Секція 5

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА КІБЕРБЕЗПЕКА В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ СУСПІЛЬНИХ ВІДНОСИН

UDC 004.89:330.341.1

S.O. Cherepnin, undergraduate *(NTU «KhPI», Kharkiv)*

CORPORATE SECRETS LEAKING DURING USAGE OF CHATGPT

Currently many people use ChatGPT to write essay for school, generate program code, get answer to questions, manipulate data, generate poems, transcript audio files and so on. It becomes very popular over the world and employers also started to use it in workplaces to increase productivity.

According to data from Cyberhaven's product[1], as of April 19, 9.3% of employees have used ChatGPT in the workplace and 7.5% have pasted company data into it since it launched. The numbers are growing, and this situation makes companies worry about risks to confidential data. This is problematic because employees are copying and pasting all kinds of confidential data into ChatGPT to have the tool rewrite it, from source code to patient medical records.

Many companies use security products to protect its data. But it's difficult for security products to monitor usage of ChatGPT and protect data going to it for two reasons:

1. Copy/paste out of a file or app – When workers input company data into ChatGPT, they don't upload a file but rather copy and paste content into their web browser. Many security products are designed around protecting files (which are tagged confidential) from being uploaded but once content is copied out of the file they are unable to keep track of it.

2. Confidential data contains no recognizable pattern – Company data going to ChatGPT often doesn't contain a recognizable pattern that security tools look for, like a credit card number. Without knowing more about its context, security tools today can't tell the difference between someone inputting the cafeteria menu and the company's Mergers and acquisitions plans.

Some companies warn employees not to put confidential data into ChatGPT, some blocks employee access to such tools, some have started seeking out custom generative AI solutions that come with more controls than ChatGPT.

Blocking access is not a sufficient solution since employee can bypass it using proxies, VPNs, Slack or Telegram bots, browser plugins, Edge chat, etc. Also, the variety of such tools is increasing.

The companies should update its corporate policy about AI tools usage, instruct employees about risks and train for possible usage without providing company data.

References:

1. 11% of data employees paste into ChatGPT is confidential. 2023. https://www.cyberhaven.com/blog/4-2-of-workers-have-pasted-company-data-into-chatgpt/

UDC 336.7

A. Koldovskyi, PhD, Senior lecturer *(WSB University, Poland)*, Instructor of international on-line courses at Global Talent International *(USA)*

THE ADVANCEMENT OF DIGITAL CURRENCIES AND ITS IMPLICATIONS, SURPRISING EFFECTS, AND POLICY SUGGESTIONS

Digital currency emerged in the 1980s and 1990s as Electronic Payment and Electronic Currency. Bitcoin marked the beginning of digital currency, bringing it into the public's attention [1]. Currently, the concept and scope of digital currency are still expanding and evolving. Different countries have different types and uses of digital currencies. Sovereign-based currencies issued by central banks are known as Digital Fiat Currency (DFC) or Central Bank Digital Currency (CBDC). On the other hand, private individuals can issue private digital currencies. The theory and