\\_Detection\\_of\\_Network\\_Vulnerabilities/links/664a789a0b0d284574482839/Study-to-Develop-AI-Models-for-Early-Detection-of-Network-Vulnerabilities.pdf](https://www.researchgate.net/profile/Sravan-Pala/publication/380712170_Study_to_Develop_AI_Models_for_Early_Detection_of_Network_Vulnerabilities/links/664a789a0b0d284574482839/Study-to-Develop-AI-Models-for-Early-Detection-of-Network-Vulnerabilities.pdf)
- [9] Генсерук Г. Р. Цифрова компетентність як одна із професійно значущих компетентностей майбутніх учителів. Open educational e-environment of modern University. 2019. № 6. С. 8–14. URL: <https://openedu.kubg.edu.ua/journal/index.php/openedu/article/view/2414-0325.2019.6.816/244>
- [10] Желязкова Л. І. Розвиток критичного мислення в учнів початкової школи в умовах НУШ. Редакційна колегія (2021). URL: [https://elibrary.kdpu.edu.ua/bitstream/123456789/10209/1/Актуальні%20питання\\_Вип\\_7%20%28верстка%29.pdf#page=51](https://elibrary.kdpu.edu.ua/bitstream/123456789/10209/1/Актуальні%20питання_Вип_7%20%28верстка%29.pdf#page=51)
- [11] Олексюк В. П., Олексюк О. Р. Стан сформованості компетентностей з інформаційної безпеки майбутніх учителів інформатики. Інформаційні технології і засоби навчання 62, № 6 (2017): 277-291. URL: <https://journal.iitta.gov.ua/index.php/itlt/article/view/1906/1285>
- [12] Освітньо-професійна програма «Середня освіта (Інформатика)» першого (бакалаврського) рівня вищої освіти за предметною спеціальністю 014.09 Середня освіта (Інформатика), спеціальності 014 Середня освіта. Запорізький національний університет. URL: [https://www.znu.edu.ua/opp/bak/math/opp\\_so-inform\\_23.pdf](https://www.znu.edu.ua/opp/bak/math/opp_so-inform_23.pdf)
- [13] Освітня програма «Середня освіта. Інформатика» першого (бакалаврського) рівня вищої освіти за спеціальністю А4.09 Середня освіта (Інформатика). Луцький національний технічний університет URL: [https://lntu.edu.ua/sites/default/files/2025-05/%21ОП\\_Инф%202025\\_СКАН\\_compressed.pdf](https://lntu.edu.ua/sites/default/files/2025-05/%21ОП_Инф%202025_СКАН_compressed.pdf)
- [14] Освітньо-професійна програма «Середня освіта (Інформатика)» першого (бакалаврського) рівня вищої освіти спеціальності А4 Середня освіта, предметної спеціальності А4.09 Середня освіта (Інформатика). Рівненський державний гуманітарний університет. URL: [https://www.rshu.edu.ua/images/osvitni\\_programi/2025/op\\_2025\\_bak\\_a4\\_09\\_soi.pdf](https://www.rshu.edu.ua/images/osvitni_programi/2025/op_2025_bak_a4_09_soi.pdf)
- [15] Освітньо-професійна програма «Середня освіта (Інформатика, математика, основи STEM-навчання)» першого (бакалаврського) рівня вищої освіти за спеціальністю А4 Середня освіта (за предметними спеціальностями), предметна спеціальність А4.09 Середня освіта (Інформатика). Тернопільський національний педагогічний університет імені В. Гнатюка. URL: [https://tnpu.edu.ua/about/public\\_inform/akredytatsiia%20ta%20litsenzuvannia/osvitni\\_prohramy/bakalavr/fizmat/%D0%904\\_09\\_2025.pdf](https://tnpu.edu.ua/about/public_inform/akredytatsiia%20ta%20litsenzuvannia/osvitni_prohramy/bakalavr/fizmat/%D0%904_09_2025.pdf)
- [16] Освітньо-професійна програма «Інформатика та Робототехніка» першого (бакалаврського) рівня вищої освіти за спеціальністю: А4 Середня освіта (за предметними спеціальностями), предметна спеціальність: Інформатика. Центральноукраїнський державний університет імені Володимира Винниченка URL: [https://cusu.edu.ua/images/download-files/OP\\_quality-education/bakalavr/2025/Informatyka\\_ta\\_Robototekhnika\\_Bakalavr.pdf](https://cusu.edu.ua/images/download-files/OP_quality-education/bakalavr/2025/Informatyka_ta_Robototekhnika_Bakalavr.pdf)
