2. Бойко І.В., Петрик М.Р., Цуприк Г.Б. Моделювання та видобуток даних (високопродуктивні обчислення у великих та числових системах, комбінаторному аналізі): навчальний посібник. Тернопіль: : ТНТУ 2019 – 62 с.

3. Information System for Design of Thin Multilayer Film Processes Parameters Management based on Diffusion M.R., Petryk, Mykhaylo R., V., Chyzh, Vitalii, H.B., Tsupryk, H. B., O.Y., Petryk, Oksana Yu ITTAP'2024: 4th International Workshop on Information Technologies: Theoretical and Applied Problems, October 23- 25, 2024, Ternopil, Ukraine, Opole, Poland, 2024, pp. 486-493 (https://ceur-ws.org/Vol-3896/)

4. Methods of constructing algorithms for comparative test statistical verification of mathematical models of bioobject responses to low-intensity stimuli / Bohdan Yavorskyy, Evhenia Yavorska, Halyna Tsupryk, Roman Kinash // Scientific Journal of TNTU. — Tern.: TNTU, 2023. — Vol 112. — No 4. — P. 82–90.

УДК 004.8

Р.З. Золотий, к.т.н., доцент, Д.А. Коломийчук
Тернопільський національний технічний університет імені Івана Пулюя

ЕФЕКТИВНІСТЬ АТАК МЕРЕЖ МАШИННОГО НАВЧАННЯ

R. Zolotyi, Ph.D., D. Kolomyichuk
Ternopil Ivan Puluj National Technical University

EFFECTIVENESS OF MACHINE LEARNING NETWORK ATTACKS

Було проведено огляд атак змагального навчання, зосереджений, зокрема, на захисті від атак на класифікатори глибоких нейронних мереж. Після ознайомлення з відповідною термінологією, цілями та діапазоном можливих знань як зловмисників, так і захисників, було розглянуто роботи з ухилення під час тестування (TTE), отруєння даних (DP), бекдор-DP та атак зворотного компілювання (RE), а також, зокрема, захист від них. При цьому розрізняли робустну класифікацію від виявлення аномалій (AD), ненавчений від контрольованого, а також захист на основі статистичних гіпотез від тих, що не мають явної нульової гіпотези (відсутність атаки).

Для побудови ефективного захисту необхідно визначити гіперпараметри, які вимагає певний метод, його обчислювальну складність, а також показники продуктивності, за якими оцінюється якість.

Також можна для аналізу атак застосовувати інноваційні методи: 1) робустна класифікація при визначенні аномалій, як стратегія захисту; 2) переконання, що успіх атаки зростає з силою атаки, яка ігнорує вразливість до аномалій; 3) невеликі збурення для атак ухилення від тестування: помилка чи вимога?; 4) обґрунтованість універсального припущення, що зловмисник TTE знає клас істинності для прикладу, що атакується; 5) атаки чорної, сірої або білої коробки як стандарт для оцінки захисту; 6) вразливість RE на основі запитів до захисту AD. Ми також обговорюємо атаки на конфіденційність навчальних даних.

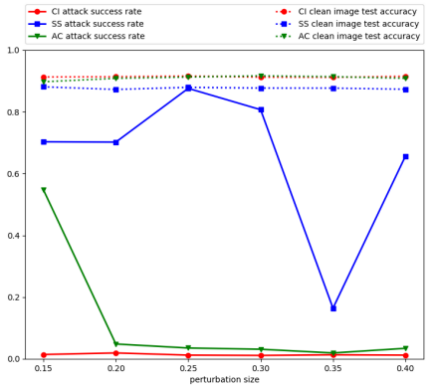

Рисунок 1 - Коефіцієнт успішності та точність атаки на чистому тестовому наборі перенавчених нейронних мереж для трьох захистів

Література.

1. Міллер Д. Дж., Сян Чж., Кесідіс Г. Adversarial Learning in Statistical Classification: A Comprehensive Review of Defenses Against Attacks // Proceedings of the IEEE. 2020. URL: https://arxiv.org/abs/1904.06292.

УДК 004.41

Д.В. Коваль, Г.Б. Цуприк, к.т.н., доц..
Тернопільський національний технічний університет імені Івана Пулюя, Україна

МОДУЛЬНА РЕАЛІЗАЦІЯ ФУНКЦІОНАЛУ ФІНАНСОВОГО КОНТРОЛЮ НА ANDROID ІЗ ЗАСТОСУВАННЯМ ПРИНЦИПІВ ІНВЕРСІЇ УПРАВЛІННЯ ТА ШАБЛОНУ MVVM

D.V. Koval, H.B. Tsupryk, Ph.D., Assoc. Prof.

MODULAR IMPLEMENTATION OF FINANCIAL CONTROL FUNCTIONALITY ON ANDROID USING INVERSION OF CONTROL PRINCIPLES AND THE MVVM PATTERN

Мобільні застосунки для фінансового контролю набули значної популярності серед користувачів, оскільки вони допомагають ефективно управляти особистими фінансами. Такі програми дозволяють стежити за доходами та витратами, створювати бюджети, аналізувати фінансові звіти та досягати фінансових цілей. Однак для забезпечення надійної та ефективної роботи таких застосунків важливо правильно організувати їх внутрішню структуру, щоб забезпечити гнучкість, масштабованість і легкість у підтримці.

Одним з основних підходів до розробки мобільних застосунків є використання модульної архітектури, що передбачає поділ програми на окремі компоненти. Кожен з цих компонентів має свою чітко визначену функцію і може бути розроблений, тестований і оновлений незалежно від інших частин програми. Наприклад, в фінансовому застосунку один модуль може відповідати за облік доходів і витрат, інший — за категоризацію витрат, а ще один — за аналіз бюджету чи формування фінансових цілей.

Такий підхід до структуризації дає можливість працювати з кожною частиною програми окремо, що значно спрощує роботу розробників. Модульність також дає можливість розподіляти завдання між кількома розробниками, зменшуючи час розробки і підвищуючи ефективність роботи над проєктом. Крім того, модульність дозволяє простіше додавати нові функції в застосунок без потреби переписувати вже готовий код, що робить програму більш гнучкою і стійкою до змін.