УДК 004.7:519.87(043.3):621.391 DOI: 10.31673/2412-4338.2023.010416

Гайдур Г. І., Гахов С.О., Бригинець А. А.
Державний університет телекомунікацій, Київ

ВИЯВЛЕННЯ МЕРЕЖЕВИХ АНОМАЛІЙ З ВИКОРИСТАННЯМ АЛГОРИТМІВ НЕЙРОННИХ МЕРЕЖ

Анотація: *Стрімка діджиталізація світу призвела до різноманітних атак на комп'ютерні системи та мережі, тому кібербезпека мереж сьогодні є надзвичайно важливою та актуальною складовою забезпечення інформаційної безпеки. Створення дієвих засобів і механізмів кіберзахисту стає дедалі складнішим в міру того, як зростає кількість різноманітних пристроїв та служб. Ідентифікація шкідливого трафіку за допомогою методів глибинного навчання стала ключовим компонентом систем виявлення вторгнень (IDS). У цій статті пропонується порівняння двох моделей глибинного навчання (рекурентної нейронної мережі та згорткової нейронної мережі) для виявлення аномалій у мережах. Обидві нейронні мережі виявились корисними в широкому діапазоні застосувань. Показано, що найкраще у виявленні мережевих аномалій себе проявляють згорткові нейронні мережі у синергії із шарами довгої короткочасної пам'яті. Розвиток технологій глибинного навчання, в тому числі розглянутих алгоритмів нейронних мереж, є перспективним напрямком у сприянні розвитку кібернетичного захисту інформаційних систем. Ці технології є унікальними, адже знаходяться на початковому етапі створення. Вищезгадані технології, на разі, не є поширеними у системах виявлення вторгнень та детектування мережевих аномалій у міру їх новизни, тому потребують більш ретельних досліджень. Звичайних алгоритмів машинного навчання з часом стане не достатньо, адже вони не мають такої хорошої здатності до навчання, як нейронні мережі глибинного навчання. У публікації наведений детальний аналіз можливостей рекурентних та згорткових нейронних мереж разом із шарами довгої короткотривалої пам'яті, що може бути корисним для використання у подальших наукових дослідженнях.*

Ключові слова: *нейронна мережа, згорткова нейронна мережа, рекурентна нейронна мережа, глибинне навчання, машинне навчання, виявлення аномалій у мережі, довга короткочасна пам'ять.*

Haidur H. I., Gakhov S.O., Bryhynets A. A.
State University of Telecommunications, Kyiv

DETECTION OF NETWORK ANOMALIES WITH NEURAL NETWORKS ALGORITHMS

Abstract: *The rapid digitalization of the world has led to various attacks on computer systems and networks, so network security is an extremely important and relevant component of information security today. Creating effective cybersecurity tools and mechanisms is becoming increasingly difficult as the number of different devices and services grows. Identification of malicious traffic using deep learning methods has become a key component of intrusion detection systems (IDS). This article compares two deep learning models (recurrent neural network and convolutional neural network) for detecting anomalies in networks. Both neural networks were found to be useful in a wide range of applications. It has been shown that convolutional neural networks are best at detecting network anomalies in synergy with layers of long short-term memory. The development of deep learning technologies, including the considered neural network algorithms, is a promising direction in promoting the development of cybersecurity of information systems. These technologies are unique because they are at the initial stage of creation. The aforementioned technologies are currently not widespread in intrusion detection and network anomaly detection systems due to their novelty, so they require more thorough research. Conventional machine learning algorithms will eventually become insufficient, as they do not have such a good learning capability as deep learning neural networks do. The article*

provides a detailed analysis of the capabilities of recurrent and convolutional neural networks along with long short-term memory layers, which may be useful for use in further research.

Keywords: *neural network, convolutional neural network, recurrent neural network, deep learning, machine learning, anomaly detection in computer network, long short-term memory*

1. Вступ

Безпека комп'ютерних систем є чутливою та важлтвою проблемою. Вражаючий прогрес інформаційно-комунікаційних технологій наразі пропонує необхідні засоби з передачі файлів, обміну повідомленнями та багато інших форм обміну інформацією. Розвиток комп'ютеризації, на жаль, супроводжувався розвитком зловмисних дій, мотиви яких настільки ж численні, наскільки вони небезпечні та розвиваються з часом. Збільшення кількості комп'ютерних систем у різних мережах, а також уразливості та недоліки, що постійно виявляються в комп'ютерних системах (операційних системах, програмах, протоколах зв'язку тощо), збільшують ризик віддалених атак. Тож атаки стають більш маштабованими та несуть в собі загрози.

Щоб виявити будь-які спроби зламу механізмів безпеки, здебільшого, запроваджується постійний або регулярний моніторинг систем: це системи виявлення вторгнень (IDS). Однак нині парадигм цих систем, які базувались на зіставленні сигнатур відомих векторів атак, уже не достатньо. Так як мережева активність може бути передбачуваною, а її подальша поведінка оцінюється щодо ймовірностей за вивченими моделями, то використання практик нейронних мереж є прогресивним та ефективним рішенням сьогодення.

Важливо також зазначити, що останні роки у сфері інформаційних технологій зростає попит на застосування технологій штучного інтелекту (ШІ) у нових продуктах. За даними дослідницької компанії Gartner, у середньому 54% проєктів, базованих на технологіях штучного інтелекту, проходять повний шлях від планування розробки до виходу готового продукту на ринок.

Така ж тенденція прослідковується і у сфері кібернетичного захисту інформації. Сьогодні все частіше можна спостерігати використання машинного навчання, штучних нейронних мереж та технологій глибинного навчання для створення нових та видозміни старих шкідливих компонентів програмного забезпечення. Саме тому деякі уже відомі засоби захисту мереж, фактично, виходять з гри, адже їхні бінарні алгоритми просто не здатні обробити ту кількість значень, які створюються шляхом квантових обчислень. Через це деякі провайдери послуг захисту впроваджують рішення, базовані на вищезгаданих алгоритмах, для виявлення аномалій у мережах.

Аномалія мережі – це раптове та короткочасне відхилення від нормальної роботи мережі. Деякі аномалії навмисно викликані зловмисниками зі шкідливими намірами, як-от атака на відмову в обслуговуванні (DoS/DDoS) в IP-мережі. Швидке виявлення аномалій необхідне для своєчасного реагування на зміни стану в інформаційній системі.

Розробка ефективної системи виявлення аномалій передбачає витяг релевантної інформації з великої кількості «забруднених» даних великої розмірності. Для цього використовують пристрої моніторингу мережі, які збирають статистичні дані з високою швидкістю. Різні аномалії проявляються в мережевій статистиці по-різному, тому складно розробити загальні моделі нормальної поведінки мережі та аномалій.

