Компания Veracode представила отчёт о безопасности ИИ-кода за 2025 год. Выводы экспертов тревожны.

Почти 45% решений, созданных языковыми моделями на основе 80 программных задач, содержали уязвимости, многие из которых входят в список OWASP Top 10. То есть речь идёт не о мелких ошибках, а о реальных дырах в безопасности.

Особенно печально, что с ростом качества сгенерированного кода, его защищённость не улучшается. Java оказалась самым небезопасным языком — 70% провалов. Python, JavaScript и C# — от 38 до 45%. На задачах вроде XSS и лог-инъекций ИИ «проваливался» в 86–88% случаев.

Отчёт подчёркивает, что ИИ помогает не только разработчикам, но и хакерам: теперь даже новичку достаточно пары запросов, чтобы найти уязвимость и написать эксплойт.

Veracode призывает встраивать проверку безопасности на всех этапах разработки: использовать статический анализ, мониторить зависимости и подключать инструменты автоматического исправления.