Американское издание ArsTechnica сообщило, что большие языковые модели (Large Language Models, LLM), используемые для генерации программного кода, могут предлагать несуществующие сторонние библиотеки, создавая уязвимости в безопасности за счёт подмены зависимостей.

Недавнее исследование показало, что почти половина примеров кода, сгенерированных популярными LLM, ссылаются на фиктивные библиотеки, причём более 440 тысяч из 576 тысяч проанализированных зависимостей являются фиктивными из-за того, что модели придумывают названия на основе шаблонов, а не реальных данных. Эта проблема «открывает двери» для таких атак, как путаница зависимостей или slopsquatting, когда регистрация пакета с ложным именем может привести к установке вредоносного кода, если разработчики не проверят зависимости должным образом.

Особенно уязвимыми считаются языки Python и JavaScript, где часто встречаются сторонние зависимости, и это представляет серьёзный риск. Также сообщается, что необходимо создавать инструменты безопасности цепочек поставок кода и ПО и переоценки «слепого доверия к рекомендациям по коду, сгенерированным ИИ».