17. **Моркун В. С.** Адаптивная система стабилизации гранулометрического состава выходного продукта замкнутого цикла измельчения на базе средств ультразвукового контроля: дис. ... канд. техн. наук: 05.13.07. Кривой Рог, 1983. 227 с.

18. **Моркун В.С. Потапов В.Н., Моркун Н.В., Подгородецкий Н.С.** Ультразвуковой контроль характеристик измельченных материалов в АСУ ТП обогатительного производства. Кривой Рог: Издат. центр КТУ, 2007. 283 с.

19. **Solodov I.** Ultrasonics of non-linear contacts: Propagation, reflection and NDE-applications // Ultrasonics. 1998, Vol. 36, P. 383–385.

20. **Solodov I., Krohn N., Busse G.** CAN: An example of nonclassical acoustic nonlinearity in solids // Ultrasonics. 2004. Vol. 40. P. 621–625.

21. **Biwa S., Nakajima M., Ohno N.** On the acoustic nonlinearity of solid-solid contact with pressure-dependent interface stiffness. Journal of Applied Mechanics. 2004, Vol. 71, P. 508–515.

22. **Pecorari C., Solodov I.** Universality of non-classical nonlinearity. Springer: New York, 2007. P. 309–336.

23. **Zhang S., Li X., Jeong H., Cho S., Hu H**. Theoretical and experimental investigation of the pulse-echo nonlinearity acoustic sound fields of focused transducers // Applied Acoustics. 2017, Vol. 117, P. 145–149.

24. **Li W., Cho Y., Achenbach J.D.** Detection of thermal fatigue in composites by second harmonic lamb waves // Smart Materials and Structures. 2012, Vol. 21, P. 85–93.

25. **Metya A., Ghosh M., Parida N., Sagar S.P.** Higher harmonic analysis of ultrasonic signal for ageing behaviour study of C-250 grade maraging steel // NDT and E International. 2008. Vol. 41. P. 484–489.

26. **Dodd C. V., Deeds W. E.** Analytical solutions to eddy-current probe-coil problems // Journal of Applied Physics. 39, 2829.

27. **Моркун В. С., Тронь В. В., Гапоненко И. А., Паранюк Д. И.** Идентификация структуры горной породы в процессе бурения на основе ультразвуковых измерений // Гірничий вісник. 2018. Вип. 104. С. 81-86.

Рукопис подано до редакції 30.03.2020

УДК 004.056.5:004.032.26

Н. Н. ШАПОВАЛОВА*, О. Г. РИБАЛЬЧЕНКО, ст. викладачі,
С. В. БІЛАШЕНКО, асист., Н. Х. САІТГАРЕЄВ, доцент
Криворізький національний університет

НЕЙРОМЕРЕЖЕВИЙ МЕТОД РАННЬОГО ВИЯВЛЕННЯ DDOS-АТАК

Мета роботи – теоретично обґрунтувати вибір методу реалізації раннього виявлення аномального трафіка та класифікації мережевих аномалій на основі використання методів машинного навчання, розробити математичну модель штучної нейронної мережі, визначити топологію сформованої моделі і метод її навчання, розробити і протестувати відповідне програмне забезпечення, експериментально перевірити систему.

Методи дослідження. У роботі використано наступні методи дослідження: аналіз джерел з досліджуваної теми, методи теорії штучного інтелекту для проектування топології нейронної мережі, моделювання процесу навчання алгоритмів класифікації, формалізація побудованих моделей, методи проектування програмного забезпечення для розробки програмної моделі, емпіричні методи обґрунтування оптимальної архітектури моделі.

Наукова новизна полягає в тому, що розроблена модель має оптимальну топологію, яка дозволяє ефективно вирішувати поставлене завдання класифікації типів мережевого трафіка, і має достатньо високу здатність до узагальнення. Створене програмне забезпечення з використанням цієї моделі дає можливість проаналізувати мережеві аномалії та виявити DDoS-атаки на ранньому етапі.

Практична значимість виконаної роботи полягає в можливості точно фіксувати початок атаки, а також отримувати навчальні вибірки, які можуть бути використані для навчання нейронних мереж та інших класифікаторів, в тому числі для фільтрації небажаного трафіка. Аналіз мережевого трафіка дозволяє виявити мережеві аномалії та розрізняти аномальну або нормальну його поведінку, внаслідок чого стає можливим не обмежувати обсяг трафіка для клієнтів. Завдяки ранньому виявленні DDoS-атак та швидкому реагуванню, компанії будуть захищені від значних збитків.