- [17] Потапук Л. М., Потапук І. П. Інформаційно-цифрова компетентність як чинник забезпечення реформування освіти в Україні. (2019). URL: <https://core.ac.uk/download/pdf/214867682.pdf>
- [18] Спірін О. М., Овчарук О. В. Цифрова компетентність. Енциклопедія освіти/ Нац. акад. пед. наук України: 2-ге вид., допов. та перероб. Київ: Юрінком Інтер, 2021. С. 1095-1096. URL:

- [https://lib.iitta.gov.ua/id/eprint/730767/1/Цифрова%20компетентність\\_Овчарук\\_Спірін%20ЕБ.pdf](https://lib.iitta.gov.ua/id/eprint/730767/1/Цифрова%20компетентність_Овчарук_Спірін%20ЕБ.pdf)
- [19] Спірін О. М., Олексюк В. П. Досвід та перспективи використання технологій штучного інтелекту у навчанні майбутніх учителів інформатики. (2023): 63-67. URL: [https://lib.iitta.gov.ua/id/eprint/736338/1/Спірін\\_О.М.%20Олексюк%20В.П.,\\_2023.%20С.63-67.pdf](https://lib.iitta.gov.ua/id/eprint/736338/1/Спірін_О.М.%20Олексюк%20В.П.,_2023.%20С.63-67.pdf)

## THE USE OF ARTIFICIAL INTELLIGENCE IN THE PROCESS OF DEVELOPING DIGITAL COMPETENCE IN INFORMATION SECURITY OF FUTURE COMPUTER SCIENCE TEACHERS

*Bohdan Oliinyk*

**Abstract.** The article examines the use of artificial intelligence to ensure information security by computer science teachers. The relevance of the article is due to the widespread use of artificial intelligence and the need to use relevant and innovative information security resources in the process of training future computer science teachers, which will allow them to increase their level of knowledge in this area, as well as more effectively counteract information security threats. The purpose of the article is to study the possibilities of using artificial intelligence in the process of developing digital competence in information security for future computer science teachers. The author explores the advantages and disadvantages of using AI in the process of developing digital competence in information security of future computer science teachers. Among the main advantages: using chatbots to obtain certain information or instructions, using AI to detect phishing and internet fraud, using specialized tools with AI to automate the process of scanning school network vulnerabilities. The author includes AI hallucination, a decrease in users' critical thinking, and the collection of personal data as the main disadvantages. The article describes real examples of the use of artificial intelligence in the process of developing digital competence in information security of future computer science teachers. The author also analyzes the concept of "digital competence", its components in the context of training future computer science teachers, as well as educational programs of the specialty A4.09 "Secondary Education (Informatics)" of Ukrainian higher education institutions regarding the presence of relevant competencies. We see the prospects for further research as an analysis of the capabilities of artificial intelligence in the process of studying social engineering methods, as well as the possibility of integrating AI tools in the process of developing digital competence in information security of future computer science teachers.

**Keywords:** artificial intelligence, information security, artificial intelligence in information security, digital competence, components of digital competence.

### References (translated and transliterated)

- [1] Alkaissi H., McFarlane S. Artificial hallucinations in ChatGPT: implications in scientific writing. *Cureus* 15.2 (2023). [Online]. Available: <https://assets.cureus.com/uploads/editorial/pdf/138667/20230219-28928-6kcyip.pdf> (in English).