Поняття «вторгнення» та «аномалії» зазвичай використовуються як синоніми в контексті IDS; однак обидва терміни мають певні відмінності. Вторгнення — це зловмисна діяльність, яка намагається скомпрометувати конфіденційність, цілісність і доступність, тоді як аномалія стосується моделей даних, які не відповідають очікуваній нормальній поведінці, тобто відхиленню від того, що вважається нормальним. Однак поняття аномалії залежить від сфери застосування та контексту, тобто аномалія не завжди є вторгненням. Наприклад, у мережевому домені відстежуються мережевий трафік, індекси продуктивності та журнали для виявлення збоїв у мережі (це не є вторгненням). Застосування виявлення аномалій поширюється на різні сфери, такі як підозрілі рухи у відеоспостереженні, збої датчиків у

промисловості, ситуації, що загрожують життю в медичних програмах, і шахрайство з кредитними картками в області виявлення злочинів. Тим не менш, IT-адміністратори у сфері кібербезпеки звужують визначення аномалії та вважають будь-які події, які відхиляються від нормальної поведінки, потенційними спробами вторгнення. Дуже часто поняття системи виявлення вторгнень та системи виявлення аномалій утотожнюються, хоч і мають відмінності.

Підходи до виявлення аномалій базуються на методі використаного навчання, на статистичних методах та методі машинного навчання. Одним із методів останнього, є глибинне навчання, яке буде детально розглянуте у цій статті.

2. Аналіз літературних даних і постановка проблеми

Останнім часом глибинне навчання активно вивчається для програм обробки зображень і сигналів. Це техніка, яка знаходить ключові функції у великій кількості даних або дуже складних даних за допомогою комбінації кількох методів нелінійного перетворення [17]. Глибинне навчання найкраще представлено двома алгоритмами: згортковими нейронними мережами (ЗНМ, англ. CNN) для розпізнавання зображень і рекурентними нейронними мережами (РНМ, англ. RNN), які в основному використовуються для обробки природної мови та розпізнавання мовлення [9]. CNN мають локальне сприйнятливе поле та спільне вагове ядро, яке може відображати просторові характеристики шляхом виділення основних візуальних характеристик, таких як орієнтовані краї, кінцеві точки та кути [6]. RNN має дуже глибоку структуру, яка з'єднує основні нейронні одиниці в хронологічному порядку, і зазвичай ефективна для моделювання послідовних даних шляхом навчання з використанням вентильних вузлів, таких як одиниці довготривалої короткочасної пам'яті (LSTM) [14].

Крім того, вивчається поєднання шарів CNN і LSTM для виділення часових і просторових характеристик [19]. Оскільки розпізнавання мовлення та обробка природної мови мають часову та просторову інформацію, поєднання CNN і LSTM може ефективно виділяти певні ознаки [4]. Наразі ці переваги застосовуються для класифікації та прогнозування даних сенсорів, що виникають у промисловій сфері [12].

У цій роботі буде зроблено акцент на виявлення мережевих аномалій засобами рекурентних нейронних мереж (RNN), а саме їх особливої форми – довгої короткочасної пам'яті (LSTM-RNN) та згорткових нейронних мереж (CNN) також у особливій формі LSTM-CNN. Буде проведено порівняння методик та визначено, яка серед них найкраще підходить для виявлення аномалій у мережі.

3. Мета і задачі дослідження

Метою дослідження є аналіз та оцінка методик глибинного навчання з метою знаходження найоптимальнішого способу виявлення мережевих аномалій. Також окреслено сфери застосування алгоритмів та проведено аналіз низки іноземних літературних джерел з метою створення базису для подальших досліджень у цій сфері.

Для досягнення поставленої мети вирішено такі завдання:

- Проаналізовано базові принципи машинного та глибинного навчання.
- Досліджено продуктивність рекуретних нейронних мереж.
- Досліджено продуктивність згорткових нейронних мереж.
- Досліджено продуктивність шарів довгої короткотривалої пам'яті.
- Доведено оптимальність застосування згорткових нейронних мереж із шарами довгої короткотривалої пам'яті у виявленні мережевих аномалій.

4. Машинне навчання

Машинне навчання може автоматично вивчати шаблони функцій і створювати класифікатори. У 2019 році Гу та ін. запропонували алгоритм виявлення DDoS атак, що мав назву SKM-HFS. Аналіз зважених K-середніх збалансовує кількість вибірок і точність, а алгоритм центру кластеризації щільності оптимізує екстремальні значення. Результати показують, що якщо вибрати TOPSIS як фактор оцінки, то цей метод працює найкраще. У 2020

році Панде та ін. використовували алгоритм випадкового лісу, щоб розрізнити звичайні зразки та зразки атаки, а також використовували інструмент WEKA для виявлення пінгів DDoS-атаки смерті. Експерименти з NSL-KDD показують, що випадковий ліс досягає найвищої точності 99,76% під час деяких атак. У 2022 році Квітік та ін. [7] розуміють виявлення DDoS як проблему класифікації кількох пристроїв і розрізняють трафік, створений різними пристроями IoT, за допомогою дерева логічної моделі. Порівняння чотирьох типових пристроїв показує, що дерево логічної моделі може краще ідентифікувати трафік DDoS від пристроїв IoT. Також у 2022 році Кумар та ін. [2] розробили рекурсивний метод усунення ознак (RFE). Він також поєднується з алгоритмом випадкового лісу для навчання класифікатора. Експерименти показують, що цей метод може впоратися зі швидким виявленням за великого мережевого трафіку.

5. Глибинне навчання

Глибинне навчання є складовою машинного навчання і складається з різноманітних методів у галузі машинного навчання, які використовують потоки нелінійних вузлів, розташованих у кількох шарах, які витягують і перетворюють значення змінних сутності зі вхідного вектора. Окремі рівні такої системи мають на вході вихідні дані попередніх рівнів, за винятком початкового вхідного рівня, який отримує сигнали або вхідні вектори із зовнішнього середовища.

Крім того, під час навчання систем можуть застосовуватися неконтрольовані або контрольовані методи. Це призводить до можливого застосування цих моделей до контрольованих навчальних завдань, таких як класифікація, і до неконтрольованих завдань, таких як аналіз шаблонів. Моделі глибинного навчання також покладаються на виділення сутностей вищого рівня з сутностей нижчого рівня, щоб отримати стратифіковане представлення вхідних даних за допомогою підходу до неконтрольованого навчання на різних рівнях сутностей.

