DOI: 10.34185/1991-7848.itmm.2025.01.096

ВИКОРИСТАННЯ НЕЙРОННИХ МЕРЕЖ РЕАЛЬНОГО ЧАСУ У СИСТЕМАХ ВИЯВЛЕННЯ МЕРЕЖЕВИХ ВТОРГНЕНЬ

Горбатов В.С.[1], Журба А.О.[2]

[1]УДУНТ, аспірант, Україна

[2]УДУНТ, кандидат технічних наук, доцент, Україна

Анотація. *В роботі розглянуто нагальні обмеження сучасних систем виявлення вторгнень (NIDS), які зазвичай базуються на статичних текстових правилах. Такий підхід перешкоджає виявленню нових або модифікованих атак, оскільки зловмисники можуть легко обійти ці статичні правила за допомогою мінімальних модифікацій. Як перспективний напрям розглянуто впровадження нейронних мереж, оснащених можливостями онлайн-навчання. Проаналізовано декілька найсучасніших рішень, у тому числі Online Sequential Extreme Learning Machine (OS-ELM), T-DFNN і різні інкрементні моделі глибоких нейронних мереж, усі з яких демонструють здатність адаптуватися в реальному часі. Робота не лише узагальнює поточні методології, але й підкреслює значний потенціал онлайн-навчання для підвищення ефективності та гнучкості систем кібербезпеки, зокрема в динамічному виявленні zero-day загроз.*

Ключові слова: *нейронні мережі, онлайн-навчання, NIDS, виявлення вторгнень, інкрементальне навчання, кібербезпека, Extreme Learning Machine, T-DFNN.*

Зі зростанням кількості та різноманітності рішень, що використовуються в сфері інформаційних технологій, одночасно зросла й варіативність мережевих атак, які можуть бути непомітно вбудовані, на перший погляд, в безпечний трафік. Системи виявлення мережевих вторгнень (NIDS) розроблені для виявлення та зупинення таких атак, проте більшість сучасних корпоративних NIDS базуються на текстових правилах, які спрямовані на конкретні атаки [1].

Правила є статичними, заздалегідь заданими наборами патернів або умов, написаними спеціалістами з мережевої безпеки. Проте цей підхід ускладнює процес виявлення атак, оскільки текстові патерни, орієнтовані на конкретну атаку, можна легко обійти, мінімально змінивши програмний код[2]. Тож, інженери мережевої безпеки повинні писати правила таким чином, щоб вони були не занадто вузько спрямовані і не занадто загальні. А враховуючи ширину

можливостей сучасних мов програмування і методів обфускації, зробити правило таким стає задачею, що майже не виконується.

Потенційним шляхом вирішення проблеми з правилами є нечіткий текстовий пошук з використанням нейро-нечітких мереж. Такі системи існують на даний час [3], але вони обмежені моделлю, яку складно оновлювати і навчити на всіх вже існуючих атаках. Тож наразі є декілька робіт, що пропонують інтеграцію так званих нейронних мереж реального часу у системи виявлення мережевих вторгнень.

Нейронна мережа реального часу — це мережа, що може навчатися по ходу роботи програми. Так, у статті «Online Sequential Extreme Learning Machine for Intrusion Detection» [4] було розроблено систему, де застосовано варіант ELM для оперативного виявлення атак. Система демонструє здатність навчатися «на льоту» — з кожним новим зразком мережевого трафіку модель миттєво оновлюється, що дозволяє виявляти невідомі раніше атаки з мінімальними затримками.

Робота [5], у свою чергу, пропонує інший, інкрементальний підхід до навчання мереж для NIDS. T-DFNN — це алгоритм, здатний вивчати нові вторгнення поступово в міру їх появи у мережі. Модель T-DFNN складається з кількох моделей нейронної мережі глибокого прямого зв’язку (DFNN), з’єднаних у деревоподібну структуру. Схожий, але простіший підхід запропоновано у роботі [6], де описано використання двоетапної системи з використанням глибокої нейронної мережі (DNN) і інкрементального навчання (IL). Модель було навчено за допомогою даних CAN на стадії офлайн. Після цього модель оновлюється новими даними за допомогою методів інкрементального навчання на етапі онлайн [7].

Висновки. Сучасні дослідження підтверджують ефективність застосування нейронних мереж з онлайн-навчанням у системах виявлення мережевих вторгнень. Вони здатні адаптуватися до нових загроз у реальному часі, що значно підвищує гнучкість та стійкість NIDS до новітніх атак. Попри це, у сфері корпоративних NIDS все ще домінують системи на основі правил.