Результати. Запропоновано алгоритм протидії DDoS-атакам на основі нейронної мережі, обґрунтовано вибір навчальної множини, що відповідає критерію достатньої репрезентативності. Розроблена математична і програмна модель нейронної мережі для виявлення мережевих аномалій. Визначена архітектура нейронної мережі та функція активації, проведено тестування роботи розробленої програмної моделі.

Ключові слова: DDoS-атака, датасет, нейронна мережа, мережева аномалія, функція активації.

doi: 10.31721/2306-5451-2020-1-50-106-112

Проблема та її зв'язок з науковими і практичними задачами. У час стрімкого розвитку інформаційних технологій компанії та підприємства активно зберігають і поширюють інфор-

* © Шаповалова Н. Н., Рибальченко О. Г., Білашенко С. В., Саітгареєв Н. Х., 2020

мацію в мережі Інтернет. Це, безумовно, зменшує обсяг додаткових витрат на необхідні рекламні послуги, заробітну плату співробітників тощо. Але з появою нових можливостей виникають нові загрози, які пов'язані з недостатнім захистом великих мережевих вузлів. В будь-який момент система, що працює бездоганно, може бути піддана DDoS-атаці (Distributed Denial of Service attack). Метою такої атаки є створення умов, при яких буде ускладнений або повністю обмежений доступ до системи [1].

Компанія, підприємство або окремий користувач, які зазнають DDoS-атаку, можуть понести значні матеріальні та моральні збитки через те, що деякий час їх послуги та ресурси будуть недоступними [2]. За даними компанії McAfee, яка займається розробкою антивірусного програмного забезпечення, світова економіка щороку втрачає близько $600 млрд через кіберзлочинців. Ця цифра враховує і збитки від DDoS-атак. Можна виділити кілька категорій ресурсів, що складають групи найбільшого ризику. Перша група – це сайти державних органів та державні реєстри. Атака на реєстри може паралізувати роботу, наприклад, нотаріусів або публічних сервісів. Сплеск відвідуваності сайту Міністерства освіти та науки під час вступної компанії іноді призводить до відмов у роботі ресурсу. Другі у групі ризику – різноманітні бізнес-компанії в галузі електронної комерції та медичні установи. Третя категорія – це банківські ресурси та ресурси фінансової системи держави. Близько третини потерпілих складають приватні особи та невеликі компанії [3].

Коли об'єктами DDoS-атак є великі установи, то для протидії таким втручанням залучаються чималі кошти для впровадження послуги фільтрації трафіка. Рішення для захисту мають наступні недоліки. По-перше, алгоритми, що використовуються, є комерційною таємницею розробників, що робить неможливим їх поширення. По-друге, висока вартість рішень робить їх недоступними для багатьох компаній і організацій. Наприклад, вартість послуг компаній AT&T та MCI у цій галузі складає близько $12 тис. на місяць.

У зв'язку з вищесказаним очевидно, що проблема виявлення та протидії DDoS-атакам є актуальною та потребує розробки якісного, економічно вигідного методу виявлення та боротьби з атаками на сервери середньої і малої інтенсивності, що здійснює фільтрацію трафіка.

Аналіз досліджень і публікацій. Для ефективної протидії DDoS-атакам потрібно вирішити дві послідовні задачі. Першою задачею є розподіл мережевого трафіка на звичайний та аномальний [4]. Другою задачею є інтелектуальний аналіз аномального трафіка, тобто достовірне діагностування DDoS-атаки на ранніх стадіях. Вирішення цих задач дозволить вчасно застосувати засоби протидії атакам, а саме налаштувати правила міжмережевих екранів, увімкнути мережеві фільтри, задіяти резервні канали тощо.