Класифікація понять і теорій виходить шляхом вивчення різних рівнів подання даних, що представляють різні рівні поглинання даних. Деякі зі структур глибинного навчання в літературі – це мережі глибинних переконань (DBN), мережі глибинних/стекованих автокодерів (DAE/SAE) і згорткові нейронні мережі (CNN). Ці структури глибинного навчання використовувалися в різних сферах, таких як обробка природної мови, розпізнавання мови, розпізнавання аудіо, розпізнавання та виявлення об’єктів і комп’ютерний зір, що може становити один із факторів автентифікації користувачів.

Глибинне навчання – це гілка алгоритмів машинного навчання, яка:

• використовує кілька рівнів вузлів нелінійної обробки для екстракції та перетворення ознак. Послідовні шари використовують вихідні дані попередніх шарів як вхідні дані;

• навчання без нагляду (наприклад, аналіз моделі) та/або під наглядом (наприклад, класифікація);

• вивчає кілька рівнів представлень, пов’язаних з різними рівнями абстракції. Ці рівні є ієрархією концепцій.

Глибинне навчання можна розділити на три основні класи залежно від цілей, для яких вони були розроблені: мережі неконтрольованого або генеративного навчання, глибинні мережі керованого навчання та гібридні. З підвидами глибинного навчання можна детальніше ознайомитись на рис. 1.

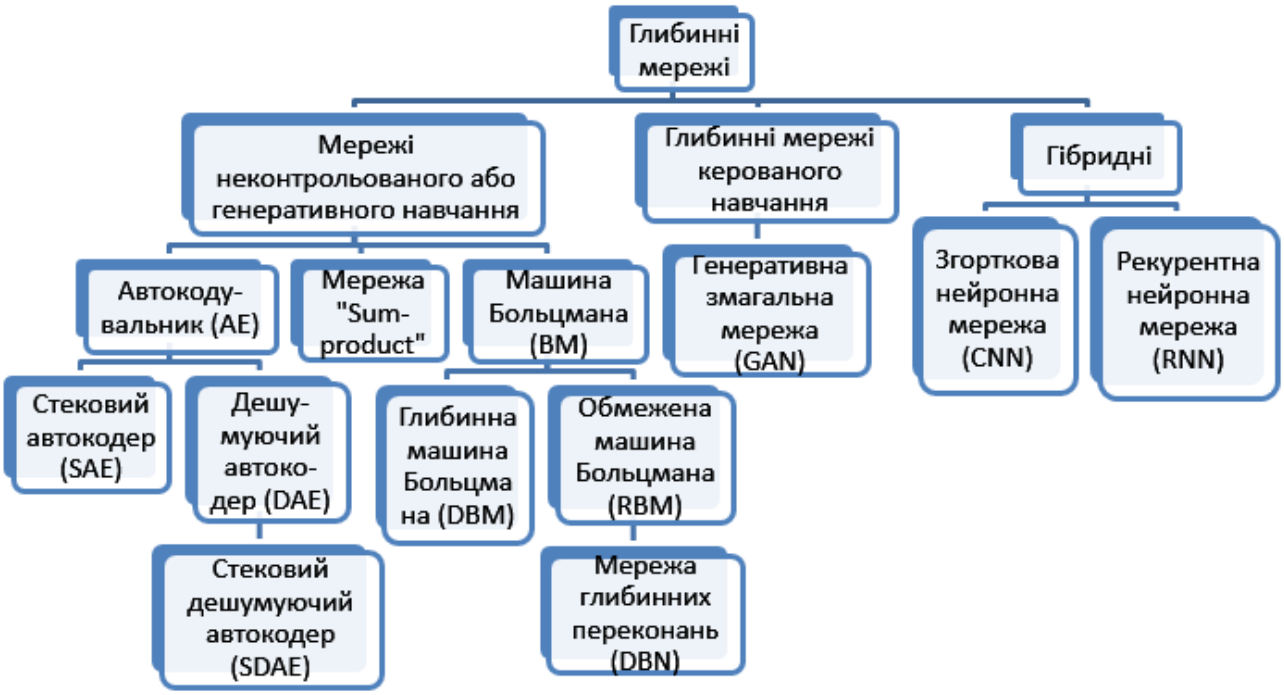


Рис. 1 – Класифікація нейронних мереж

На практиці всі алгоритми глибинного навчання є нейронними мережами, які мають деякі спільні базові властивості. Усі вони складаються з взаємопов'язаних нейронів, організованих у шари. Їх відрізняє архітектура мережі (або спосіб організації нейронів у мережі), а іноді й спосіб їх формування.

6. Рекурентні нейронні мережі RNN/RNN LSTM

Рекурентні нейронні мережі (англ. Recurrent Neural Networks, RNN) – це мережі, що містять зворотні зв'язки і дозволяють зберігати інформацію.

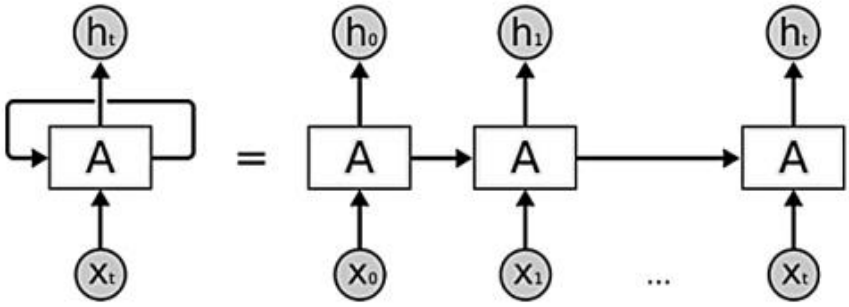


Рис. 2 – Рекурентна мережа у розгорці

На схемі вище фрагмент нейронної мережі A приймає вхідне значення x_t і повертає значення h_t. Наявність зворотного зв'язку дозволяє передавати інформацію від одного кроку навчання мережі до іншого

Особливою формою рекурентної нейронної мережі (RNN), є LSTM, яка широко застосовується для обробки даних часових рядів. У стандартній RNN вихід будь-якого шару залежить не лише від поточного входу, але й базується на попередньому виході. Однак однією з головних проблем для навчання стандартної RNN є проблема зникаючих градієнтів. Градієнти використовуються для оновлення вагових значень нейронної мережі, як показано в

рівнянні 1. Однак коли значення градієнта стає надзвичайно малим, коли воно поширюється в часі, це не надто сприяє навчанню. RNN страждає від невеликих оновлень градієнта, особливо на попередніх шарах. Таким чином, він не може зберігати інформацію для довгих послідовностей.

