ВИСНОВОК

про наукову новизну, теоретичне та практичне значення результатів дисертації «Виявлення мережевих атак алгоритмами штучного інтелекту» Панчука Богдана Олександровича, поданої на здобуття наукового ступеня доктора філософії за спеціальністю 122 «Комп'ютерні науки» у галузі знань 12 «Інформаційні технології» (Витяг з протоколу наукового семінару відділу № 100 Теорії цифрових автоматів Інституту кібернетики ім.В.М. Глушкова НАН України від «21» березня 2025 р.)

ПРИСУТНІ:

т.в.о. завідувача відділу №100 к.ф.-м.н. Волков В.А., д.ф.-м.н. Летичевський О.О., д.ф.-м.н. Песчаненко В.С., д.т.н. Гордєєв О.О., к.ф.-м.н. Вейцбліт О.Й., д.ф. Стовба В.О., с.н.с., к.ф.-м.н. Годлевський О.Б., н.с., к.ф.-м.н. Донченко А.В, с.н.с., к.ф.-м.н. Колчин О.В., с.н.с., к.ф.-м.н. Мороховець М.К., н.с., к.ф.-м.н. Тарасіч Ю.Г., н.с. Щоголева Н.М., н.с., к.ф.-м.н. Яковлев В.М., аспірант відділу № 100 Панчук Б.О.

СЛУХАЛИ: доповідь аспіранта відділу №100 Теорії цифрових автоматів Панчука Богдана Олександровича за матеріалами підготовленої дисертаційної роботи «Виявлення мережевих атак алгоритмами штучного інтелекту», яка подається на здобуття наукового ступеня доктора філософії за спеціальністю 122 – Комп'ютерні науки.

Дисертаційна робота виконана в Інституті кібернетики імені В.М. Глушкова НАН України.

Науковий керівник – доктор фізико-математичних наук Летичевський О.О.

Тема дисертаційної роботи затверджена Вченою радою Інституту кібернетики імені В.М. Глушкова НАН України (протокол № 20 від 07.12.2021 р.).

В обговоренні доповіді взяли участь: Волков В.А., Песчаненко В.С., Яковлев В.М, Гордєєв О.О, Летичевський О.О.

УХВАЛИЛИ: за підсумками обговорення основних результатів дисертаційної роботи, отриманих здобувачем, їх наукової новизни та практичної цінності, а також узявши до уваги важливість опублікованих за темою дисертації наукових робіт, прийняти такий висновок щодо дисертації Панчука Б.О.

Робота виконувалась відповідно до плану наукових досліджень відділу № 100 Інституту кібернетики імені В.М. Глушкова НАН України у межах науково-дослідної теми:

«Розробити формальні методи виявлення зловмисної поведінки в мережі та хмарному оточенні на основі комбінації алгебраїчних методів та машинного

навчання» (номер теми за перспективним тематичним планом з виконання **ВП.100.17**, 2022-2024 рр., **номер держреєстрації** 0122U001164).

Актуальність теми дисертаційної роботи зумовлена постійним зростанням частоти мережевих атак на інтернет ресурси, а разом з тим і зростанням шкоди, які вони наносять. Джерелом таких атак найчастіше є автономне зловмисне програмне забезпечення, здатне само розповсюджуватись мережею та здійснювати зараження нових пристроїв. Виявлення мережевого трафіку таких програм є першочерговою проблемою для досліджень у даній області. Поведінка зловмисних програм є дуже різноманітною і часто непередбачуваною, що робить малоефективним застосування класичних механізмів виявлення вторгнень, на зразок систем, заснованих на правилах та сигнатурах. Для вирішення даної проблеми дослідники все частіше використовують алгоритми штучного інтелекту (ШІ), які здатні самостійно вивчати шаблони поведінки зловмисних програм та виявляти їх. Однак, більшість наукових робіт в даній області носять суто експериментальний характер і не адресують деякі важливі проблеми, обумовлені даним підходом. Особливо гостро стоїть проблема нестачі та застарілості наборів навчальних даних, що негативно відбивається на якості використаних моделей класифікації. Крім того, застосування нейромереж робить такі системи вразливими до методів ухилення від виявлення за допомогою внесення спеціальних збурень у трафік, за яким ведеться спостереження. Також не надається жодних гарантій щодо якості роботи таких систем на даних за межами тестової вибірки.