Всі сучасні DDoS-атаки проводять з використанням ботнету, із застосуванням підміни IP-адрес або комбінованим методом. Їх можна розподілити на три великі групи [5]. Перша група – це атаки з насиченням смуги пропускання, вони направлені на переповнення каналу зв'язку, а саме різні типи flood (затоплення). Їх метою є створити потужний потік запитів, який займає всю виділену смугу трафіка, пакети користувачів не проходять і ресурс змушений відмовляти їм в обслуговуванні (UDP, ICMP та інші потоки фальсифікованих пакетів). Друга група – це атаки на рівні протоколів, вони використовують вразливості стека мережевих протоколів. При атаці через помилки протоколів TCP/IP можуть використовуватися SYN-пакети (запити на відкриття з'єднання), в результаті чого на комп'ютері, що атакується, швидко вичерпується кількість доступних сокетів і сервер припиняє відповідати (так званий SYN- flood). Третя група – це низькоінтенсивні і малопотужні атаки (low-rate DDoS) [6]. Відмова в обслуговуванні досягається приховано, невеликою кількістю трафіка і не вимагає виснаження смуги пропускання. Атакуючий відкриває безліч нескінченних з'єднань і при перевищенні деякого порога викликає в мережі «жертви» відмову в обслуговуванні. Використовуються протоколи транспортного (TCP) або прикладного (HTTP) рівнів моделі OSI. Такі атаки дуже важко виявити, оскільки самі по собі такі з'єднання не є «аномальною» поведінкою.

Нині є багато робіт, присвячених тематиці виявлення атак із застосуванням різноманітних методів, що містять як традиційні підходи на основі відповідності сигнатурним зразкам, так і адаптивні моделі із застосуванням методів інтелектуального аналізу даних. В роботі [7] автори розглянули відомі методи виявлення мережевих атак та запропонували узагальнену схему їх класифікації. Зокрема, запропоновано виділити наступні класи методів виявлення DDoS-атак:

поведінкові методи, методи на основі знань, методи машинного навчання, методи штучного інтелекту.

До поведінкових методів віднесені наступні методи виявлення атак: вейвлет-аналіз, статистичний аналіз, аналіз ентропії, спектральний аналіз, фрактальний аналіз, кластерний аналіз. Ці методи засновані на використанні інформації про нормальну поведінку системи та її порівнянні з параметрами поточної поведінки. Випадок значних відхилень може розглядатися як свідчення наявності атаки. Представлена група методів орієнтована на побудову моделі штатного, або нормального, функціонування системи або користувача.

До методів на основі знань віднесені такі методи, які в контексті заданих фактів і правил зіставлення, що відображають ознаки заданих атак, виконують дії по виявленню атак на основі закладеного механізму пошуку. Своєю назвою ці методи зобов'язані тому, що такі системи працюють з базою знань, в якій містяться дані щодо вже відомих атак. До методів на основі знань віднесені експертні системи, кінцеві автомати, мережі Петрі, сигнатурний метод тощо.

Методи машинного навчання і методи штучного інтелекту застосовують як при виявленні аномалій, так і при виявленні зловживань. Це пояснюється тим, що зазначені підходи в якості вихідних даних для навчання часто використовують шаблони як нормальної, так і аномальної поведінки в мережі. До методів машинного навчання віднесені наступні підходи до виявлення мережевих атак: дерева рішень, Байєсівські мережі, MAP-сплайни, алгоритми кластеризації та алгоритми регресії. До методів штучного інтелекту віднесені штучна нейронна мережа (ШНМ), генетичні алгоритми, нечітка логіка, імунні системи, роєві алгоритми тощо.

Останнім часом все частіше для класифікації трафіка і виявлення мережевих атак використовуються сучасні методи машинного навчання та штучні нейронні мережі. Зокрема, автори у статтях [6, 8] пропонують метод виявлення low-rate атак. Особливістю методу є попередня кластеризація пакетів за допомогою карт Кохонена. Вихідний вектор карти є вхідним вектором багатошарового персептрона, який виконує бінарну класифікацію – визначає, чи є набір мережевих пакетів нормальним або атакуючим. В результаті досягнута помилка розпізнавання атаки склала 0,84%. В роботі [9] для навчання і тестування нейронної мережі, що складалася з 11 вхідних, 1 вихідного нейрона та мала один прихований шар з 23 нейронів, використовувався набір даних «NSL-KDD». Точність класифікації склала 97,87%. Відзначимо, що розглянуті авторами підходи розраховані на виявлення тільки одного класу DDoS-атак. В статті [10] запропонована система для виявлення і класифікації як відомих, так і невідомих аномалій за 4 класами, при цьому оптимальну архітектуру нейронної мережі визначено експериментально. Робота [11] присвячена різним задачам класифікації атак – бінарній та на 4 класи атак. Автори використали рекурентні нейронні мережі для класифікації великого обсягу даних. В результаті для бінарної класифікації досягнута точність менше 0,1% помилок, для класифікації за типом атак – 0,5%.