Нова вага = вага – швидкість_навчання*градієнт (1)

За словами Ральфа С. Штаудемейєра [14], RNN пропонує варіант усунення серйозних проблем раптового зникнення потоку даних та «вибуху» мережевого трафіку за допомогою довготривалої короткочасної пам'яті (LSTM). Як і стандартні нейронні системи прямого зв'язку, LSTM має вхідні асоціації. Вона може не лише обробляти тільки окремі інформаційні фокуси (наприклад, зображення), але ще й цілі масиви даних (такі як відео). Існує багато запропонованих варіантів розробки LSTM.

Більшість сучасних класичних LSTM тепер включають коригування, включно з пропуском шару фільтра забуття і асоціацій комірок. Інші варіації також включають менш складну конструкцію Gated Recurrent Unit (GRU). Результати, отримані в 2018 році, продемонстрували переваги класичних LSTM у підтримці різних інформаційних індексів у порівнянні з різними варіаціями.

Формули реалізації без комірки, які пропонують передовий перехід:

$$f_t = \sigma(W_f \bullet [h_{t-1}, x_t] + b_f) \quad (2)$$
$$i_t = \sigma\,(W_i \bullet [h_{t-1}, x_t] + b_i) \quad (3)$$
$$o_t = \sigma\,(W_o \bullet [h_{t-1}, x_t] + b_o) \quad (4)$$
$$c_t = (c_{t-1}) \odot (f_t + i_t \odot tanh\,(W_c \bullet [h_{t-1}, x_t] + b_c)) \quad (5)$$
$$h_t = tanh(c_t) \odot o_t \quad (6)$$

Три основні сценарії, коли кожна комірка LSTM є: шаром фільтру забуття f_t, вхідним фільтром i_t, вихідним фільтром o_t у момент часу t. Активація входів використовує глибинно розрахований компонент сигмовидної ємності (σ). Навантаження та зміщення W і b - для входів або стану. x_t — вхідна інформація, а h_{t-1} — таємний прихований стан з попереднього кроку. Оновлений стан комірки заповнюється як пам'ять і виводиться за допомогою h_t Значення між 0, 1 є шарами фільтру забуття. Нарешті, ⊙ це компонентне множення двох векторів. Комірки LSTM можуть навчатися під час виконання складних завдань і невиправдано тривалих завдань, коли вміст пам'яті перезавантажується.

У цій роботі розглянуто LSTM, оскільки часова кореляція мережевого трафіку генерує дані часових рядів. Крім того, RNN досягла хороших результатів в обробці зображень завдяки здатності вивчати просторові особливості. Таким чином, інтеграція RNN з LSTM може значно витягнути просторові та часові атрибути необроблених даних і, отже, підвищити точність технологій виявлення вторгнень та аномалій.

7. Виявлення аномалій журналів (логів) на основі RNN-LSTM

Останнім часом RNN-LSTM широко використовується для аналізу даних журналу, ґрунтуючись на подібності методів LSTM, що використовуються в обробці природної мови [17]. Метод кластеризації використовується для кількох записів журналу, які вводяться в мережу LSTM для виявлення та прогнозування збою системи. Узагальнене виявлення та діагностика на основі LSTM використовується, коли необроблені дані обробляються, а потім аналізуються для виявлення. Стекова LSTM — це глибинна архітектура, яка використовується в журнальних даних, де вихід кожного рівня LSTM є входом для наступного рівня LSTM, а повторюваний рівень у часі може бути розгорнутий як мережа прямого зв'язку. У порівнянні зі звичайною RNN, LSTM вимагає мінімальної попередньої обробки даних або взагалі її не вимагає; крім того, вона не вимагає функцій, підготовлених експертами, оскільки вона працює на необроблених даних, а також не вимагає попередньої анотації для функціонування

аномалій.

RNN-LSTM може виконувати багатовимірний послідовний часовий ряд для виявлення зловмисних точок в латентних функціях без необхідності зменшення розмірності. У деяких дослідженнях LSTM використовує багатовимірний розподіл Гаусса. Деякі підходи подібні до запропонованого [11] рішення тим, що LSTM використовується для виявлення аномалій; однак, загалом, неспецифічні дослідження надали результати з багатьох джерел даних журналу, таких як моделювання часових рядів LSTM. У багатоваріантних випадках необхідна анотація, і такі проблеми, як неструктуровані дані, повинні бути розглянуті, оскільки виявлення аномалій із формату послідовного журналу включає вивчення довгострокових залежностей, які сприяють кінцевій ефективності виявлення.

Приклад структури виявлення аномалій запропоновано в [16] для одновимірних даних часового ряду. Їхня структура перевірена на наборі даних NAB і розділена в основному на три частини відповідно до їх опису: «На основі тесту Дікі-Фуллера, швидкого перетворення Фур'є (ШПФ) і коефіцієнта кореляції Пірсона, дані поділені на три класи, а саме: (1) стаціонарні, (2) періодичні та (3) нестаціонарні та неперіодичні часові ряди». Підхід до класифікації аномалій у часових рядах третього типу базується на варіації моделі LSTM, Gated Recurrent Unit (GRU), де помилка передбачення відображається на нормальному розподілі для класифікації точок даних. Їхній підхід показує чудові результати з майже ідеальною точністю, запам'ятовуванням і показником F1 для всіх тестованих наборів даних.

Іншим досить подібним підходом є структура, розроблена в [9], де стекована мережа LSTM використовується для прогнозування на ковзному вікні вхідних даних над даними. На основі передбачень створюється набір помилок, на основі якого підходить класифікатор GNB, щоб потім класифікувати точки даних як нормальні чи аномальні. Використовується набір даних про трафік, подібний до набору даних NAB, але також два інших із різних джерел. Тут цей тип інфраструктури також демонструє великі перспективи для виявлення аномалій у даних часових рядів.

Згадані системи виявлення аномалій досить схожі за своїм підходом. Вони використовують форму мережі на основі LSTM для прогнозування даних часових рядів і класичний метод машинного навчання для класифікації аномалій. З прогнозів створюється набір даних про помилки, і форма нормального розподілу підлаштовується до помилки. Потім можна класифікувати точки даних як нормальні чи аномальні на основі отриманих параметрів. Однак недоліком є те, що ці дослідницькі статті не досліджують ефективність їх моделей на багатовимірних даних.

