Contribution ID: **266** Type: **Усна**

ЯК ОБДУРИТИ НЕЙРОННУ МЕРЕЖУ?

Thursday, 25 April 2019 14:55 (15 minutes)

Abstract

За останні декілька десятиліть різко зріс рівень автоматизації у всіх сферах життя. Це призвело до підвищення рівня продуктивності праці, якості продукції і захисту населення. Одним із найбільш прогресивних способів автоматизації є використання машинного навчання. Найчастіше нейромережі використовуються в системах розпізнавання обличь, системах безпеки і системах прийняття рішення. Загалом, нейромережі використовуються там, де необхідно опрацьовувати велику кількість даних. Оскільки, нейромережа використовує алгоритми для узагальнення і аналізу даних, то можливо знайти такі конфігурації вхідних даних при яких навіть натренована нейромережа буде давати збої. Розглянемо найпоширеніші випадки “злому” на прикладі нейромереж розроблених для розпізнавання образів.

Contact Phone

Primary authors: OLIFIROVICH, Mykola; BORETSKIJ, Viacheslav (Taras Shevchenko National University of Kyiv)

Presenter: OLIFIROVICH, Mykola

Session Classification: Загальні питання інформаційної безпеки України

Track Classification: Загальні питання інформаційної безпеки України