Верифікація/валідація включає низку функцій для підтримки верифікації і валідації експертних систем, зокрема підтримку модульного проектування і розділення бази знань, статичну і динамічну перевірку обмежень значень слотів та аргументів функцій, а також семантичний аналіз шаблонів правил для можливості визначення, чи можуть невідповідності перешкоджати роботі правилі чи генерувати помилку.

Експертна система, яка є частиною штучного інтелекту, розробляється для вирішення складних проблем за допомогою правил, заснованих на знаннях, замість використання довгих процедурних кодів. Вона працює, застосовуючи визначені правила до бази знань системи за допомогою механізму логічного висновку. Експерт створює базу знань, яка є набором фактів з певних галузей. Далі на основі цієї бази знань і різних запитів користувачів розробляється набір правил. Механізм логічного висновку пов'язує базу знань і набір правил, з якими користувач може взаємодіяти через зручний інтерфейс користувача.

Визначення правил для створення експертної системи зі штучним інтелектом.

Кожне визначене правило може мати набір умов, які ґрунтуються на базі знань експертної системи. Якщо вони виконуються після відповіді користувача на запит, тоді можуть виконуватися певні дії.

Вхідні дані зчитуються користувачем після відповіді на ці запити. Далі ці вхідні дані стверджуються як факти для розширення бази знань експертної системи для подальшого використання.

CLIPS - це проста для розуміння мова програмування, яка працює на базових принципах, але водночас дозволяє створювати глибокі складні системи. Базового синтаксису і гарного розуміння правил і фактів достатньо, щоб почати створювати власні базові експертні системи зі штучним інтелектом.

CLIPS надає багато можливостей для вивчення і використання, зокрема можна інтегрувати з Android для створення експертних системних додатків. Експертні системи також можна використовувати на веб-сайтах для отримання бажаних результатів на основі вподобань користувачів.

У CLIPS можна використовувати безліч різних речей та елементів дизайну. Він дозволяє створювати надійні експертні системи, які можуть імітувати прийняття рішень користувачем.

Отже, CLIPS стає набагато більш життєздатним варіантом для створення експертних систем, ніж використання великих процедурних кодів.

Завдяки своїй портативності, розширюваності, можливостям і відносно низькій вартості, CLIPS отримує широке визнання, зокрема в уряді, промисловості та академічних колах різних провідних країн. CLIPS допомагає покращити можливості впровадження технології експертних систем у державному і приватному секторах для широкого спектру застосувань і різноманітних обчислювальних середовищ.

Список використаної літератури

[1] Giarratano J., Riley G. Expert Systems: Principles and Programming. English edition, Course Technology Inc., 2004. 842p.

[2] CLIPS Rule Based Programming Language. URL: https://sourceforge.net/projects/clipsrules/

[3] CLIPS: A Tool for Building Expert Systems. URL: https://www.clipsrules.net/

УДК: 004.8

ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ НЕЙРОМЕРЕЖЕВОГО МЕТОДУ РОЗПІЗНАВАННЯ МАНІПУЛЯТИВНИХ ФІШИНГОВИХ ПОВІДОМЛЕНЬ У КОНТЕКСТІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Мазурець О.В., Назаров В.В.

(exe.chong@gmail.com, uuu.vich228@gmail.com)

Хмельницький національний університет, комунальний заклад загальної середньої освіти «Ліцей №17 Хмельницької міської ради» (Україна)

Досліджено ефективність нейромережевого методу розпізнавання маніпулятивних фішингових повідомлень, який реалізує двоетапний принцип аналізу: на першому етапі

відбувається бінарна класифікація повідомлень за ознакою «фішинг / не фішинг», а на другому визначення типу маніпулятивного впливу у виявлених фішингових текстах. Запропонований підхід поєднує компактні та багатомовні трансформерні архітектури, зокрема DistilBERT і XLM-RoBERTa, що дозволяє досягти високої точності при мінімальному споживанні обчислювальних ресурсів. За результатами експериментів отримано показники якості на рівні Accuracy 0.991, F1 0.991, F1-macro 0.991, що свідчить про стабільність методу та його здатність відтворювати семантичні маркери маніпуляцій типу urgency, authority та persuasion.

