Міністерство освіти і науки України
Харківський національний університет імені В. Н. Каразіна

ВІСНИК

Харківського національного університету імені В.Н. Каразіна

Серія
«Математичне моделювання.
Інформаційні технології.
Автоматизовані системи управління»

Випуск 60

Серія заснована 2003 р.

BULLETIN

of V.N. Karazin Kharkiv National University

Series
«Mathematical Modeling.
Information Technology.
Automated Control Systems»

Issue 60

First published in 2003

Харків
2023

Статті містять дослідження у галузі математичного моделювання та обчислювальних методів, інформаційних технологій, захисту інформації. Висвітлюються нові математичні методи дослідження та керування фізичними, технічними та інформаційними процесами, дослідження з програмування та комп'ютерного моделювання в наукоємних технологіях.

Для викладачів, наукових працівників, аспірантів, працюючих у відповідних або суміжних напрямках.

Наказом Міністерства освіти і науки України від 17.03.2020 № 409 наукове фахове періодичне видання Вісник Харківського національного університету імені В.Н. Каразіна серія «Математичне моделювання. Інформаційні технології. Автоматизовані системи управління» включено до Категорії «Б» Переліку наукових фахових видань України за наступними спеціальностями: 113 – Прикладна математика;122 – Комп'ютерні науки та інформаційні технології; 123 – Комп'ютерна інженерія; 125 – Кібербезпека.

Затверджено до друку рішенням Вченої ради Харківського національного університету імені В. Н. Каразіна (протокол № 22 від 11.12.2023 р.)

Адреса редакційної колегії: 61022, м. Харків, майдан Свободи, 6, ХНУ імені В. Н. Каразіна, к. 534.
Тел. +380 (57) 705-42-81, Email: journal-mia@karazin.ua.

Мова публікації: українська, англійська.

Статті пройшли внутрішнє та зовнішнє рецензування.

Свідоцтво про державну реєстрацію КВ № 21578-11478 Р від 18.08.2015.

The articles are present research in the field of mathematical modeling and computing methods, information technologies, information security. New mathematical methods of research and management of physical, technical and information processes, research on programming and computer modeling in science-intensive technologies are covered.

For teachers, researchers, graduate students working in relevant or related fields.

By the order of the Ministry of Education and Science of Ukraine from 17.03.2020 № 409 scientific professional periodical Bulletin of V.N. Karazin Kharkiv National University series "Mathematical modeling. Information Technologies. Automated control systems" is included in Category "B" of the List of scientific professional publications of Ukraine in the following specialties: 113 – Applied Mathematics, 122 – Computer Science and Information Technology; 123 – Computer engineering; 125 – Cybersecurity.

Approved for publication by the decision of the Academic Council of V.N. Karazin Kharkiv National University (Minutes № 22 of 11.12.2023).

Editorial Address: 61022, Kharkiv, Svobodi sq., 6, V.N. Karazin Kharkiv National University, r. 534.
Phone. +380 (57) 705-42-81, Email: journal-mia@karazin.ua.

Language of publication: Ukrainian, English.

The articles pass internal and external review.

Certificate of state registration: KV № 21578-11478P dated 18.08.2015

ЗМІСТ

CONTENTS

DOI: https://doi.org/10.26565/2304-6201-2023-60-01

УДК 539.3+519.6

Гнітько Василь Іванович
к.т.н., старший науковий співробітеик
Інститут проблем машинобудування ім. А.М. Підгорного НАН України, , м. Харків, вул. Комунальників, 2/10, 61023
e-mail: gnitkovi@gmail.com;
https://orcid.org/0000-0001-7855-3957

Дегтярьов Кирило Гергійович
к.т.н., науковий співробітеик
Інститут проблем машинобудування ім. А.М. Підгорного НАН України, , м. Харків, вул. Комунальників, 2/10, 61023
e-mail: kdegt89@gmail.com;
https://orcid.org/0000-0002-4486-2468

Дорошенко Володимир Олексійович
д.ф.-м.н., професор; декан факультету інформаційно-аналітичних технологій та менеджменту,
Харківський національний університет радіоелектроніки, м. Харків, пр. Науки, 14, 61166
e-mail:volodymyr.doroshenko@nure.ua;
https://orcid.org/0000-0001-8454-394X

Крютченко Денис Володимірович
доктор філософії., молодший науковий співробітеик
Інститут проблем машинобудування ім. А.М. Підгорного НАН України, , м. Харків, вул. Комунальників, 2/10, 61023
e-mail: wollydenis@gmail.com;
https://orcid.org/0000-0003-6804-6991