- [2] Chokkappagari R. How AI Detects Phishing Scams. *Insights2Techinfo*, pp.1. 2024. [Online]. Available: <https://insights2techinfo.com/how-ai-detects-phishing-scams/> (in English).
- [3] Columbus L. DeepSeek AI's AI Breakthrough: A Bold Innovation or a Serious Data Privacy Risk? *LinkedIn*, 2025. [Online]. Available: [https://www.linkedin.com/posts/louis-columbus\\_is-deepseek-really-sending-data-to-china-activity-7289771690425827331-6sBR](https://www.linkedin.com/posts/louis-columbus_is-deepseek-really-sending-data-to-china-activity-7289771690425827331-6sBR) (in English).
- [4] Hodhod R., Wang S., Khan S. Cybersecurity curriculum development using ai and decision support expert system. *International Journal of Computer Theory and Engineering* 10.4 (2018): 111. [Online]. Available: [https://www.researchgate.net/profile/Rania-Hodhod/publication/330320538\\_Cybersecurity\\_Curriculum\\_Development\\_Using\\_AI\\_and\\_Decision\\_Support\\_Expert\\_System/links/5c5dc101a6fdccb608b0be80/Cybersecurity-Curriculum-Development-Using-AI-and-Decision-Support-Expert-System.pdf](https://www.researchgate.net/profile/Rania-Hodhod/publication/330320538_Cybersecurity_Curriculum_Development_Using_AI_and_Decision_Support_Expert_System/links/5c5dc101a6fdccb608b0be80/Cybersecurity-Curriculum-Development-Using-AI-and-Decision-Support-Expert-System.pdf) (in English).
- [5] Ilomäki L., Kantosalo A., Lakkala M. "What is digital competence." *Linked portal* (2011): 1-12. [Online]. Available: [https://digitalcompetenceforum.wordpress.com/wp-content/uploads/2011/05/digital\\_competence\\_definition1.pdf](https://digitalcompetenceforum.wordpress.com/wp-content/uploads/2011/05/digital_competence_definition1.pdf) (in English).
- [6] Kulkarni N., Tupsakhare P. Crafting effective prompts: enhancing ai performance through structured input design. *Journal of recent trends in computer science and engineering (JRTCSE)* 12.5 (2024): 1-10. [Online]. Available: [https://www.researchgate.net/profile/Preeti-Tupsakhare/publication/385591891\\_Crafting\\_Effective\\_Prompts\\_Enhancing\\_AI\\_Performance\\_through\\_Structured\\_Input\\_Design/links/672bd21edb208342deeced9/Crafting-Effective-Prompts-Enhancing-AI-Performance-through-Structured-Input-Design.pdf](https://www.researchgate.net/profile/Preeti-Tupsakhare/publication/385591891_Crafting_Effective_Prompts_Enhancing_AI_Performance_through_Structured_Input_Design/links/672bd21edb208342deeced9/Crafting-Effective-Prompts-Enhancing-AI-Performance-through-Structured-Input-Design.pdf) (in English).
- [7] Lang D., Pillet J. Information and Communications Technology Threats: Personal Data and User Behaviour. *Communications of the IBIMA* (2011). [Online]. Available: <https://pdfs.semanticscholar.org/a2a2/0826ce9f6366fe968f897bede80ebfd6a6b0.pdf> (in English).
- [8] Pala S. Study to Develop AI Models for Early Detection of Network Vulnerabilities. *International Journal of*

- Enhanced Research in Science, Technology & Engineering ISSN: 2319-7463. [Online]. Available: [https://www.researchgate.net/profile/Sravan-Pala/publication/380712170\\_Study\\_to\\_Develop\\_AI\\_Models\\_for\\_Early\\_Detection\\_of\\_Network\\_Vulnerabilities/links/664a789a0b0d284574482839/Study-to-Develop-AI-Models-for-Early-Detection-of-Network-Vulnerabilities.pdf](https://www.researchgate.net/profile/Sravan-Pala/publication/380712170_Study_to_Develop_AI_Models_for_Early_Detection_of_Network_Vulnerabilities/links/664a789a0b0d284574482839/Study-to-Develop-AI-Models-for-Early-Detection-of-Network-Vulnerabilities.pdf) (in English).