Сучасний розвиток цифрових комунікацій зумовив посилення ризиків, пов'язаних із соціотехнічними атаками, які ґрунтуються не лише на технічних вразливостях, а й на маніпулятивному впливі на користувачів [1]. Одним із найнебезпечніших проявів таких атак є фішингові повідомлення, що імітують достовірну комунікацію з метою отримання конфіденційних даних [2]. Проблема виявлення фішингу виходить за межі традиційних методів сигнатурного пошуку, оскільки зловмисники дедалі частіше використовують складні лінгвістичні стратегії переконання, апеляції до авторитету та створення штучного відчуття терміновості [3]. У цьому контексті актуальним є дослідження нейромережевих методів, здатних до виявлення прихованих маніпулятивних патернів у текстовому змісті електронних повідомлень.

Метою дослідження є перевірка ефективності двоетапного нейромережевого методу розпізнавання маніпулятивних фішингових повідомлень, який поєднує в собі попереднє бінарне виявлення фішингового контенту та подальшу класифікацію типу маніпулятивного впливу. Запропонований метод базується на використанні глибинних трансформерних архітектур різного масштабу, що дає змогу оцінити їхню точність, узагальнювальну здатність і ресурсну ефективність у єдиному обчислювальному середовищі. Експериментальне дослідження здійснено на двох репрезентативних корпусах текстів: перший охоплює приклади фішингових повідомлень із маркуванням за типами маніпуляцій: urgency, authority та persuasion, тоді як другий використовується для навчання бінарного класифікатора, що відрізняє фішингові повідомлення від звичайних електронних листів.

Метод реалізовано у вигляді двоетапного конвеєру, у якому на першому рівні працює бінарний детектор, призначений для швидкої фільтрації повідомлень за ознакою «фішинг / не фішинг», а на другому класифікатор маніпулятивних стратегій, який оцінює тип застосованої соціотехнічної маніпуляції у випадках, попередньо відфільтрованих як фішингові. На етапі попередньої обробки текст уніфікується, очищується від зайвих пробілів і токенізується із жорстким обмеженням довжини для мінімізації латентних витрат; бінарна модель працює в режимі низької затримки з налаштованою пороговою функцією та калібруванням ймовірностей, що дає змогу відсікати явні контр-приклади та направляти до другого етапу лише ті повідомлення, для яких довіра до позитивного висновку достатня. Другий етап використовує контекстно-чутливу трансформерну архітектуру, що аналізує семантичні і прагматичні маркери тексту і формує багатоваріантний розподіл ймовірностей по типах маніпуляцій.

Підготовка даних здійснювалася із дотриманням принципів чистоти вибірки: усуненням пропусків, очищенням текстів від надлишкових пробілів і стандартизацією маркування. Навчальні, валідаційні та тестові підмножини формувалися за стратифікованою схемою у пропорції 70:15:15. Для відтворюваності результатів використовувалося фіксоване зерно випадковості SEED = 42. Модель XLM-RoBERTa-base застосовувалася з максимальною довжиною послідовності 256 токенів і параметрами, орієнтованими на повноцінне відтворення контексту; модель DistilBERT-base-uncased з коротким контекстом 96 токенів, градієнтною акумуляцією та обмеженою кількістю епох, що забезпечувало низьке споживання графічної пам'яті. Усі обчислення виконувалися у середовищі PyTorch із використанням бібліотек Transformers і HuggingFace Datasets.

Отримані результати свідчать про виняткову точність нейромережевого підходу. Модель XLM-RoBERTa досягла повної збіжності вже після двох епох навчання з макропоказником F1 = 1.000 та відсутністю перехресних помилок між класами urgency, authority і persuasion. Матриця помилок наведена на рисунку 1.

Такі результати свідчать про високу чутливість трансформерної архітектури до семантичних і прагматичних маркерів маніпуляцій, зокрема модальних дієслів, форм наказового способу та риторичних конструкцій переконання. Модель DistilBERT продемонструвала аналогічну

стабільність із показником точності понад 99 %, зберігаючи при цьому компактність і ефективність у використанні пам'яті. Помилки класифікації становили менше одного відсотка, що дозволяє розглядати цей варіант для виявлення фішингових повідомлень.

