

Специалисты Центра практического искусственного интеллекта Сбербанка предложили способ повышения безопасности программного обеспечения с использованием искусственного интеллекта (ИИ). Результаты их исследования опубликованы в научном журнале IEEE Access.

Новый подход позволяет эффективнее выявлять ошибки в коде, которые могут привести к утечке данных или кибератакам. В отличие от традиционных методов анализа, ИИ-модель работает быстрее и точнее. Учёные дообучили нейросеть на специально подготовленных данных, что значительно улучшило её способность находить уязвимости.

Особое внимание исследователи уделили качеству обучающей выборки. Они использовали только те примеры, где наличие уязвимостей было точно подтверждено. Кроме того, оптимизация процесса обучения позволила ускорить его в 13 раз. В результате получилась модель, превосходящая по эффективности существующие аналоги.

Разработка особенно актуальна для компаний с большими кодовыми базами. Она поможет быстрее находить и исправлять ошибки в выпускаемом программном обеспечении, повышая его безопасность. Также метод открывает новые возможности для совершенствования технологий анализа кода.