УДК 004.056.55:004.8:355.45

Юкальчук А. І., здобувач вищої освіти,
Загоруйко Л. В., канд. техн. наук, доцент,
доцент кафедри інформаційних технологій,
Донецький національний університет імені Василя Стуса

ЗРІВНЯННЯ ЕФЕКТИВНОСТІ ЗАСТОСУВАННЯ РІЗНИХ АРХІТЕКТУР НЕЙРОННИХ МЕРЕЖ ДЛЯ ЗАПОБІГАННЯ ТА ВИЯВЛЕННЯ КІБЕРАТАК НА МЕРЕЖЕВІ РЕСУРСИ В ПЕРІОД ВОЄННОГО СТАНУ

Анотація. У роботі проведено порівняльний аналіз ефективності різних архітектур штучних нейронних мереж (MLP, CNN, SOM, Hopfield, а також гібридних моделей CNN+MLP і Transformer+Hopfield) для задачі запобігання та виявлення різних типів кібератак і мережеві ресурси в умовах воєнного стану. Реалізацію всіх архітектур виконано мовою Python із використанням сучасних бібліотек машинного навчання.

Ключові слова: нейронна мережа, виявлення вторгнень, DOS, R2L, U2R.

Вступ. Зі зростанням кількості кібератак та залежності критичних систем від мережевої інфраструктури виникає потреба у створенні надійних систем виявлення вторгнень. У роботі досліджено застосування штучних нейронних мереж для автоматичного розпізнавання аномалій у мережевому трафіку та виявлення складних атак. Метою є порівняння ефективності різних архітектур нейромереж на основі датасету KDD’99, визначення їх переваг і недоліків, а також формування рекомендацій щодо використання в умовах підвищених вимог до кібербезпеки [1–2].

Для моделювання й аналізу ефективності виявлення кібератак обрано кілька підходів: багатошарові персептрони (MLP), згорткові мережі (CNN), самоорганізуючі карти Кохонена (SOM), мережі Хопфілда та гібридні архітектури – щоб комплексно оцінити різні парадигми в контексті кіберзахисту. MLP використано як базову модель – це послідовність повнозв’язних шарів для класифікації; підходить для загальних взаємозв’язків між ознаками, але може вимагати багато параметрів за умови сильно структурованих шаблонів. CNN застосовано для виявлення локальних закономірностей у векторі ознак мережевого трафіка: локальні фільтри дають змогу ефективно знаходити повторювані підструктури й шаблони пакетних послідовностей. SOM використано для ненадзорного виявлення аномалій і візуалізації простору ознак; карта зберігає топологію даних і може слугувати попереднім фільтром або джерелом додаткових ознак. Мережі Хопфілда розглядались як асоціативна пам’ять для збереження прототипів нормального й атакувального трафіка – корисні для перевірки схожості зразків, але мають обмежену масштабованість для високорозмірних наборів. Гібридні архітектури поєднують сильні сторони різних підходів (наприклад, CNN+MLP або Transformer+Hopfield), щоб одночасно захоплювати локальні й глобальні залежності та підвищувати чутливість до рідкісних патернів. Практично важливими були методи роботи з дисбалансом класів і стійкістю до шуму (корекція ваг, sampling, focal loss), а також стандартні механізми контролю якості; система реалізована як

конвеєр: попередній фільтр – основний класифікатор – модуль асоціативного контролю. Загалом різні архітектури виконують різні ролі: щільні мережі – базова класифікація, CNN – локальні патерни, SOM – аномалії й візуалізація, Hopfield – прототипний контроль; гібриди забезпечують гнучкість. Далі в статті наведені методологічні деталі і критерії порівняння.

Результати дослідження. Dos – майже всі моделі демонструють дуже високий recall: SOM 99.76 %, CNN+MLP 99.34 %, MLP ≈99.50 % (оцінка), Hopf+Trans 98.66 %, CNN 99.29 %; суттєво відстає Hopfield (≈64 %). Підсумок: dos-патерн детектується більшістю архітектур, крім Hopfield.

