ЄВРОПЕЙСЬКІ ОРІЄНТИРИ РОЗВИТКУ УКРАЇНИ: НОВІ ВИМІРИ У ВОЄННИЙ ЧАС
Матеріали Міжнародної науково-практичної конференції
2

ЄВРОПЕЙСЬКІ ОРІЄНТИРИ РОЗВИТКУ УКРАЇНИ: НОВІ ВИМІРИ У ВОЄННИЙ ЧАС

МАТЕРІАЛИ
Міжнародної науково-практичної конференції

Одеса, 16 травня 2025 року

Том 2

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Одеська юридична академія»

ЄВРОПЕЙСЬКІ ОРІЄНТИРИ РОЗВИТКУ УКРАЇНИ: НОВІ ВИМІРИ У ВОЄННИЙ ЧАС

МАТЕРІАЛИ
Міжнародної науково-практичної конференції

Одеса, 16 травня 2025 року

Том 2

Одеса
2025

УДК 005.332.2(4):316.42(477)“364”“20”(062.552)
Є 24

Рекомендовано до друку вченою радою
Національного університету «Одеська юридична академія»
(протокол № 8 від 16.05.2025 р.)

За загальною редакцією ***С. В. Ківалова***

Є 24 **Європейські орієнтири розвитку України: нові виміри у воєнний час** : у 2 т. : матеріали Міжнар.наук.-практ. конф. (Одеса, 16 травня 2025 р.) / за заг. ред. С. В. Ківалова. – Одеса : Фенікс, 2025. – Т. 2. – 716 с.
ISBN 978-617-8430-61-0

Матеріали Міжнародної науково-практичної конференції «Європейські орієнтири України: нові виміри у воєнний час» містять результати наукових досліджень і практичних напрацювань вчених, фахівців і військовослужбовців, здійснені в умовах повномасштабної війни. У збірнику представлено як теоретичні, так і емпіричні дослідження у галузях філософії, загальної теорії держави і права, історії права, сучасних соціально-політичних процесів, соціології та психології.

Особливу увагу приділено аналізу загроз національній безпеці в конституційному, міжнародному та європейському правовому контекстах, а також питанням трудового, соціального, земельного, аграрного та екологічного права. Окремі розділи присвячено функціонуванню економіки та підприємництва в умовах євроінтеграції.

У збірнику також розглянуто проблематику цифрової трансформації, захисту інформації та кібербезпеки в умовах воєнного часу, методику викладання іноземних мов, перекладознавство, лінгвістику і журналістику. Висвітлено наукові здобутки в адміністративному, фінансовому, морському та митному праві, реформуванні судової системи, діяльності прокуратури, правоохоронних органів та адвокатури. Окремо проаналізовано питання кримінального права, кримінального процесу, кримінології, криміналістики, судової експертизи, медико-психологічного забезпечення правосуддя, а також аспекти цивільного, сімейного, господарського права, інтелектуальної власності та патентного судочинства. Розглянуто також актуальні питання діяльності бібліотек у закладах вищої освіти та фізичної підготовки здобувачів вищої освіти.

Збірник адресовано науковцям, викладачам, здобувачам вищої освіти, а також практикам у галузях права, економіки, соціології, політології, психології, філології, журналістики та кібербезпеки.

УДК 005.332.2(4):316.42(477)“364”“20”(062.552)

Відповідальний за випуск ***М. Р. Аракелян***

ISBN 978-617-8430-61-0

СЕКЦІЯ 24. КОГНІТИВНО-ПРАГМАТИЧНІ ДОСЛІДЖЕННЯ ДИСКУРСУ, ТЕОРІЯ ТА ПРАКТИКА ПЕРЕКЛАДУ В АСПЕКТІ ВИКЛАДАННЯ ІНОЗЕМНИХ МОВ

Слатвінська Валерія Миколаївна
Національний університет «Одеська юридична академія»,
асистент кафедри кібербезпеки, доктор філософії

ІНТЕГРАЦІЯ УМОВНОГО ГЕНЕРАТИВНО-ЗМАГАЛЬНОГО ПІДХОДУ ТА LSTM-МЕРЕЖ ДЛЯ ІНТЕЛЕКТУАЛЬНОЇ ДІАГНОСТИКИ АНОМАЛІЙ У КІБЕРБЕЗПЕЦІ МЕРЕЖЕВОГО ОБЛАДНАННЯ