- [9] Henseruk H. R. Tsyfrova kompetentnist yak odna iz profesiino znachushchykh kompetentnostei maibutnikh uchyteliv [Digital competence as one of the professionally significant competencies of future teachers]. Open educational e-environment of modern University. 2019. № 6. Pp. 8–14. [Online]. Available: <https://openedu.kubg.edu.ua/journal/index.php/openedu/article/view/2414-0325.2019.6.816/244> (in Ukrainian).
  - [10] Zheliazkova, L. I. Rozvytok krytychnoho myslennia v uchniv pochatkovoї shkoly v umovakh NUSH [Development of critical thinking in primary school students in the conditions of the NUS]. Redaktsiina kolehiia (2021). [Online]. Available: [https://elibrary.kdpu.edu.ua/bitstream/123456789/10209/1/Актуальні%20питання\\_Вип\\_7%20%28верстка%29.pdf#page=51](https://elibrary.kdpu.edu.ua/bitstream/123456789/10209/1/Актуальні%20питання_Вип_7%20%28верстка%29.pdf#page=51) (in Ukrainian).
  - [11] Oleksiuk V. P., Oleksiuk O. R. Stan sformovanosti kompetentnostei z informatsiinoi bezpeky maibutnikh uchyteliv informatyky [The state of formation of information security competencies of future computer science teachers]. Informatsiini tekhnolohii i zasoby navchannia 62, № 6 (2017): 277–291. [Online]. Available: <https://journal.iitta.gov.ua/index.php/itlt/article/view/1906/1285> (in Ukrainian).
  - [12] Osvitno-profesiina prohrama «Serednia osvita (Informatyka)» pershoho (bakalavrskoho) rivnia vyshchoi osvity za predmetnoi spetsialnistiu 0.14.09 Serednia osvita (Informatyka), spetsialnosti 014 Serednia osvita [Educational and professional program "Secondary Education (Informatics)" of the first (bachelor's) level of higher education in the subject specialty 0.14.09 Secondary Education (Informatics), specialty 014 Secondary Education]. Zaporizkyi natsionalnyi universytet. [Online]. Available: [https://www.znu.edu.ua/opp/bak/math/opp\\_so-inform\\_23.pdf](https://www.znu.edu.ua/opp/bak/math/opp_so-inform_23.pdf) (in Ukrainian).
  - [13] Osvitnia prohrama «Serednia osvita. Informatyka» pershoho (bakalavrskoho) rivnia vyshchoi osvity za spetsialnistiu A4.09 Serednia osvita (Informatyka) [Educational program "Secondary Education. Informatics" of the first (bachelor's) level of higher education in the specialty A4.09 Secondary Education (Informatics)]. Lutskyi natsionalnyi tekhnichnyi universytet. [Online]. Available: [https://lntu.edu.ua/sites/default/files/2025-05/%21ОП\\_Інф%202025\\_СКАН\\_compressed.pdf](https://lntu.edu.ua/sites/default/files/2025-05/%21ОП_Інф%202025_СКАН_compressed.pdf) (in Ukrainian).
  - [14] Osvitno-profesiina prohrama «Serednia osvita (Informatyka)» pershoho (bakalavrskoho) rivnia vyshchoi osvity spetsialnosti A4 Serednia osvita, predmetnoi spetsialnosti A4.09 Serednia osvita (Informatyka) [Educational and professional program "Secondary Education (Informatics)" of the first (bachelor's) level of higher education, specialty A4 Secondary Education, subject specialty A4.09 Secondary Education (Informatics)]. Rivnenskyi derzhavnyi humanitarnyi universytet. [Online]. Available: [https://www.rshu.edu.ua/images/osvitni\\_programi/2025/op\\_2025\\_bak\\_a4\\_09\\_soi.pdf](https://www.rshu.edu.ua/images/osvitni_programi/2025/op_2025_bak_a4_09_soi.pdf) (in Ukrainian).