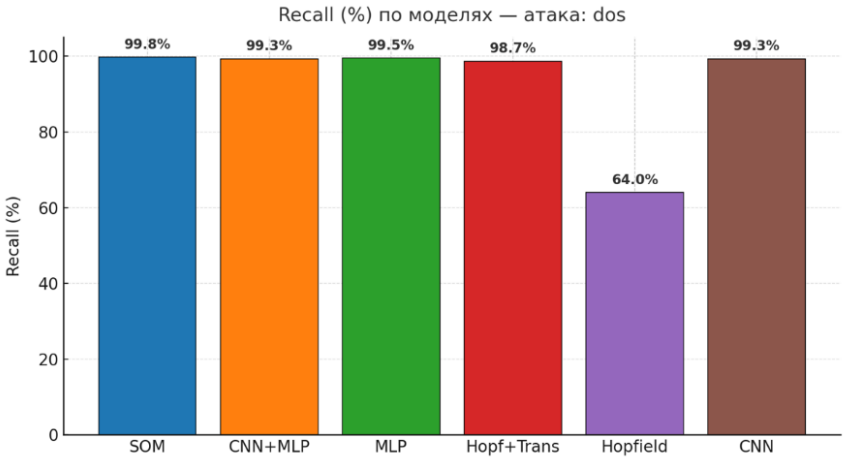

Рисунок 1 – Графік ефективності моделей по атаках dos

R2L – великий розрив між моделями: CNN+MLP 99.56 % і Hopf+Trans 99.47 % – дуже високі; Hopfield ≈63 %; SOM 57.64 %; MLP 0.00 % і CNN ≈0.98 % – майже не виявляють. Підсумок: r2l дає сильно нерівномірні результати між підходами.

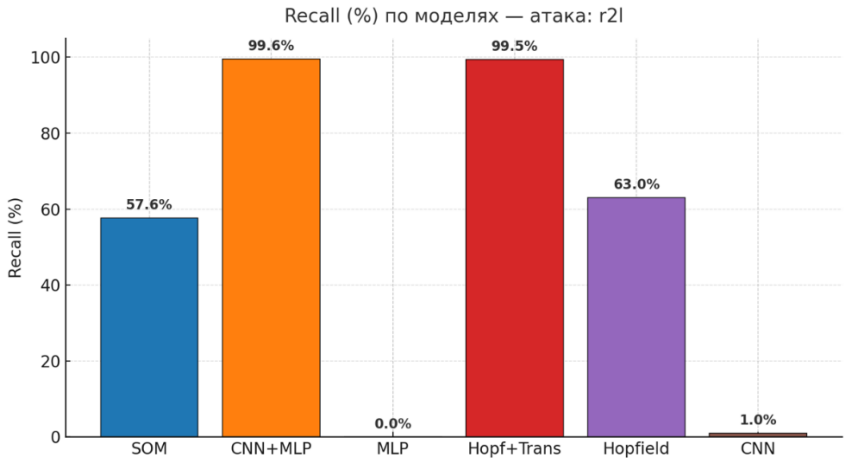

Рисунок 2 – Графік ефективності моделей за атаками r2l

U2R – показники дуже розділені: CNN+MLP 100.00 %, Hopf+Trans 98.08 %, Hopfield ≈92.50 %; натомість SOM 0.00 %, MLP 0.00 % і CNN 0.00 % – практично не виявляють. Підсумок: u2r виявляється лише у деяких спеціалізованих / гібридних архітектурах.