Постановка завдання. Необхідно створити програмне забезпечення, яке б дозволяло в режимі реального часу виявляти аномальну поведінку у web-трафіка та давало можливість автоматично запобігати зловмисним діям. Для реалізації поставленої мети необхідно вирішити наступні завдання: визначити набір ознак, за якими можливо визначити потенційну атаку; обрати метод створення моделі виявлення DDoS-атаки, або аномальної поведінки на web-ресурсі; реалізувати математичну постановку створюваної моделі; обрати засоби програмної реалізації моделі; реалізувати програмне забезпечення; перевірити валідність робочої моделі на тестових даних.

Викладення матеріалу та результати. Дані, що буде використовувати розроблювальна система, являють собою часовий ряд, з якого були відібрані лише ті ознаки, що дозволяють виявити потенційну небезпеку: порядок надходження пакетів на сервер; поля заголовка рівня IP; поля заголовка рівня TCP; поля заголовка протоколу HTTP; корисне навантаження протоколу HTTP; порядок надходження пакетів на мережевий вузол; кількість пакетів за одиницю часу, що надходить на цільовий вузол; кількість біт інформації за одиницю часу, що надходить на цільовий вузол; проміжки часу між надходженням пакетів [8].

За певними значеннями відібраних ознак необхідно кваліфікувати запити як «нормальні», або як такі, що є небезпечними, – «атаки». Існують навчальні набори записів, які вже розмічені за цими двома категоріями, і в дослідженні будуть використовуватися саме такі набори для відпрацювання здатності розроблювального програмного засобу виявляти небезпеку.

Поставлена задача виявлення ступеню небезпеки для web-ресурсу є задачею класифікації – об'єкти описані зазначеним набором ознак і відома приналежність кожного об’єкту до певного класу. Оскільки у досліджуваній проблемі наявні лише два класи – «норма» і «атака», що будуть закодовані відповідно як «0» і «1», задача належить до типу бінарної класифікації.

На сьогоднішній день найпотужнішим засобом, здатним вирішити поставлену задачу, є технологія машинного навчання – набір методів побудови алгоритмів, що навчаються [12]. До методів, здатних ефективно вирішувати завдання класифікації, належать композиційні методи: Bagging, Random Forest, Gradient Boosting тощо. Цей клас методів заснований на побудові ансамблю простих базових алгоритмів, наприклад, вирішальних дерев, кожне з яких робить внесок у роботу всієї моделі. Перевагою композиційних алгоритмів є можливість розпаралелювання процесу побудови моделі, а також доволі висока якість їх роботи. До недоліків належить велика кількість гіперпараметрів методу. Гіперпараметри – це такі параметри, що заздалегідь невідомі і не настроюються під час навчання моделі, але їх необхідно визначити перед запуском процесу навчання. Серед таких параметрів кількість базових алгоритмів у композиції, глибина дерев, ознаки і їх порогові значення, які визначаються в вершинах кожного дерева, параметр рандомізації вибірок, що потрапляють до навчання тощо. Наявність такої кількості ступенів свободи моделі уповільнює настройку параметрів композиції.

Ще одним класом методів машинного навчання є ШНМ. Модель ШНМ подібна до спрощеної біологічної моделі нейронної мережі (НМ), де нейрони зв'язані між собою синапсами, по яким інформація передається у вигляді електричних імпульсів. Останнім часом ШНМ набули великої популярності у вирішенні задач високої складності, алгоритми розв’язання яких часом не відомі або зовсім не існують. Така здатність ШНМ вирішувати складні задачі обумовлена перевагами біологічних НМ, оскільки модель обробки інформації в них однакова. ШНМ вчиться так само, як мозок живої істоти – на прецедентах. Процес пред’явлення ШНМ об'єктів із зазначенням належності кожного об’єкту до певного класу є навчанням за прецедентами, або навчанням з учителем (supervised learning). Маючи велику кількість прецедентів (прикладів) і відомих відповідей на цих прикладах, можна за кінцевий час навчити ШНМ з заданою точністю класифікувати об'єкти, які навіть не брали участь у процесі навчання, згідно теореми збіжності персептрона Ф. Розенблатта [13]. Крім того, ШНМ є універсальною моделлю, яка здатна апроксимувати будь-які поверхні, і, за теоремою про універсальне наближення [14], може бути представлена у вигляді суперпозиції функцій від однієї змінної – вектору ознак об’єкту.