  - [15] Osvitno-profesiina prohrama «Serednia osvita (Informatyka, matematyka, osnovy STEM-navchannia)» pershoho (bakalavrskoho) rivnia vyshchoi osvity za spetsialnistiu A4 Serednia osvita (za predmetnymi spetsialnostiamy), predmetna spetsialnist A4.09 Serednia osvita (Informatyka) [Educational and professional program "Secondary education (Informatics, mathematics, fundamentals of STEM education)" of the first (bachelor's) level of higher education in the specialty A4 Secondary education (by subject specialties), subject specialty A4.09 Secondary education (Informatics)]. Ternopilskyi natsionalnyi pedahohichnyi universytet imeni V. Hnatiuka. [Online]. Available: [https://tnpu.edu.ua/about/public\\_inform/akredytatsiia%20ta%20litsenzuvannia/osvitni\\_prohramy/bakalavr/fizmat/%D0%904\\_09\\_2025.pdf](https://tnpu.edu.ua/about/public_inform/akredytatsiia%20ta%20litsenzuvannia/osvitni_prohramy/bakalavr/fizmat/%D0%904_09_2025.pdf) (in Ukrainian).
  - [16] Osvitno-profesiina prohrama «Informatyka ta Robototekhnika» pershoho (bakalavrskoho) rivnia vyshchoi osvity za spetsialnistiu: A4 Serednia osvita (za predmetnymi spetsialnostiamy), predmetna spetsialnist: Informatyka [Educational and professional program "Informatics and Robotics" of the first (bachelor's) level of higher education in the specialty: A4 Secondary education (by subject specialties), subject specialty: Informatics]. Tsentralnoukrainskyi derzhavnyi universytet imeni Volodymyra Vynnychenka. [Online]. Available: [https://cusu.edu.ua/images/download-files/OP\\_quality-education/bakalavr/2025/Informatyka\\_ta\\_Robototekhnika\\_Bakalavr.pdf](https://cusu.edu.ua/images/download-files/OP_quality-education/bakalavr/2025/Informatyka_ta_Robototekhnika_Bakalavr.pdf) (in Ukrainian).
  - [17] Potapiuk L. M., Potapiuk I. P. Informatsiino-tsyfrova kompetentnist yak chynnyk zabezpechennia reformuvannia osvity v Ukraini [Information and digital competence as a factor in ensuring education reform in Ukraine] (2019). [Online]. Available: <https://core.ac.uk/download/pdf/214867682.pdf> (in Ukrainian).
  - [18] Spirin O. M., Ovcharuk O. V. Tsyfrova kompetentnist [Digital competence]. Entsyklopediia osvity / Nats. akad. ped. nauk Ukrainy: 2-he vyd., dopov. ta pererob. Kyiv: Yurinkom Inter, 2021. S. 1095–1096. [Online]. Available: [https://lib.iitta.gov.ua/id/eprint/730767/1/Цифрова%20компетентність\\_Овчарук\\_Спирін%20ЕБ.pdf](https://lib.iitta.gov.ua/id/eprint/730767/1/Цифрова%20компетентність_Овчарук_Спирін%20ЕБ.pdf) (in Ukrainian).
  - [19] Spirin O. M., Oleksiuk V. P. Dosvid ta perspektyvy vykorystannia tekhnolohii shtuchnogo intelektu u navchanni maibutnikh uchyteliv informatyky [Experience and prospects of using artificial intelligence technologies in teaching future computer science teachers]. (2023): 63–67. [Online]. Available: [https://lib.iitta.gov.ua/id/eprint/736338/1/Спирін\\_О.М.%20%20Олексюк%20В.П..\\_2023.%20С.63-67.pdf](https://lib.iitta.gov.ua/id/eprint/736338/1/Спирін_О.М.%20%20Олексюк%20В.П.._2023.%20С.63-67.pdf) (in Ukrainian).