Початкові дані збираються з інструменту, а потім попередньо обробляються перед поділом на набір для навчання та перевірки, що містить лише звичайні затягування, і набір для тестування зі змішаними даними про звичайні та аномальні затягування. Потім будується модель LSTM відповідно до архітектури та вибору оптимізатора, навчальний набір використовується для навчання моделі, а гіперпараметри налаштовуються на основі продуктивності набору перевірки. Потім тестовий набір звичайних і несправних затягувань можна використати для остаточного тестування продуктивності навченої моделі LSTM. Оскільки тестовий набір не використовується для вибору параметрів моделі LSTM і не впливає на її продуктивність, його можна пізніше навчити та перевірити класифікатор аномалій.

8. Згорткова нейронна мережа CNN/LSTM-CNN

Згорткова нейронна мережа (CNN) — це варіант нейронної мережі, метою якої є вивчення відповідних представлень ознак вхідних даних. Мережа CNN має дві основні відмінності від мереж, що походять від MLP (у нашому випадку це RNN), а саме розподіл ваги та об'єднання. Кожен рівень мережі CNN може складатися з багатьох ядер згортки, які використовуються для створення різних карт функцій. Кожна сусідня область нейрона з'єднана з нейроном у карті характеристик наступного шару. Крім того, щоб створити карту функцій, усі просторові шари входу ділять ядро. Після кількох шарів згортки та кластеризації для класифікації використовується один або кілька повністю пов'язаних шарів [1].

Завдяки використанню спільних вагових коефіцієнтів у CNN модель може вивчати той самий шаблон, що виникає в різних позиціях входів, не вимагаючи навчання окремих детекторів для кожної позиції.

Шари об'єднання зменшують обчислювальне навантаження, оскільки вони зменшують кількість з'єднань між шарами згортки. Крім того, шари кластеризації збільшують властивості інваріантності трансляції та покращують поле прийому наступних згорткових шарів. Як правило, один або кілька повністю зв'язаних рівнів додаються в кінці потоку згортки мережі, а функція втрат використовується для вимірювання помилок з метою навчання.

Як досліджено у роботі [3], CNN має деякі особливості у виявленні мережевих аномалій. Наприклад, для оцінки нашої моделі CNN використовуються чотири показники ефективності: точність (Acc), уточнення (Pre), відкликання (Rec) і значення F1. Математичне представлення цих показників обчислюється на основі рівнянь 3, 4, 5 і 6 відповідно.

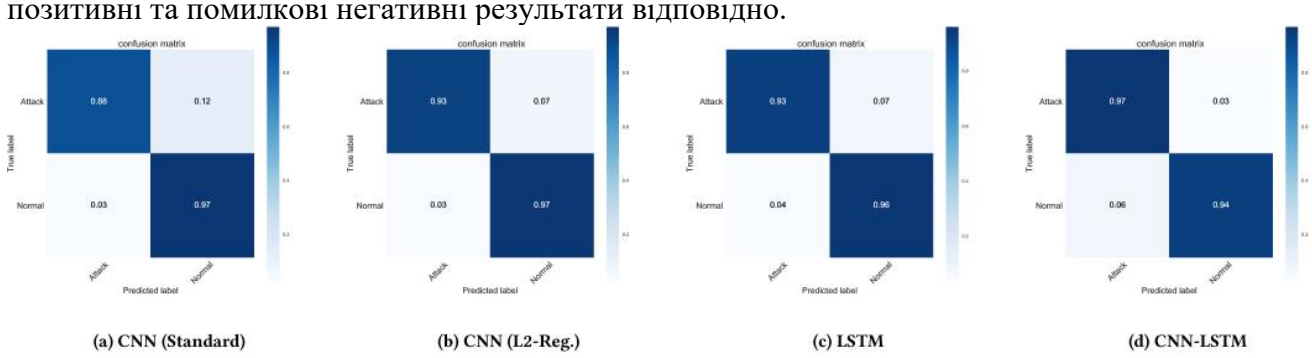
$$Acc=\frac{TP+TN}{TP+TN+FP+FN} \quad (3)$$

$$Pre=\frac{TP}{TP+FP} \quad (4)$$

$$Rec=\frac{TP}{TP+FN} \quad (5)$$

$$F1=\frac{2\times Pre\times Rec}{Pre+Rec} \quad (6)$$

TP, TN, FP і FN позначають справжні позитивні, справжні негативні, помилкові позитивні та помилкові негативні результати відповідно.



(a) CNN (Standard) (b) CNN (L2-Reg.) (c) LSTM (d) CNN-LSTM

Рисунок 3: Матриця помилок для двійкової класифікації, отримана з підходів DL.

Таблиця 1

Уточнення, відкликання та значення F1 для різних методів.

Модель	Уточнення %		Відкликання %		Значення F1 %	
	Норма	Атака	Норма	Атака	Норма	Атака
Стандартна CNN	76,69	98,86	97,47	88,11	85,84	93,18
LSTM	84,53	98,31	96,02	92,95	89,91	95,55
CNN (L2Reg.)	84,24	98,56	96,62	92,75	90,00	95,56
CNN-LSTM	93,18	97,60	94,04	97,24	93,61	97,42

Результати оцінки представлені в таблиці 1, рис. 3, рис. 4 та рис. 5. Можна побачити, що запропонована модель CNN-LSTM працює добре порівняно з іншими існуючими методами. Таблиця 1 і рис. 4 показують, що стандартний алгоритм CNN має низьку продуктивність порівняно з іншими моделями глибинного навчання. Середня точність стандарту CNN становить 90,79%; тоді як коли ми використовуємо методи нормалізації, продуктивність CNN значно підвищується, і вона набирає точність 93,83%. Крім того,

продуктивність LSTM є відносно вищою порівняно зі стандартною CNN, але значно нижчою, ніж CNN з нормалізацією. Крім того, поєднання CNN з LSTM перевершує всі інші алгоритми – отримана точність становить 96,32%, що доводить ефективність запропонованої гібридної моделі CNN-LSTM для виявлення вторгнень. З іншого боку, ми бачимо, що модель CNN (L2Reg.) має вищу уточнюваність для класу атаки та вищу відкликаність для нормального класу порівняно з усіма іншими алгоритмами. Однак модель CNN-LSTM забезпечує найкращий показник F1 для двох класів.

Крім того, можемо спостерігати ефективність запропонованого нами методу для класифікації звичайних даних і даних атаки. Матриця помилок різних підходів глибинного навчання, отримана на етапі тестування, проілюстрована на рис. 3. Кожна подія в наборі для тестування відноситься до звичайних подій або подій атаки. Запропонована модель CNN-LSTM вказує на вищий ступінь точності (0,97) у правильному виявленні подій атаки. Однак точність дещо нижча – 0,94 для звичайних подій трафіку. Це пов'язано з низькими нормальними зразками, які використовуються під час фаз навчання та тестування, порівняно з класами атаки.

