Новые исследования показывают, что так называемые «агентные» ИИ-браузеры, которые сами ищут информацию в интернете и выполняют задачи за пользователя, могут легко попасться на мошеннические сайты. И да, пострадают от этого обычные люди

Компания Guardio протестировала Comet AI, один из таких браузеров. В одном эксперименте ИИ купил Apple Watch на фальшивом сайте, выдававшем себя за Walmart, игнорируя «явные признаки обмана» — странный логотип и адрес сайта. В другом тесте Comet ввёл данные банковского аккаунта на фишинговой странице, замаскированной под письмо от Wells Fargo. Третий тест показал, что ИИ может поддаться на команду с фальшивого сайта скачать файл.

Проблема, как пишут исследователи, в том, что ИИ лишён здравого смысла и выполняет любую команду пользователя. Если человек иногда может заметить мошенничество, ИИ почти всегда будет доверять указаниям.

Это особенно важно сейчас, когда крупные компании активно развивают агентные ИИ-браузеры: Microsoft, OpenAI, Google, Perplexity, у которых в том или ином виде есть планы на этот рынок.