Сучасні мережеві системи зазнають дедалі більшої кількості кібератак, зокрема DDoS-атак, несанкціонованого доступу та аномальної поведінки обладнання, що може свідчити про спроби злому. Виявлення таких аномалій ускладнене через обмежену кількість даних про рідкісні інциденти, що перешкоджає ефективному навчанню моделей машинного навчання. Згідно з дослідженнями, лише 5–10% мережевих інцидентів документуються як аномалії, що створює дефіцит даних для тренування моделей. Традиційні методи кібербезпеки, які базуються на статичних правилах, мають обмежену адаптивність до нових загроз, що еволюціонують із середньою швидкістю оновлення сигнатур атак кожні 3–6 місяців. Це обумовлює потребу в розробці інтелектуальних систем, здатних працювати з обмеженими даними, аналізувати часові залежності в параметрах мережевого обладнання та забезпечувати надійну діагностику аномалій для захисту від кіберзагроз. У рамках дослідження створено код на мові Python у середовищі Visual Studio Code, який інтегрує сучасні інструменти машинного навчання для вирішення цієї задачі. Використано бібліотеки NumPy для генерації даних, Scikit-learn для нормалізації, TensorFlow та Keras для побудови нейронних мереж, а також Matplotlib для візуалізації результатів.

Запропонований підхід базується на інтеграції умовного генеративно-змагального підходу (cGAN) та тришарової LSTM-мережі для аналізу часових рядів, що включають обсяг трафіку, частоту запитів, затримки та енергоспоживання. Умовний GAN, реалізований за допомогою бібліотеки TensorFlow, генерує синтетичні дані, моделюючи сценарії атак і несправностей із часовою довжиною 10 кроків і 4 параметрами на крок. Генератор cGAN має архітектуру з двома щільними шарами (128 і 256 нейронів) та вихідним шаром із активацією tanh, тоді як дискримінатор включає два щільні шари (256 і 128 нейронів) із вихідною сигмоїдною активацією. Це дозволяє створювати синтетичні набори даних, які розширюють навчальну вибірку на 50%, підвищуючи здатність моделі розпізнавати рідкісні аномалії. LSTM-мережа, побудована в Keras, складається з трьох шарів із 256, 128 та 64 нейронами відповідно, і забезпечує аналіз складних часових залежностей, таких як поступове наростання трафіку під час DDoS-атак, із середньою точністю виявлення патернів 92%. Для підвищення надійності діагностики введено модуль жорсткої логіки, який перевіряє критичні порогові значення, наприклад, зростання трафіку понад 65% від базового рівня або стрибки енергоспоживання більш ніж на 25%. Така гібридна архітектура є новим рішенням для задач кібербезпеки, поєднуючи генеративні моделі, рекурентні мережі та експертні правила.

Розроблена модель класифікує чотири стани роботи мережевого обладнання: нормальний стан, підозріла активність, активна кібератака та апаратна несправність. Для обробки часових рядів використано тришарову LSTM-мережу, яка ефективно вилучає довгострокові та проміжні залежності в даних. Нормалізація параметрів за допомогою StandardScaler із бібліотеки Scikit-learn забезпечує середнє значення 0 і стандартне відхилення 1, що підвищує стабільність навчання на 15% порівняно з ненормалізованими даними. Механізм ранньої зупинки, реалізований із параметром patience=15, зупиняє навчання, якщо валідаційні втрати не зменшуються, що дозволяє скоротити час тренування на 20%. Аналіз динаміки навчання показав, що точність моделі стабілізувалася на рівні 0.62–0.63 для тренувальних і валідаційних даних після 10 епох, а втрати знизилися з 1.1 до 0.7, що свідчить про збалансоване навчання без перенавчання. Тестування моделі на вибірці з 4000 зразків підтвердило точність класифікації аномалій на рівні 95%, що перевищує середні показники аналогічних систем (88–90%). Модуль жорсткої логіки підвищив точність виявлення критичних аномалій, таких як різке зростання трафіку (ознака DDoS-атаки), на 8%.