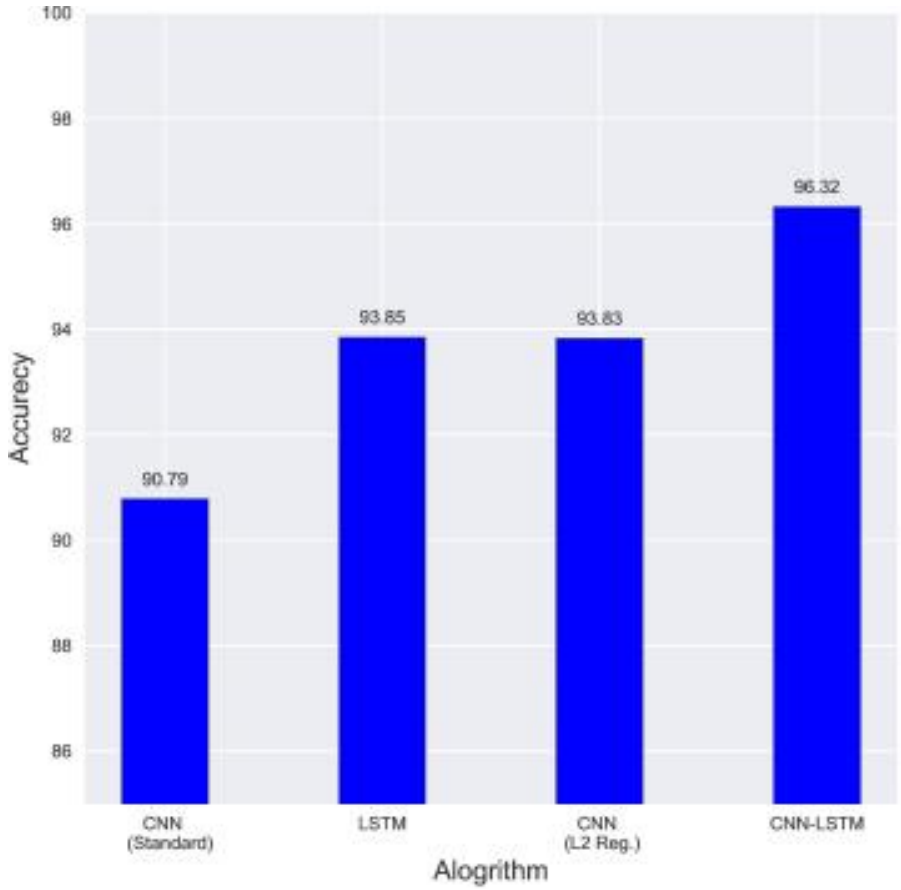


Рис. 4 – Порівняння точності алгоритмів

Для подальшої оцінки запропонованої нами моделі CNN-LSTM використовується крива робочих характеристик приймача (ROC) (рис. 5), щоб показати, як працює модель виявлення в цілому. Крива ROC представляє співвідношення між показниками істинно-позитивних і хибно-позитивних результатів, а площа під кривою (AUC) використовується для вимірювання можливостей моделі. Запропонована модель CNN-LSTM має вищу AUC зі значенням 0,956, за нею йдуть алгоритми CNN (L2Reg.) і LSTM зі значеннями 0,947 і 0,945 відповідно. Навпаки, стандартний CNN забезпечує найнижче значення AUC (0,928), що вказує на нижчу продуктивність цього алгоритму для виявлення мережевих аномалій [3].

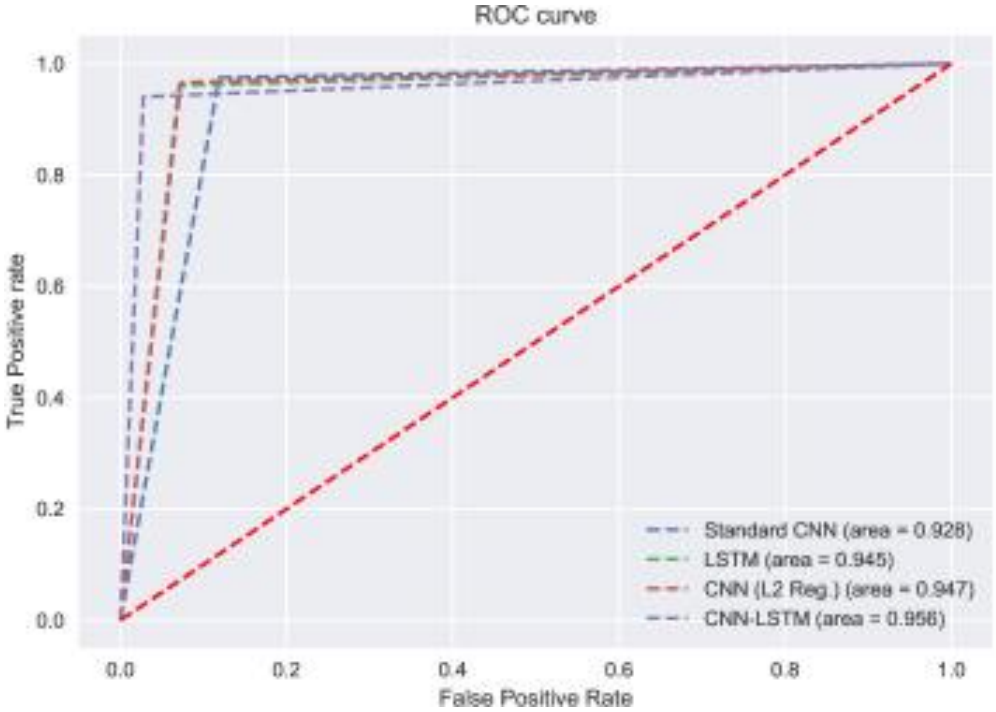


Рис. 5 Крива робочих характеристик приймача (ROC)

8. Узагальнення результатів порівняння CNN, RNN, CNN LSTM і RNN LSTM

У цій статті було проаналізовано ряд характеристик рекурентних та згорткових нейронних мереж, а також їх модифікацій у парі з LSTM. Якщо розглядати їх з точки зору ефективності виявлення мережевих аномалій, то найефективнішими виявляться саме моделі, в яких додатково використовуються шари довгої короткотривалої пам'яті.

Варто зазначити, що при проведені аналізу усіма науковцями використовувався набір даних NSL-KDD. NSL-KDD - це набір даних, запропонований для вирішення деяких проблем, властивих набору даних KDD'99. Незважаючи на те, що ця нова версія набору даних KDD все ще страждає має деякі проблеми і може не бути ідеальним представленням існуючих реальних мереж, через відсутність загальнодоступних наборів даних для мережевих IDS, вважається, що це може бути використано як ефективний еталонний набір даних, щоб допомогти дослідникам порівняти різні методи виявлення вторгнень.

