УДК 004.896:004.58
Maksym Teslia[1], Nataliia Zhukova[2]
[1] student of group CST-125 NU "Zaporizhzhia Polytechnic"
[2] PhD (Philology), Associate Professor NU "Zaporizhzhia Polytechnic"

AI AGENTIC WORKFLOW

M.F. Teslia, N.M. Zhukova

Artificial Intelligence (AI) has already become part of our daily lives, and the next step in the AI integration is to embed it into the workflow. Nowadays, there are a few tools that can help you with integrating AI into your work as helpers or secretaries. These helpers are called AI agents because they can perform tasks such as answering, suggesting, predicting, reasoning, and searching for data on their own, with minimal human supervision. This technology is considered a breakthrough because it enables the use of AI in work processes, redistributing human resources to perform complex tasks more efficiently than before.

Objectives of AI agentic workflow:

1. to make workflow more effective compared to the times before AI;
2. to free employees from routine tasks and allow them to apply their skills to more complex tasks;
3. to help make decisions;
4. to optimize the general workflow in the team.

A modern AI agent usually consists of two parts: an LLM (Large language model), which represents a computational model trained on data, and agentic software that helps the LLM perform the actions it wants. This diversion can help make multiple agents on the same base.

In general, an AI agent is an AI-driven system that autonomously performs tasks by designing workflows using available tools [1]. These workflows are designed by LLMs after processing the situation at the moment, so they can adapt to some challenges over time.

AI agents are created using tools such as OpenClaw, LangGraph, CrewAI, etc. The main differences between these tools are how agents are created and how workflows are implemented. For example, OpenClaw does not require much coding to

create an agent, while in LangGraph it is necessary. Also, the first two options support single-agent execution, whereas in CrewAI multiple agents are mandatory, so it may be effective for some tasks but is also more forgetful in general. To run these agents, people buy or rent dedicated computers where they run their assistants in a sandbox environment. The reason behind the sandbox is security concerns. There have been reported incidents [2–4] when AI performed harmful actions due to configuration bugs, software vulnerabilities, etc.

As of now, AI agents' technology is not ready for mass deployment, and their capabilities are not spectacular. Major security concerns in agentic software, centralized AI infrastructure, and the high resource consumption of recent and decent LLMs are not making agents too promising to develop now, but in the near future, they can be effectively combined with other development platforms like OpenAI Codex, Claude Code, Google Antigravity, etc. It can also be used to make predictions and decisions, assist with customer service, and still serve as an assistant or secretary.

REFERENCES

1. Gutowska A. What Are AI Agents? URL : https://www.ibm.com/think/topics/ai-agents/ (Accessed : 20.03.2026).

2. Lakshmanan R. ClawJacked Flaw Lets Malicious Sites Hijack Local OpenClaw AI Agents via WebSocket. URL : https://thehackernews.com/2026/02/clawjacked-flaw-lets-malicious-sites.html/ (Accessed : 20.03.2026).

3. Martindale J. Meta Security Researcher's AI Agent Accidentally Deleted Her Emails. URL : https://www.pcmag.com/news/meta-security-researchers-openclaw-ai-agent-accidentally-deleted-her-emails/ (Accessed : 20.03.2026).

4. Durnas D. Why Trying to Secure OpenClaw is Ridiculous. – aikido. URL : https://www.aikido.dev/blog/why-trying-to-secure-openclaw-is-ridiculous/ (Accessed : 20.03.2026).