Спектральна крайова задача для коаксіальних оболонок обертання

Основною метою цього дослідження є розробка ефективного чисельного підходу з використанням граничних елементів для оцінки власних частот коливань рідини у складених резервуарах. Проаналізовано власні коливання конструкцій оболонок, що включають циліндричні та конічні оболонки, поєднані кільцями. Область між оболонками заповнена ідеальною нестисливою рідиною. У числовому моделюванні використовуються метод суперпозиції у поєднанні з методом граничних елементів. Здійснено числовий розв'язок спектральної граничної задачі щодо коливань рідини в жорстких оболонкових конструкціях. Частоти і форми визначаються шляхом розв'язання систем сингулярних інтегральних рівнянь. Для оболонки обертання, ці системи спрощуються до одновимірних рівнянь, де інтеграли обчислюються вздовж кривих і відрізків прямих. Для обчислення одновимірних інтегралів із логарифмічними особливостями та особливостями типу Коші використовуються ефективні числові процедури. Тестові розрахунки підтверджують високу точність і ефективність запропонованого методу. Важливість і практична значимість методу полягає в можливості досліджувати коливання рідини в реальних складених паливних баках ракет-носіїв за різні умови навантаження.

Ключові слова: *циліндрично-конічні резервуари, системи сингулярних інтегральних рівнянь .метод граничних елементів, плескання рідини.*

Як цитувати: Гнітько В. І., Дегтярьов К.Г., Дорошенко В.О., Крютченко Д.В. Спектральна крайова задача для коаксіальних оболонок обертання. *Вісник Харківського національного університету імені В.Н.Каразіна, серія Математичне моделювання. Інформаційні технології. Автоматизовані системи управління*. 2023. вип. 60. С.6-14. https://doi.org/10.26565/2304-6201-2023-60-01

How to quote: V.I. Gnitko, K.G. Degtyarev, V.O. Doroshenko and D.V. Kriutchenko, “Spectral boundary value problem for coaxial shells of revolution”, *Bulletin of V.N. Karazin Kharkiv National University, series Mathematical modelling. Information technology. Automated control systems*, vol. 60, pp.6-14, 2023. https://doi.org/10.26565/2304-6201-2023-60-01 [In Ukrainian].

1 Вступ

Оболонки обертання як резервуари для зберігання рідини. широко використовуються на об'єктах водопостачання, нафти і газу, в різних галузях промисловості, в ядерних установок для зберігання різноманітних рідких або подібних до них матеріалів, хімічної рідини та різних відходів. При діє раптово прикладених зовнішніх навантажень в частково заповнених резервуарах відбуваються інтенсивні плескання вільної поверхі. Плескання означає будь-який рух вільної

поверхні рідини всередині контейнера. Це явище має значний вплив на динамічний відгук контейнера. Спектральна крайова проблема для резервуарів з рідиною полягає в знаходженні власних частот та форм плескань вільної поверхні. Розрахунок гідродинамічних сил на стінки резервуарів з рідиною є важливою проблемою для забезпечення міцності та стійкості руху промислових резервуарів і посудин. Основні проблеми при вивченні рідини полягають в оцінці розподілу гідродинамічного тиску, сил, моментів і визначенні власних частот вільної поверхні рідини. Ці параметри безпосередньо впливають на динамічну стійкість і міцність контейнерів. Хоча лише натурний експеримент може надати адекватну оцінку міцності резервуарів з рухомою рідиною, але проведення таких повномасштабних експериментів є коштовною та небезпечною процедурою, тому на передній фланг в сучасних наукових дослідженнях виходить комп'ютерне моделювання.

2 Постановка проблеми та огляд сучасного стану питання

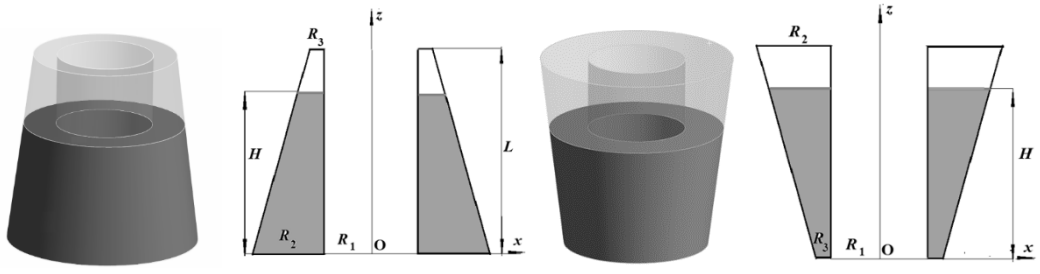
Проблема коливань рідини є викликом для різних галузей промисловості, таких як авіакосмічна, хімічна, машинобудівна, ядерна інженерія, а також складним завданням для фізиків та математиків. Коливання рідини може призводити до катастрофічних пошкоджень резервуарів для зберігання води та нафти, сходженню з розрахункової траєкторії ракет-носіїв. Завдяки потенційно небезпечному впливу, плескання рідини в резервуарах є об'єктом багатьох теоретичних та експериментальних досліджень протягом останніх кількох десятиліть [1-3]. Багато важливих явищ було розглянуто в цих дослідженнях, особливо лінійні та нелінійні ефекти плескання як для нев'язкої, так і для в'язкої рідини [4-6]. Загальний огляд існуючих підходів до проблеми плескань зроблено в [7-9]. Зауважимо, що хоча складені оболонки обертання є типовими конструкціями паливних баків ракет-носіїв, резервуарів, що використовуються в автомобільній, хімічній та сільськогосподарській галузях, в науковій літературі вивченню коливань таких резервуарів приділено недостатньо уваги [10-12].