Представлене дослідження пропонує підхід до підвищення надійності таких систем за допомогою розширення навчальної вибірки як реальними, так і штучно згенерованими даними. Також був запропонований підхід до оцінювання стійкості використаних моделей нейромереж до спроб навмисного ухилення від виявлення та розроблено метод формальної верифікації їхніх властивостей.

Наукова новизна отриманих результатів.

- Вперше запропоновано підхід до оцінювання вразливості системи виявлення мережевих загроз до спроб ухилення від виявлення за допомогою варіювання розмірів пакетів та міжпакетних інтервалів, який базується на генеруванні правдоподібних змагальних прикладів потоків мережевого трафіка.

- Вперше показана можливість підвищення стійкості системи виявлення мережевих загроз до змагальних атак через розширення навчального набору штучними прикладами.
- Вперше створено метод формальної верифікації нейромереж із використанням спрощення обчислювального графу мережі через розв'язання локальних SMT-задач для функцій активації окремих нейронів.
- Вперше застосовано методи формальної верифікації до нейромережі-класифікатора потоків мережевих даних.

Практичне значення отриманих результатів. Отримані результати були використані для розроблення прототипу багатоцільового аналізатора мережевого трафіку «NetWatcher»; програма здатна виявляти сліди мережевої активності зловмисного програмного забезпечення й у режимі реального часу, й на основі історичних даних. Також «NetWatcher» може бути використана іншими дослідниками в області як інструмент для побудови власних наборів для навчання та тестування моделей класифікації мережевих даних. Екземпляр даної програми було впроваджено в експлуатацію у ролі системи виявлення мережевих загроз у компанії ТОВ «НВП „Радікс"».

Науковий рівень дисертанта. Було визнано, що науковий рівень роботи відповідає вимогам МОН України на здобуття наукового ступеня доктора філософії. У своїх дослідженнях дисертант зробив важливий крок у напрямs вирішення нагальних прикладних та наукових проблем в сфері інформаційної безпеки. Отримані у роботі результати дають змогу поліпшити захищеність мережевих систем є внеском у перспективи подальшого застосування методів штучного інтелекту в даній області.

Науковий шлях здобувача. Панчук Б. О. здобув ступінь бакалавра за спеціальністю «Програмна інженерія» в 2019 р. на факультеті кібернетики Київського національного університету ім. Т.Г. Шевченка і згодом у 2021 р. здобув ступінь магістра за спеціальністю «Комп'ютерні науки» за напрямом «Штучний інтелект». Під час навчання на магістра, здобувач зацікавився розробленням систем виявлення мережевих вторгнень і розпочав пошук можливостей використання моделей штучного інтелекту в даній області. Таким чином, представлене дисертаційне дослідження

будувалось на основі початкових напрацювань до магістерської дипломної роботи. Окрім основної академічної діяльності, здобувач має 8 років досвіду роботи інженером програмного забезпечення та хмарної інфраструктури в комерційних компаніях, що дозволило здобути розуміння багатьох практичних аспектів даної області.

Під час дослідження Панчук Б. О. розробляв програмний інструмент для моніторингу мережевих пристроїв під назвою «NetWatcher», який пізніше був впроваджений у використання в компанії компанії ТОВ «НВП „Радікс”» у ролі системи виявлення загроз.

Повнота викладення матеріалів дисертації у роботах, що опубліковані автором.

Опублікування результатів дисертації повністю відповідає вимогам наказу МОН України „Про опублікування результатів дисертації на здобуття наукових ступенів доктора і кандидата наук” №1220 від 23.09.2019.

Основні наукові результати дисертації в повній мірі викладено у 4 роботах, з яких 3 – наукові статті і 1 – теза доповіді міжнародної наукової конференції. Згідно з вимогами Наказу:

- три роботи [1,2,3] опубліковано у виданнях з наукового напряму дисертаційної роботи, з Переліку наукових фахових видань України;
- одна робота [4] опублікована у збірнику матеріалів міжнародної наукової конференції.

Наукові статті:

1. Б. Панчук. Виявлення ботнет-трафіку на основі потоків, використовуючи ШІ. ISSN 1727-4907. *Проблеми програмування.* 2022. № 3-4. Спеціальний випуск.
2. Б. Панчук. Генерація та використання змагальної вибірки для протидії ухиленню ботнетів від виявлення нейронними мережами. *Проблеми керування та інформатики*. 2023, № 5.
3. Б. Панчук. Формальна верифікація нейронних мереж глибокого навчання. ISSN 1727-4907, *Проблеми програмування*, 2024; 2-3: 253-262.