ЛІТЕРАТУРА

1.Sagar N. Shah, Ms. Purnima Singh. Signature-Based Network Intrusion Detection System Using SNORT And WINPCAP. INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT). 2012. T. 01, № 10.

2.Kothamali, P. Reddy & Banik, S. Limitations of Signature-Based Threat Detection. 2022.

3.Detecting Zero-days with SnortML White Paper. Cisco. URL: https://www.cisco.com/c/en/us/products/collateral/security/firewalls/detecting-zero-days-with-snortml-wp.html (дата звернення: 13.04.2025).

4.Li Y., Qiu R., Jing S. Intrusion detection system using Online Sequence Extreme Learning Machine (OS-ELM) in advanced metering infrastructure of smart grid. PLOS ONE. 2018. T. 13, № 2. С. e0192216. URL: https://doi.org/10.1371/journal.pone.0192216 (дата звернення: 13.04.2025).

5.Data M., Aritsugi M. T-DFNN: An Incremental Learning Algorithm for Intrusion Detection Systems. IEEE Access. 2021. T. 9. С. 154156–154171. URL: https://doi.org/10.1109/access.2021.3127985 (дата звернення: 13.04.2025).

6.Intrusion Detection System Based on Deep Neural Network and Incremental Learning for In-Vehicle CAN Networks / J. Lin та ін. Communications in Computer and Information Science. Singapore, 2022. С. 255–267. URL: https://doi.org/10.1007/978-981-19-0468-4_19 (дата звернення: 13.04.2025).

7.Malialis K., Panayiotou C. G., Polycarpou M. M. Nonstationary Data Stream Classification with Online Active Learning and Siamese Neural Networks. Neurocomputing. 2022. URL: https://doi.org/10.1016/j.neucom.2022.09.065 (дата звернення: 13.04.2025).

USING REAL-TIME NEURAL NETWORKS IN INTRUSION DETECTION SYSTEMS

Vitalii Gorbatov, Anna Zhurba

Abstract. *This paper addresses the pressing limitations of modern intrusion detection systems (NIDS), which are typically based on predefined text-based rules. Such an approach hinders the detection of new or modified attacks, as these static rules can easily be evaded by attackers using minimal modifications. As a promising direction, the study explores the implementation of neural networks equipped with online learning capabilities. Several state-of-the-art solutions are analyzed, including Online Sequential Extreme Learning Machine (OS-ELM), T-DFNN, and various incremental deep neural network models, all of which demonstrate the ability to adapt in real time. The work not only summarizes current methodologies but also emphasizes the significant potential of online learning to enhance the effectiveness and flexibility of cybersecurity systems, particularly in the dynamic detection of emerging network threats.*

Keywords: *neural networks, online learning, NIDS, intrusion detection, incremental learning, cybersecurity, Extreme Learning Machine, T-DFNN.*

REFERENCE:

1.Sagar N. Shah, Ms. Purnima Singh. Signature-Based Network Intrusion Detection System Using SNORT And WINPCAP. INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT). 2012. T. 01, № 10.

2.Kothamali, P. Reddy & Banik, S. Limitations of Signature-Based Threat Detection. 2022.

3.Detecting Zero-days with SnortML White Paper. Cisco. URL: https://www.cisco.com/c/en/us/products/collateral/security/firewalls/detecting-zero-days-with-snortml-wp.html (date of access: 13.04.2025).

4.Li Y., Qiu R., Jing S. Intrusion detection system using Online Sequence Extreme Learning Machine (OS-ELM) in advanced metering infrastructure of smart grid. PLOS ONE. 2018. Vol. 13, no. 2. P. e0192216. URL: https://doi.org/10.1371/journal.pone.0192216 (date of access: 13.04.2025).

5.Data M., Aritsugi M. T-DFNN: An Incremental Learning Algorithm for Intrusion Detection Systems. IEEE Access. 2021. Vol. 9. P. 154156–154171. URL: https://doi.org/10.1109/access.2021.3127985 (date of access: 13.04.2025).

6.Intrusion Detection System Based on Deep Neural Network and Incremental Learning for In-Vehicle CAN Networks / J. Lin et al. Communications in Computer and Information Science. Singapore, 2022. P. 255–267. URL: https://doi.org/10.1007/978-981-19-0468-4_19 (date of access: 13.04.2025).

7.Malialis K., Panayiotou C. G., Polycarpou M. M. Nonstationary Data Stream Classification with Online Active Learning and Siamese Neural Networks. Neurocomputing. 2022. URL: https://doi.org/10.1016/j.neucom.2022.09.065 (date of access: 13.04.2025).