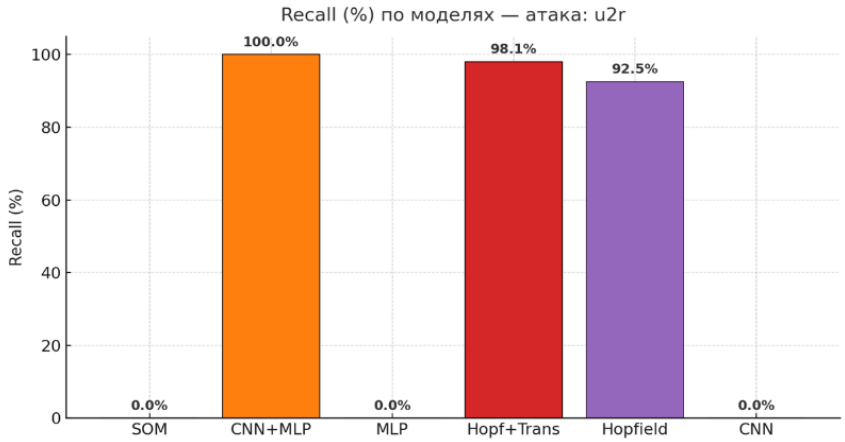

Рисунок 3 – Графік ефективності моделей за атаками u2r

Probe – розкид результатів: CNN+MLP 99.88 % і Hopf+Trans 99.71 % – найкраще; MLP 95.08 %, CNN 93.86 %, SOM 88.26 %, Hopfield ≈72 %. Підсумок: для probe кращі показники у гібридних підходів.

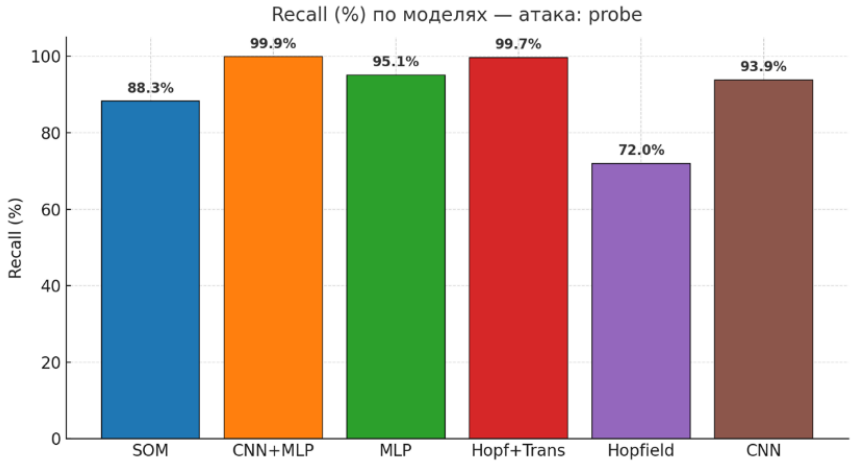

Рисунок 4 – Графік ефективності моделей за атаками probe

Normal – високі показники для більшості моделей: CNN 99.90 %, SOM 99.50 %, MLP ≈99.40 %, CNN+MLP 99.22 %; нижчі у Hopf+Trans (88.16 %) і Hopfield (≈70 %). Підсумок: нормальний трафік добре відокремлюється більшістю моделей, з окремими винятками.

Висновки. Найзбалансованішою й найефективнішою виявилась гібридна модель CNN+MLP, яка дає майже стовідсоткові показники у всіх п’яти класах (≈99 %+), тобто найкраще поєднує виявлення масових і рідкісних атак. Transformer+Hopfield також сильно розпізнає атаки (високі recall для dos, r2l, u2r, probe), але за рахунок цього значно гірше відокремлює нормальний трафік (normal ≈88 %), що призводить до підвищеної кількості хибних спрацювань. Чисті архітектури MLP та CNN добре працюють для домінуючих класів (dos, normal), проте майже не виявляють рідкісні атаки (r2l, u2r ≈0 %). SOM демонструє хороше групування для dos і normal та пристойний результат для probe, але слабко виявляє дуже рідкісні u2r і частково r2l. Hopfield показав помірні результати і не конкурує з найкращими архітектурами за загальною ефективністю.

Список використаних джерел

1. Malik M. Advancing Network Security Through Artificial Intelligence and Machine Learning: A Comprehensive Survey and Future Directions. *International Journal of Network Security Advances.* 2025. URL: https://www.academia.edu/143363874/Advancing_Network_Security_Through_Artificial_Intelligence_and_Machine_Learning_A_Comprehensive_Survey_and_Future_Directions

2. Bensaoud A., Jugal K. Optimized detection of cyber-attacks on IoT networks via hybrid deep learning models. *Ad Hoc Networks.* 2025. Vol. 170: 103770. URL: https://www.sciencedirect.com/science/article/abs/pii/S1570870525000186