Тези конференцій, на яких відбувалася апробація результатів дисертаційної роботи:

4. Bohdan Panchuk. Flow-based Botnet Detection with AI Models. Proceedings of the *13th International Scientific and Practical Programming Conference UkrPROG 2022*: 315-328.

Результати дисертаційної роботи доповідались на двох міжнародних конференціях: UkrPROG 2022 та UkrPROG 2024.

Особистий внесок здобувача. Усі основні наукові результаті отримано здобувачем самостійно і виносяться на захист вперше. В опублікованих працях дисертанту належать наступні результати:

[1] – здобувачем описано метод виділення потоків з мережевих даних та здійснено низку експериментів з їх класифікації різними моделями ШІ на предмет виявлення слідів активності ботнетів. На основі цього здобувачем здійснена порівняльна характеристика та сформовані висновки щодо ефективності застосування такої методики для виявлення мережевих загроз.

[2] – здобувачем запропоновано та реалізовано підхід до оцінювання стійкості до змагальних атак систем виявлення мережевих загроз на основі нейромереж. Здобувачем описано метод підвищення стійкості таких систем за допомогою штучного генерування навчальних даних та експериментально показано його ефективність в контексті можливих спроб ухилення від виявлення.

[3] – здобувачем формалізовані критерії надійності системи виявлення мережевих загроз на основі потоків. Здобувачем було запропоновано метод формальної верифікації повнозв'язних нейромереж і продемонстровано можливість його застосування для перевірки сформованих критеріїв стійкості класифікаторів мережевих даних.

[4] – здобувачем експериментально показана можливість підвищення ефективності виявлення трафіку ботнетів за допомогою організації історичних мережевих даних у часові ряди і їх подальшої класифікації рекурентними та згортковими нейромережами.

Достовірність одержаних результатів. Результати, представлені в дисертаційній роботі, є науково обґрунтовані та логічно доведені. Достовірність результатів підтверджується експериментальними даними, отриманими за допомогою створеного прототипу програми з відкритим вихідним кодом, і базується на відкритих наборах даних.

Дисертаційна робота відповідає паспорту спеціальності 122 – Комп'ютерні науки, в галузі знань 12 - Інформаційні технології.

Стиль та мова дисертації. Дисертаційна робота Панчука Б.О. «Виявлення мережевих атак алгоритмами штучного інтелекту» написана державною мовою, стиль викладення матеріалу відповідає прийнятому в науковій літературі. Усі наведені результати достовірні і належним чином обґрунтовані. Бібліографія роботи має достатню повноту та складена відповідно до існуючих вимог. Дисертація оформлена відповідно до вимог наказу МОН України від 12 січня 2017 року № 40.

Рекомендація дисертації до захисту.

1. Дисертаційна робота Панчука Б.О. «Виявлення мережевих атак алгоритмами штучного інтелекту» є актуальною, самостійно виконаною, завершеною науковою працею, в якій містяться нові та раніше не захищені наукові результати, і яка має наукове та прикладне значення. Дисертація відповідає усім вимогам п. 11 „Порядку присудження наукових ступенів і присвоєння вченого звання старшого наукового співробітника" (Постанова Кабінету міністрів України від 24.07.2013 р. № 567).

2. Дисертаційна робота Панчука Б.О. «Виявлення мережевих атак алгоритмами штучного інтелекту» відповідає паспорту спеціальності та рекомендується до захисту на здобуття наукового ступеня доктора філософії за спеціальністю 122 – Комп'ютерні науки – на разовій спеціалізованій вченій раді в Інституті кібернетики імені В.М. Глушкова НАН України.

3. Рекомендовано наступний склад разової спеціалізованої вченої ради.

Голова ради: д.т.н. Будник М.М.

Опоненти: д.т.н. Гордєєв О.О., к.т.н. Ізонін І.І.

Рецензенти: д.ф.-м.н. Пепеляєв, д.ф.-м.н. Горбачук В.М.

Керівник семінару,
к.ф.-м.н. Волков В.А.

Секретар семінару,
к.ф.-м.н. Мороховець М.К.

Інститут кібернетики імені В.М.Глушкова Національної Академії наук України ідентифікаційний код 05417176 м.Київ ДЛЯ ДОВІДОК

Підписи Волкова В.А., Мороховця М.К.
ЗАСВІДЧУЮ
Зав. канц.
ІК НАН України