На користь застосування ШНМ для вирішення поставленого завдання також свідчить ряд переваг цього класу методів: стійкість до зашумлених даних, адаптація до зміни вхідних даних, швидкодія тощо. Серед недоліків ШНМ є ймовірність збіжності методу навчання у локальному мінімумі в процесі оптимізації функціоналу помилки ШНМ при використанні градієнтних методів оптимізації, а за умови застосування стохастичних оптимізаційних методів, які завжди знаходять глобальний мінімум, результат роботи ШНМ не завжди передбачуваний.

З огляду на вищевикладене, для вирішення поставленого завдання буде застосовано метод ШНМ. Для побудови моделі необхідно виконати наступні етапи: визначити тип нейронної мережі; визначити топологію ШНМ (кількість шарів, кількість нейронів у шарах); визначити тип функції активації для кожного шару; визначити функцію помилки; визначити метод навчання ШНМ.

Для задач класифікації використовується тип ШНМ прямого поширення (feedforward мережі), в яких сигнал поширюється строго від вхідного шару до вихідного. У зворотному напрямку сигнал не поширюється.

Оскільки не існує ніяких рекомендацій щодо архітектури ШНМ, ця задача є творчою і вибір певної структури залежить лише від досвіду дослідника, або від вивченого досвіду інших дослідників у цій галузі. Виходячи з того, що найвірогідніше залежність не буде лінійною, оберемо топологію ШНМ з двома прихованими шарами. На користь цього вибору свідчить дослідження Р. Липпманна [15], в якому він доводить, що наявності двох прихованих шарів достатньо для створення областей класифікації будь-якої бажаної форми.

Дуже важливо вірно вибрати кількість нейронів у прихованих шарах: недостатня кількість зробить неможливим навчання мережі, а занадто велика кількість може спричинити ефект перенавчання моделі (overfitting). Перенавчання проявляється у тому, що модель чудово працює на даних, на яких навчалась, але погано на прикладах, яких не було у навчальній вибірці. Для

розрахунку кількості нейронів у двох прихованих шарах скористаємось евристичним правилом геометричної піраміди (geometric pyramid rule) (1)

$$r = \sqrt[3]{\frac{n}{m}}\ ;\ k_1 = mr^2;\ k_2 = mr, \tag{1}$$

де n – кількість нейронів у вхідному шарі; m – кількість нейронів у вихідному шарі; k_1 – кількість нейронів у першому прихованому шарі; k_2 – кількість нейронів у другому прихованому шарі.

Таким чином, обрано наступну топологію ШНМ: у вхідному шарі за кількістю ознак – 9 нейронів; у першому прихованому шарі – 4 нейрони; у другому прихованому шарі – 2 нейрони; у вихідному шарі – 1 нейрон. Вихідний нейрон визначатиме належність об'єкту до класу "атака" - чим ближче до одиниці буде вихідне значення, тим ймовірніша належність об'єкту до цього класу.

Для кожного шару необхідно обрати функцію активації. Оскільки вирішується задача бінарної класифікації, тобто необхідно об'єкти віднести до одного з двох класів, будемо використовувати сигмоїдну функцію активації (2), яка є гладким аналогом порогової функції. В силу того, що для навчання ШНМ буде використано метод зворотного розповсюдження помилки, який потребує диференційованих функцій активації і помилки, застосувати порогову функцію не є можливим. Окрім того, бажано не лише знати клас, до якого модель віднесла той чи інший об'єкт, а й ще ступінь «впевненості» моделі у зробленому виборі. Саме сигмоїдальна функція повертає вірогідність належності об'єкту до певного класу. Сигмоїд є «стискаючою» функцією, тобто незалежно від аргументу (зваженої суми), вихідний сигнал завжди буде в межах від 0 до 1. Будемо використовувати сигмоїдальну функцію активації для всіх шарів НМ

$$out(net) = \frac{1}{1 + \exp(-a \cdot net)}, \tag{2}$$

де net – значення зваженої суми нейрону, a – параметр, що визначає ступінь крутизни графіка цієї функції.