Як показують незалежні досліди вчених, порівняно найнижчу ефективність виявлення аномалій мають моделі рекурентних нейронних мереж, що не є дивним через особливості їх функціонування.

Згорткові нейронні мережі показують себе набагато краще за рекурентні, хоч і в деяких дослідників значення варіюються на лічені відсотки.

Додавання шарів LSTM значно пришвидшує точність виявлення. До прикладу, у випадку з рекурентними нейронними мережами показники точності можуть вирости майже на 30%. Знову ж таки, якщо обирати між CNN-LSTM та RNN-LSTM, то кращі результати покажуть саме згорткові нейронні мережі, що знову ж таки зобумовлено особливістю їх структури. До того ж, рекурентним нейронним мережам знадобиться в рази більше часу на виявлення аномалії через рекурсію кожного елемента всередині мережі, а при додаванні додаткових шарів довгої короткотривалої пам'яті результуватиме неабияким навантаженням на ресурси обчислювальної системи.

З іншого боку, значення показника F1 найкраще у рекурентних нейронних мереж з шарами LSTM (таблиця 1). Тому тут постає питання пріоритезації показників, що різнитиметься у залежності від випадку.

Таблиця 1

Результати порівняння CNN, RNN, CNN LSTM і RNN LSTM

Стаття	Модель	Набір даних	Точність	Уточнення	Відкликання	F1
Їн та ін.	RNN	NSLKDD	71.35	86.64	83.28	83.28
Ліу та ін.	RNN	NSLKDD	91.90	-	-	88.10
Арівуд та ін.	CNN	NSLKDD	99.67	99.69	-	-
Ліу та ін.	CNN	NSLKDD	92.70	-	-	89.20
Лі та ін.	LSTM	NSLKDD	82.78	-	-	83.34
Ліу та ін.	CNN-LSTM	NSLKDD	98.90	-	-	-
Касонго та ін.	RNN-LSTM	NSLKDD	98.59	83.70	-	98.72

Однак використання лише шарів довгої короткотривалої пам’яті не допоможе розв’язати проблему використання часового ресурсу. Річ у тім, що сама LSTM має дуже низький рівень точності виявлень, що у деяких випадках дещо вищий за 80%. Загалом, на невеликих обчислювальних системах, які не мають великого ресурсу, можна було б використовувати і таке рішення, однак якщо мова йде про найвищу точність, то LSTM краще поєднувати із одною з існуючих нейронних мереж.

9. Висновки

Таким чином, дослідження проведені у цій роботі довели, що найоптимальнішою у використанні для виявлення мережевих аномалій є згорткова нейронна мережа з довгою короткотривалою пам’яттю. Вона значно швидша за рекурентну нейронну мережу та достовірніша за звичайні шари довгої короткотривалої пам’яті. До того ж, вона зручніша у використанні та відкриває широкий спектр можливостей для виявлення аномалій у мережі. Це полегшить роботу аналітикам (компетентним спеціалістам), автоматизує процес, зекономить час та мінімізує помилку через людський фактор. Ця робота є важливою із наукової точки зору, адже надає нові можливості у сфері кібернетичного захисту та є перспективним напрямком досліджень.

Список використаної літератури

1. A Convolutional Neural Network for Network Intrusion Detection System / L. Mohammadpour et al. Barcelona, 24–26 October 2018. 2018. P. 50–55.

2. A hybrid approach for feature selection based on genetic algorithm and recursive feature elimination / P. Rani et al. International journal of information system modeling and design. 2021. Vol. 12, no. 2. P. 17–38. URL: https://doi.org/10.4018/ijismd.2021040102 (date of access: 15.03.2023).

3. A hybrid CNN-LSTM based approach for anomaly detection systems in sdns / M. Abdallah et al. 2021. URL: https://dl.acm.org/doi/fullHtml/10.1145/3465481.3469190.

4. Attention and localization based on a deep convolutional recurrent model for weakly supervised audio tagging / Y. Xu et al. Interspeech 2017. ISCA, 2017. URL: https://doi.org/10.21437/interspeech.2017-486 (date of access: 15.03.2023).

5. Elbasani E., Kim J.-D. LLAD: life-log anomaly detection based on recurrent neural network LSTM. Journal of healthcare engineering. 2021. Vol. 2021. P. 1–7. URL: https://doi.org/10.1155/2021/8829403 (date of access: 15.03.2023).

6. Gradient-based learning applied to document recognition / Y. Lecun et al. Proceedings of the IEEE. 1998. Vol. 86, no. 11. P. 2278–2324. URL: https://doi.org/10.1109/5.726791 (date of access: 15.03.2023).

I. Cvitić, D. Perakovic, B. B. Gupta and K. -K. R. Choo, "Boosting-Based DDoS Detection in Internet of Things Systems," in IEEE Internet of Things Journal, vol. 9, no. 3, pp. 2109-2123, 1 Feb.1, 2022, doi: 10.1109/JIOT.2021.3090909.

7. Kasongo S. M. A deep learning technique for intrusion detection system using a Recurrent Neural

Networks based framework. Computer communications. 2022. URL: https://doi.org/10.1016/j.comcom.2022.12.010 (date of access: 15.03.2023).

8. Long-Term recurrent convolutional networks for visual recognition and description / J. Donahue et al. IEEE transactions on pattern analysis and machine intelligence. 2017. Vol. 39, no. 4. P. 677–691. URL: https://doi.org/10.1109/tpami.2016.2599174 (date of access: 15.03.2023).

9. LSTM learning with bayesian and gaussian processing for anomaly detection in industrial iot / D. Wu et al. IEEE transactions on industrial informatics. 2020. Vol. 16, no. 8. P. 5244–5253. URL: https://doi.org/10.1109/tii.2019.2952917 (date of access: 15.03.2023).

10. Malhotra P., Vig L., Shroff G. Long short-term memory networks for anomaly detection in time series. proceedings of the european symposium on artificial neural networks;. Bruges. P. 22–24.

11. Oehmcke S., Zielinski O., Kramer O. Input quality aware convolutional LSTM networks for virtual marine sensors. Neurocomputing. 2018. Vol. 275. P. 2603–2615. URL: https://doi.org/10.1016/j.neucom.2017.11.027 (date of access: 15.03.2023).

12. Review of anomaly detection systems in industrial control systems using deep feature learning approach / R. Kabore et al. Engineering. 2021. Vol. 13, no. 01. P. 30–44. URL: https://doi.org/10.4236/eng.2021.131003 (date of access: 15.03.2023).