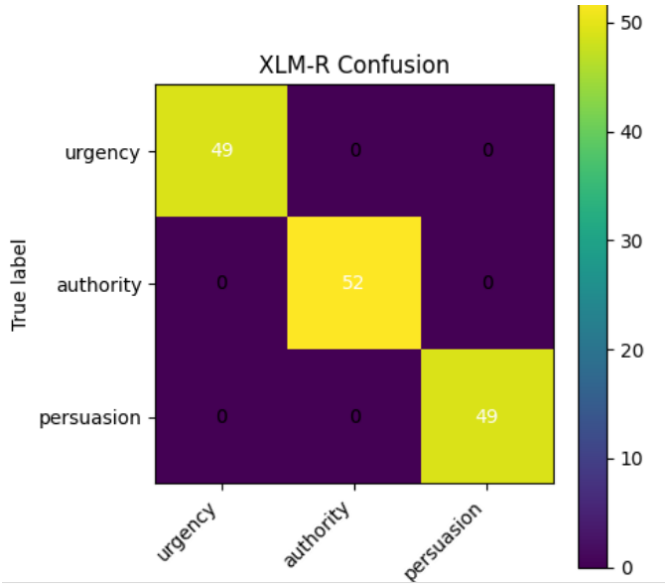

Рисунок 1 – Матриця помилок нейромережі XLM-RoBERTa

Аналіз ефективності продемонстрував, що контекстно-залежні трансформери істотно перевищують традиційні моделі машинного навчання на основі TF-IDF або bag-of-words, оскільки здатні відтворювати складні семантичні залежності та латентні прагматичні ознаки. Високі значення макро- та зваженого F1 пояснюються можливістю моделі адаптивно розпізнавати маніпулятивні стратегії, незалежно від довжини або тематики повідомлення. Виявлено, що наявність емоційно забарвлених лексем, конструкцій, які формують відчуття терміновості або авторитетності, є найінформативнішими для класифікатора, що підтверджує гіпотезу про лінгвістичну природу маніпуляцій.

Розроблений підхід має практичну цінність у контексті підвищення рівня інформаційної безпеки. Використання нейромережевих моделей для автоматичного аналізу текстів електронних повідомлень відкриває можливості створення систем раннього попередження фішингових атак і персональних засобів цифрової гігієни. Модель DistilBERT може бути інтегрована як легковаговий компонент у поштові клієнти, браузерні плагіни або внутрішні корпоративні системи моніторингу комунікацій. Такий підхід дозволяє виявляти не лише прямі фішингові атаки, а й приховані соціотехнічні маніпуляції, які формують поведінкові ризики користувачів.

Отримані результати засвідчують, що поєднання нейромережевих архітектур із високорівневим семантичним аналізом забезпечує нову якість виявлення фішингових загроз. Висока точність класифікації при низьких ресурсних вимогах дає підстави вважати метод придатним для широкого практичного застосування у сфері кіберзахисту та освітніх платформ. Подальший розвиток дослідження передбачає використання інтерпретованих методів атрибуції, таких як Integrated Gradients або LIME, для побудови пояснюваних профілів маніпулятивних стратегій та візуалізації токенів, що найбільше впливають на рішення моделі.

У підсумку доведено, що нейромережеві методи розпізнавання маніпулятивних фішингових повідомлень формують нову парадигму у сфері цифрової безпеки, поєднуючи точність глибинного навчання з інтерпретованістю поведінкових закономірностей. Такий підхід відповідає сучасним викликам кіберпростору, забезпечуючи адаптивність, масштабованість та відповідність принципам надійності й прозорості штучного інтелекту.

Список використаних джерел

[1] A. I. Champa, M. F. Rabbi, F. Eishita, and M. Zibran, "Trick or Treat: A Study of Human Detection of Manipulative Tactics in Phishing Emails" in Proceedings of the International Conference on

Computer Safety, Reliability, and Security, Cham, Switzerland: Springer Nature, Aug. 2025, pp. 299–311.