Для оптимізації параметрів мережі, так званих синаптичних вагів, необхідно обрати критерій оптимальності всієї моделі. Таким критерієм у задачах класифікації є мінімум функції похибки алгоритму Q. В якості функції помилки оберемо перехресну ентропію – показник, який використовується для оцінки точності ймовірнісних прогнозів (3)

$$Q(w) = \sum_{i=1}^{l}(y_i \ln a(x_i, w) + (1 - y_i)\ln(1 - a(x_i, w))), \tag{3}$$

де w – матриця параметрів моделі (синаптичні ваги); y_i – істинна відповідь на i-ому об'єкті; $a(x_i, w)$ – відповідь моделі на i-ому об'єкті; l – кількість об'єктів у вибірці; x_i – i-ий об'єкт з матриці x.

Запишемо математичну модель отриманої ШНМ (4)

$$a(x,W) = \sigma^3(\sum_{i=1}^{2} w_i^3 \sigma^2(\sum_{i=1}^{4} w_i^2 \sigma^1(\sum_{i=1}^{9}(w_i^1 x_i) + w_0^1) + w_0^2) + w_0^3), \tag{4}$$

де W – матриця параметрів моделі (синаптичні ваги); w_i^1 – вектор ваг для першого прихованого шару; w_i^2 – вектор ваг для другого прихованого шару; w_i^3 – вектор ваг для вихідного шару; w_0^1 – вільний коефіцієнт першого прихованого шару; w_0^2 – вільний коефіцієнт другого прихованого шару; w_0^3 – вільний коефіцієнт вихідного шару; x_i – i-ий об'єкт з матриці x; σ – функція активації.

Для навчання НМ будемо використовувати популярний і досить швидкий метод – алгоритм зворотного розповсюдження помилки (back propagation). Ідея алгоритму полягає у розрахунку похідної помилки (5) для кожного нейрона і корекції синаптичних ваг з урахуванням помилки, яку, у свою чергу, спричинили помилки нейронів попередніх шарів. Таким чином, обчислення виконуються у зворотному напрямі поширення сигналу мережею, виконуючи корекцію параметрів кожного шару.

Обчислюється градієнт функції помилки за кожним параметром w

$$\nabla_w \varphi(z) = \frac{\partial \varphi(z)}{\partial z} \nabla_w z = \frac{\partial \varphi(z)}{\partial z} x, \tag{5}$$

де $\frac{\partial \varphi(z)}{\partial z}$ – похідна помилки по значенню виходу нейрона і його параметрам.

Потім параметри коригуються за формулою градієнтного спуску (6)

$$w_{k+1} = w_k - \alpha \sum_{i=1}^{l} \nabla_w \varphi(w_k, x_i), \quad (6)$$

де $\varphi(w_k, x_i)$ – помилка на одному об'єкті x_i; α – розмір кроку; k – номер ітерації.

Ітераційний процес продовжується до стабілізації функціоналу похибки.

Реалізуємо НМ у популярній бібліотеці глибокого навчання keras. Перш за все підготуємо дані. Для навчання ШНМ будемо використовувати набір даних CICDDoS2019, який знаходиться у відкритому доступі [16]. Набір складається з 129973 об'єктів, які описані 42 ознаками. Авторами було відібрано лише ті ознаки, за якими було прийнято рішення проводити навчання ШНС. Після формування дата-сету, його було розділено на дві частини у співвідношенні 0,632/0,368. Більша частина даних використовується безпосередньо для навчання моделі, а менша виступає у ролі валідатора – для перевірки якості алгоритму на даних, які не брали участь у навчанні. Ця процедура називається відкладеною вибіркою, і використовується для запобігання перенавчанню НМ.

Створимо Sequential–модель, модель прямого поширення з двома прихованими шарами і обраною активаційною функцію для всіх шарів, скомпілюємо модель. Для навчання моделі необхідно обрати кількість епох навчання. Оскільки не існує будь-якого способу визначення кількості епох, крім емпіричного, проведемо серію експериментів, і встановимо це значення за кращим результатом (рис. 1).