13. Sak H., Beaufays F., Senior A. Long short-term memory recurrent neural network architectures for large scale acoustic modeling. 2014. URL: https://www.researchgate.net/publication/279714069_Long_short-term_memory_recurrent_neural_network_architectures_for_large_scale_acoustic_modeling.

14. Staudemeyer R. C. Applying long short-term memory recurrent neural networks to intrusion detection. South african computer journal. 2015. Vol. 56. URL: https://doi.org/10.18489/sacj.v56i1.248 (date of access: 15.03.2023).

15. T.-H. Meen, I. of Electrical, E. Engineers, N. F. University, I. I. of Knowledge Innovation, and Invention, “Anomaly detection for univariate time series with statistics and deep learning,” 2019

16. Xue-Wen Chen, Xiaotong Lin. Big data deep learning: challenges and perspectives. IEEE access. 2014. Vol. 2. P. 514–525. URL: https://doi.org/10.1109/access.2014.2325029 (date of access: 15.03.2023).

17. Young T., Nammous M. K., Saeed K. Advanced Computing and Systems for Security. Berlin, Germany: Springer; 2019. Natural language processing: speaker, language, and gender identification with LSTM; pp. 143–156.

18. Z. Zhou, L. Yao, J. Li, B. Hu, C. Wang and Z. Wang, "Classification of botnet families based on features self-learning under Network Traffic Censorship," 2018 Third International Conference on Security of Smart Cities, Industrial Control System and Communications (SSIC), Shanghai, China, 2018, pp. 1-7, doi: 10.1109/SSIC.2018.8556792.

References

1. A Convolutional Neural Network for Network Intrusion Detection System / L. Mohammadpour et al. Barcelona, 24–26 October 2018. 2018. P. 50–55.

2. A hybrid approach for feature selection based on genetic algorithm and recursive feature elimination / P. Rani et al. International journal of information system modeling and design. 2021. Vol. 12, no. 2. P. 17–38. URL: https://doi.org/10.4018/ijismd.2021040102 (date of access: 15.03.2023).

3. A hybrid CNN-LSTM based approach for anomaly detection systems in sdns / M. Abdallah et al. 2021. URL: https://dl.acm.org/doi/fullHtml/10.1145/3465481.3469190.

4. Attention and localization based on a deep convolutional recurrent model for weakly supervised audio tagging / Y. Xu et al. Interspeech 2017. ISCA, 2017. URL: https://doi.org/10.21437/interspeech.2017-486 (date of access: 15.03.2023).

5. Elbasani E., Kim J.-D. LLAD: life-log anomaly detection based on recurrent neural network LSTM. Journal of healthcare engineering. 2021. Vol. 2021. P. 1–7. URL: https://doi.org/10.1155/2021/8829403 (date of access: 15.03.2023).

6. Gradient-based learning applied to document recognition / Y. Lecun et al. Proceedings of the IEEE. 1998. Vol. 86, no. 11. P. 2278–2324. URL: https://doi.org/10.1109/5.726791 (date of access: 15.03.2023).
I. Cvitić, D. Perakovic, B. B. Gupta and K. -K. R. Choo, "Boosting-Based DDoS Detection in Internet of Things Systems," in IEEE Internet of Things Journal, vol. 9, no. 3, pp. 2109-2123, 1 Feb.1, 2022, doi: 10.1109/JIOT.2021.3090909.

7. Kasongo S. M. A deep learning technique for intrusion detection system using a Recurrent Neural Networks based framework. Computer communications. 2022.

URL: https://doi.org/10.1016/j.comcom.2022.12.010 (date of access: 15.03.2023).

8. Long-Term recurrent convolutional networks for visual recognition and description / J. Donahue et al. IEEE transactions on pattern analysis and machine intelligence. 2017. Vol. 39, no. 4. P. 677–691. URL: https://doi.org/10.1109/tpami.2016.2599174 (date of access: 15.03.2023).

9. LSTM learning with bayesian and gaussian processing for anomaly detection in industrial iot / D. Wu et al. IEEE transactions on industrial informatics. 2020. Vol. 16, no. 8. P. 5244–5253. URL: https://doi.org/10.1109/tii.2019.2952917 (date of access: 15.03.2023).

10. Malhotra P., Vig L., Shroff G. Long short-term memory networks for anomaly detection in time series. proceedings of the european symposium on artificial neural networks;. Bruges. P. 22–24.

11. Oehmcke S., Zielinski O., Kramer O. Input quality aware convolutional LSTM networks for virtual marine sensors. Neurocomputing. 2018. Vol. 275. P. 2603–2615. URL: https://doi.org/10.1016/j.neucom.2017.11.027 (date of access: 15.03.2023).

12. Review of anomaly detection systems in industrial control systems using deep feature learning approach / R. Kabore et al. Engineering. 2021. Vol. 13, no. 01. P. 30–44. URL: https://doi.org/10.4236/eng.2021.131003 (date of access: 15.03.2023).

13. Sak H., Beaufays F., Senior A. Long short-term memory recurrent neural network architectures for large scale acoustic modeling. 2014. URL: https://www.researchgate.net/publication/279714069_Long_short-term_memory_recurrent_neural_network_architectures_for_large_scale_acoustic_modeling.

14. Staudemeyer R. C. Applying long short-term memory recurrent neural networks to intrusion detection. South african computer journal. 2015. Vol. 56. URL: https://doi.org/10.18489/sacj.v56i1.248 (date of access: 15.03.2023).

15. T.-H. Meen, I. of Electrical, E. Engineers, N. F. University, I. I. of Knowledge Innovation, and Invention, “Anomaly detection for univariate time series with statistics and deep learning,” 2019

16. Xue-Wen Chen, Xiaotong Lin. Big data deep learning: challenges and perspectives. IEEE access. 2014. Vol. 2. P. 514–525. URL: https://doi.org/10.1109/access.2014.2325029 (date of access: 15.03.2023).

17. Young T., Nammous M. K., Saeed K. Advanced Computing and Systems for Security. Berlin, Germany: Springer; 2019. Natural language processing: speaker, language, and gender identification with LSTM; pp. 143–156.

18. Z. Zhou, L. Yao, J. Li, B. Hu, C. Wang and Z. Wang, "Classification of botnet families based on features self-learning under Network Traffic Censorship," 2018 Third International Conference on Security of Smart Cities, Industrial Control System and Communications (SSIC), Shanghai, China, 2018, pp. 1-7, doi: 10.1109/SSIC.2018.8556792.