[2] М. О. Молчанова, О. В. Мазурець, О. В. Собко, Р. В. Віт, і В. В. Назаров, «Алгоритм виявлення аб'юзивного вмісту в україномовному аудіоконтенті для імплементації в об'єктно-орієнтовану інформаційну систему», Вісник Хмельницького національного університету. Серія: Технічні науки, № 1 (331), с. 101–106, 2024. DOI: 10.31891/2307-5732-2024-331-17.

[3] V. Nazarov and M. Molchanova, "Information System for Detecting Abusive Speech in Audio Content by Means of Natural Language" in Proceedings of the V International Scientific and Practical Conference «Modern Strategies of Global Scientific Solutions», Stockholm, Sweden: International Scientific Unity, Dec. 27–29, 2023, pp. 132–135. [Online]. Available: https://isu-conference.com/wp-content/uploads/2023/12/Modern-strategies-of-global-scientific-solutions-Dec-27-29-2023-Stockholm-Sweden.pdf [Accessed: Oct. 22, 2025].

УДК 004.8:629.735.083.5

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ У НАВІГАЦІЙНИХ СИСТЕМАХ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ

Майданик О.О., Мацуй А.М., Мелешко Є.В.
(maidanyksmail@gmail.com, matsuiam@kntu.kr.ua, elismeleshko@gmail.com)
Центральноукраїнський національний технічний університет (Україна)

У роботі розглянуто основні напрями застосування штучного інтелекту (ШІ) у навігаційних системах безпілотних літальних апаратів (БПЛА). Описано сучасні підходи до автономного ухилення від перешкод, планування траєкторії польоту та навігації без використання GPS. Даний підхід до навігації БПЛА з використанням ШІ повинен вирішити проблему польоту з високим рівнем автономності, енергоефективності та надійності в складних умовах середовища (робота в зонах дії радіоелектронної протидії).

Використання штучного інтелекту у навігаційних системах набуває все більше застосувань, як в комерційних так і у військових БПЛА. Перше і головне застосування в комерційних БПЛА – навігація та ухиляння від перешкод з відсутнім чи поганим сигналом GPS. Ця тема дуже актуальна для агродронів, які на сьогоднішній день, змушені працювати в умовах повітряних тривог та дії РЕБ (радіоелектронної протидії). Такі системи можуть швидко та безпечно повертати БПЛА до точки зльоту без його втрати.

Для військового застосування найпопулярніша задача систем навігації з ШІ – це утримання позиції БПЛА (коптерного типу, які використовуються для ретрансляції радіосигналу) на місці без використання GPS та донаведення на ціль. Наступна та дуже важлива задача – це навігація польоту без GPS (розвідка у радіомовчанні або повернення без радіосигналу).

Системи на основі ШІ дають змогу БПЛА розпізнавати перешкоди та ухилятися від них без участі оператора. Для цього використовуються дані з камер, лідарів (лазерних датчиків відстані) або радарів, які обробляються за допомогою нейронних мереж глибокого навчання. Такі рішення дозволяють забезпечити автономний політ у складному або невідомому середовищі [1], [2].

Застосування алгоритмів підкріпленого навчання (Reinforcement Learning, RL) дає змогу БПЛА самостійно планувати траєкторію польоту, мінімізуючи споживання енергії та час виконання місії. Поєднання цих алгоритмів із цифровими двійниками забезпечує можливість тренування моделей у віртуальному середовищі до реального застосування [3], [4].

В умовах де GPS-сигнал недоступний або зазнає перешкод (наприклад, у міській забудові чи під час РЕБ), ШІ використовується для оцінки положення апарата за допомогою комп'ютерного зору, аналізу оптичного потоку та мультисенсорної локалізації [5]. Це дозволяє підтримувати стабільний політ і точне позиціювання навіть у складних умовах.

Однак існуючі системи навігації, які доступні виробникам, мають серйозні недоліки, а саме нестійкість до завад та навмисного заглушення радіочастот керування і GPS-системи навігації. Це