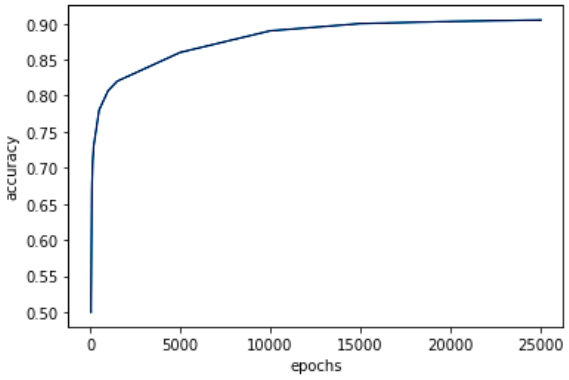

Рис. 1. Точність моделі в залежності від кількості епох

За результатами експерименту обрано кількість епох у розмірі 20 000, оскільки при подальшому їх збільшенні, співвідношення точності моделі до витраченого часу на навчання є не прийнятним. Якість моделі, яка складає 0,9% на тестових даних є цілком задовільною для задачі класифікації, і прийнята як робочий показник для отриманих параметрів ШНМ. Розраховані параметри використовуємо для побудови моделі у розроблювальному програмному забезпеченні для виявлення в режимі реального часу ризику виникнення атаки на web-ресурс.

Висновки та напрямок подальших досліджень. У процесі дослідження проблеми розробки програмного забезпечення системи для виявлення DDoS-атак було проаналізовано сучасний стан питання діагностування втручань на ранніх стадіях, обґрунтовано вибір методів реалізації нейромережевої моделі визначення аномалій трафіка, розроблено і протестоване в лабораторних умовах відповідне програмне забезпечення. Результати експериментального використання системи показали, що програмне забезпечення доцільно доповнити можливістю не лише виявляти потенційну небезпеку, а й визначати тип можливої атаки. Крім того, бажано реалізувати програмний модуль збору інформації про аномальну поведінку трафіка для розширення набору даних, на якому проводилось навчання ШНМ, з метою виявлення та відстеження нових мережевих загроз.

Список літератури

1. **Шаньгин В. Ф.** Информационная безопасность компьютерных систем и сетей / **Шаньгин В. Ф.** // М.: ИД «ФОРУМ»: ИНФРА-М. 2008. 416 с.

2. Understanding Denial-of-Service Attacks. US-CERT. 6 February 2013. Retrieved 26 May 2016 [Електронний ресурс] – Режим доступу до ресурсу: https://www.us-cert.gov/ncas/tips/ST04-015

3. Актуальные киберугрозы – 2018. Тренды и прогнозы. [Електронний ресурс] – Режим доступу до ресурсу: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2018/#id5.

4. **Мурасов Р.К.** Завчасне попередження про DDoS атаку на базі методів прогнозування / **Мурасов Р.К.**, Мельник Я.В.. // Національний університет оборони України імені Івана Черняховського. – 2016. – С. 59.

5. Классификация DDoS-атак: краткий обзор современных подходов [Електронний ресурс] – Режим доступу до ресурсу: https://ddos-guard.net/ru/info/blog-detail/classification-of-ddos-attacks-a-short-overview-of-modern-approaches

6. **Тарасов Я. В.** Метод обнаружения низкоинтенсивных DDoS-атак на основе гибридной нейронной сети / **Я. В. Тарасов** // Известия ЮФУ. Технические науки. – 2014. – С. 47-57.

7. **А. А. Браницкий**. Анализ и классификация методов обнаружения сетевых атак / **А. А. Браницкий**, И. В. Котенко. // Тр. СПИИРАН. – 2016. – С. 207–244.

8. **Тарасов Я.В.** Исследование применения нейронных сетей для обнаружения низкоинтенсивных DDoS-атак прикладного уровня / **Тарасов Я.В.** // Вопросы кибербезопасности. 2017. № 5(24). С. 23-29.

9. Нейросетевая модель выявления DDOS-атак / Воробьёва Ю.Н., Катасёва Д.В., Катасёва А.С., Кирпичников А.П.. // Вестник технологического университета, Т. 21, №. 2. – 2018. – С. 94–98.

10. **Van N.** An anomaly-based network intrusion detection system using Deep learning / **Van N.,** Thinh T., Sach L. // 2 International Conference on System Science and Engineering (ICSSE). Ho Chi Minh City, 2017. Pp. 210-214. DOI: 10.1109/ICSSE.2017.8030867

11. **Yin C.** A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks / **Yin C.**, Zhu Y., Fei J., He X. // IEEE Access. 2017. Vol. 5. Pp. 21954-21961. DOI: 10.1109/ACCESS.2017.2762418

12. **Шолле Ф.** Глубокое обучение на Python / **Шолле Ф.** – Питер: СПб, 2018. – 400 с.

