Openai said that ChatGPT messages are not confidential and can be provided to government agencies. General Director Sam Altman admitted that correspondence is not legally protected. In addition, in his speech, he emphasized that chat with ChatGPT needs encryption. However, as they say, there is a nuance.

Altman noted that many users discuss personal problems in chats and proposed the concept of AI Privilege, similar to a lawyer secret. Now, temporary chats in ChatGPT are not preserved, but since May of this year Openai is obliged to store all ordinary chats, even remote, by court decision. Full through encryption in the current architecture is impossible, since the model should decipher requests on the side of the company.

For example, Apple partially solved the confidentiality problem using Private Cloud Compute, but for Openai it is more difficult due to the personalization of the service. Altman believes that loud requests from state bodies can change the attitude of users to the issue of confidentiality.