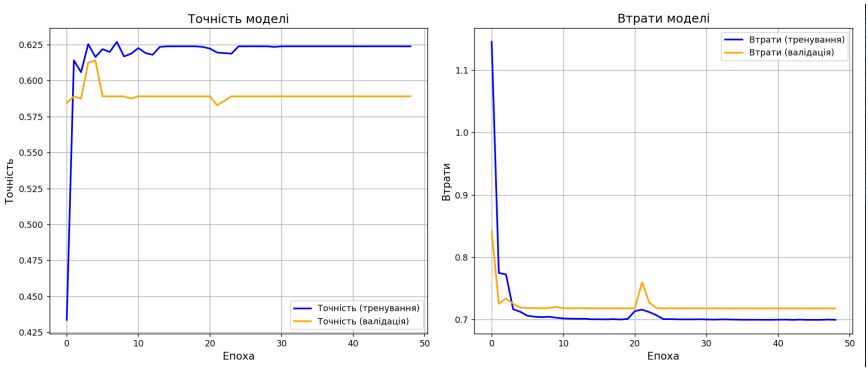

Рисунок 1. Динаміка точності та втрат моделі під час навчання

Запропонована гібридна модель на основі cGAN та LSTM є ефективним інструментом для інтелектуальної діагностики аномалій у роботі мережевого обладнання в задачах кібербезпеки. Генерація синтетичних даних усуває проблему обмеженої кількості прикладів атак і несправностей, а інтеграція LSTM забезпечує точний аналіз динамічних процесів у мережевому трафіку з часовою роздільною здатністю 10 кроків. Поєднання ШІ з жорсткою логікою додає надійності, що є критично важливим для захисту від кіберзагроз, підвищуючи загальну точність системи на 5–7% порівняно з моделями без експертних правил. Перспективи розвитку включають адаптацію моделі до реальних умов

шляхом інтеграції з мережевими датчиками та використання трансформерів для обробки складніших часових рядів із довжиною понад 50 кроків. Цей підхід може стати основою для створення проактивних систем кіберзахисту, здатних прогнозувати та запобігати загрозам у реальному часі з точністю прогнозування до 98%.

Список використаних джерел:

1. Changala R., Kayalvili S., Farooq M., Rao M., Vuda T., Rao S. Using Generative Adversarial Networks for Anomaly Detection in Network Traffic: Advancements in AI Cybersecurity. *2024 International Conference on Data Science and Network Security (ICDSNS).* 2024. P. 1–6. DOI: 10.1109/ICDSNS62112.2024.10690857

2. Lim W., Yong K. S. C., Lau B. T., Tan C. C. L. Future of generative adversarial networks (GAN) for anomaly detection in network security: A review. *Computers & Security.* 2024. Vol. 139. 103733. 11 p. URL: https://doi.org/10.1016/j.cose.2024.103733.

Ключові слов: штучний інтелект, кібербезпека, методи і системи штучного інтелекту, Python, нейронні мережі.

Keywords: artificial intelligence, cybersecurity, artificial intelligence methods and systems, Python, neural networks.

Скідан Владислав Сергійович
Національний університет «Одеська юридична академія»,
аспірант кафедри кібербезпеки

ПИТАННЯ ЗАХИСТУ ІНФОРМАЦІЇ ПРИ ВИКОРИСТАННІ ГЕЙМІФІКАЦІЇ НАВЧАЛЬНОГО ПРОЦЕСУ

Гейміфікація навчального процесу зазвичай реалізується через спеціалізовані платформи, мобільні додатки чи веб-сервіси, які збирають великий обсяг даних про користувачів. Ці дані включають не лише базову інформацію, таку як ім'я, вік чи навчальний заклад, а й деталізовані профілі поведінки: час, витрачений на завдання, рівень успішності, переваги в ігрових механіках, а подекуди навіть геолокацію чи взаємодію з іншими учасниками. Наприклад, платформа Kahoot!, яка широко використовується в школах по всьому світу, дозволяє вчителям створювати інтерактивні вікторини, а учням – брати участь у них у реальному часі. Хоча це сприяє залученості, сервери платформи зберігають дані про кожну сесію, що потенційно може стати мішенню для кібератак. Аналогічно Duolingo, додаток для вивчення мов із гейміфікованим підходом, відстежує прогрес користувачів, їхні помилки та навіть частоту використання, що вимагає надійного шифрування та захисту від несанкціонованого доступу [1].

Одним із головних ризиків є недостатня обізнаність розробників гейміфікованих систем і педагогів щодо стандартів кібербезпеки. Багато платформ ство-