13. **Розенблатт Ф.** Принципы нейродинамики: перцептроны и теория механизмов мозга = Principles of Neurodynamic: perceptrons and the theory of brain mechanisms / **Фрэнк Розенблатт**. – М.: Мир, 1965. – 480 с.

14. **Ian Goodfellow.** Deep learning (Adaptive computationand machine learning series)./ **Ian Goodfellow**, Yoshua Bengio, Aaron Courville. – Cambridge, MA: MIT Press, 2017. – 775 с. –

15. **Richard P. Lippmann**. An introduction to computing with neural nets / **Richard P. Lippmann.** // IEEE ASSP Magazine. – С. 4 – 22.

16. Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy [Електронний ресурс] / Iman Sharafaldin, Arash Habibi Lashkari, Saqib Hakak, and Ali A. Ghorbani // IEEE 53rd International Carnahan Conference on Security Technology, Chennai, India – 2019. – Режим доступу до ресурсу: https://www.unb.ca/cic/datasets/ddos-2019.html.

Рукопис подано до редакції 28.02.2020

УДК 622.026.01:669

С.Г. САВЕЛЬЄВ*, д-р техн. наук, проф., В.В. ПЛОТНІКОВ, канд. техн. наук, доц.,
О.В. БАБАЄВСЬКА, асистент
Криворізький національний університет

ЗАСТОСУВАННЯ ЕЛЕКТРОВПЛИВУ ДЛЯ ЕФЕКТИВНОГО ДРОБЛЕННЯ МАТЕРІАЛІВ В УМОВАХ МЕТАЛУРГІЙНОЇ ПЕРЕРОБКИ

Метою виконуваної роботи є дослідження механізму руйнування матеріалу під дією електрогідравлічного удару й встановлення технологічних можливостей застосування даного явища в металургійній переробці.

Методи дослідження для вирішення поставлених завдань у роботі використовувалися такі, як узагальнення наукової інформації; pH-метрія й потенціометрія рідкої фази; вимірювання електрокінетичного потенціалу поверхні мінералів; лабораторні дослідження; технологічні випробування; гранулометричний і мінералогічний аналізи; методи статистичної обробки результатів досліджень; мікроскопічний аналіз; магнітний аналіз мономінеральних фракцій.

Наукова новизна даного дослідження полягає у встановленні механізму прояву електрогідравлічного ефекту і його руйнуючого впливу на провідні матеріали при їх дробленні.

Практична значимість роботи полягає в дослідженні електрогідравлічного дроблення шлакових систем, а також розробці способів дроблення крихких провідних матеріалів з використанням електровпливу, що може слугувати основою для нових технологій дроблення металургійних шлаків з метою їх подальшого використання в металургійній переробці.

Результати роботи. У роботі розглянуті процеси, що відбуваються при здійсненні методу спільного електрогідравлічного дроблення в'язкого не провідного струм і крихкого провідного матеріалів. Встановлений механізм руйнуючого впливу електрогідравлічного ефекту. З'ясовано, що сутність методу «зовнішнього удару» зводиться до того, що електрогідравлічний удар здійснюється в рідині, але не всередині об'єму, заповненого провідним матеріалом, а поза ним й на такій відстані від матеріалу, щоб іскровий розряд, маючи достатню довжину для повного використання енергії даного імпульсу, був розташований можливо ближче до поверхні шару матеріалу, що руйнується.

Представлені конструкції й принцип роботи дробарок, призначених для дроблення крихких провідних матеріалів до будь-якої крупності – від 20 мм і дрібніше. Представлена технологія може бути застосована для дроблення металургійних шлаків, що становить значний промисловий інтерес. Знайдене ефективне технологічне рішення, що дозволяє виділяти метал з металургійних шлаків в установках надтонкого дроблення з використанням електровпливу.

Ключові слова: дроблення, електровплив, металургійний шлак, електрогідравлічний ефект, розряд.

doi: 10.31721/2306-5451-2020-1-50-112-118

* © Савельєв С.Г., Плотніков В.В., Бабаєвська О.В., 2020