Тому дане дослідження, присвячене розв'язанню спектральної крайової задачі щодо коливань рідини в складених оболонках обертання, виконано на актуальну тему.

3 Мета дослідження та формулювання задачі

Мета дослідження полягає в розробці комп'ютерної технології на основі поєднання методів суперпозицій мод та граничних елементів для оцінки власних частот та форм коливань рідини в складених оболонкових конструкціях.

Розглянуто складені оболонки обертання, частково заповнені рідиною, рис.1(а-б). Як S_1 будемо позначена змочену поверхню оболонкової конструкції, тоді як S_0 є вільною поверхнею рідини. Вважається, що рідина ідеальна і нестислива.



а) *б)*

Рис. 3.1. Складені оболонкові конструкції та їх схеми

Резервуари, що розглядаються, складаються з коаксіальних циліндричної та конічної оболонок, з'єднаних кільцями, що утворюють днища.. Рідина знаходиться між оболонками. Поверхні оболонок і днищ змочуються, а вільна поверхня в спокої знаходиться на висоті H, утворюючи кільце, яке описується в полярній системі координат таким чином: $\{z = H, R_1 < r < R_0\}$. Тут $R_0 = R_3 + (R_2 - R_3)(L - H)/L$ для оболонкової конструкції, що зображена на рис. 1а), а для конструкції 1б) маємо $R_0 = R_3 + (R_2 - R_3)H/L$.

Припустимо, що рух рідини, яка знаходиться між оболонками, є безвихровим. Позначимо як $\mathbf{V}(V_x, V_y, V_z)$ вектор швидкості рідини, тоді умова нестисливості приймає вигляд $\mathrm{div}\mathbf{V} = 0$. Умова потенційності руху означає, що існує скалярний потенціал швидкостей Ф, такий що $\mathbf{V} = \mathrm{grad}\Phi$.

Х цих припущень випливає, що потенціал Ф задовольняє рівнянню Лапласа в області, що зайнята рідиною. Нехай Ω – область, що зайнята рідиною, **P** – точка всередині області Ω .Тиск рідини p на змочені поверхні оболонки визначається з інтегралу Бернуллі за формулою

$$\frac{p}{\rho_l} = -\frac{\partial \Phi}{\partial t} - gz + \frac{p_0}{\rho_l}, \tag{3.1}$$

де ρ_l – густина рідини, g – прискорення вільного падіння, z – вертикальна координата точки **P**.

Сформулюємо граничні умови для рівняння Лапласа для знаходження потенціалу Ф. На змочених поверхнях S_1 має виконуватись умова непротікання, в той час як на вільній поверхі ставимо динамічні і кінематичні умови [13]. Умова непротікання має вигляд

$$\left.\frac{\partial \Phi}{\partial \boldsymbol{n}}\right|_{S_1} = 0. \tag{3.2}$$

На вільній поверхні виконуються кінематична та динамічна умови

$$\left.\frac{\partial \Phi}{\partial \boldsymbol{n}}\right|_{S_0} = \frac{\partial \zeta}{\partial t}; \quad p - p_0|_{S_0} = 0, p - p_0 = -\rho\left(\frac{\partial \Phi}{\partial t} + g\zeta\right). \tag{3.3}$$

Тут p – тиск рідини на змочені поверхні, p_0 – атмосферний тиск, ρ - густина рідини, g – прискорення вільного падіння, $\zeta=\zeta(x, y, t)$ – заздалегідь невідома функція, яка описує положення та рух вільної поверхні. Область, яку займає рідина, позначимо як Ω, а як **P** – точки всередині Ω.

Таким чином, для рівняння Лапласа сформульована крайова задача

$$\nabla^2\Phi = 0, \mathbf{P}\in\Omega, \frac{\partial \Phi}{\partial \mathbf{n}} = 0, \ \mathbf{P}\in S_1, \ \frac{\partial \Phi}{\partial \mathbf{n}} = \frac{\partial \zeta}{\partial t}, p - p_0 = 0, \ \mathbf{P}\in S_0 \tag{3.4}$$

відносно невідомого потенціалу Ф, що пов'язаний кінематичною граничною умовою з функцією $\zeta(x, y, t)$.

4 Метод заданих форм

Оскільки розглядаються оболонки обертання та внаслідок лінійності співвідношень (3.4) зобразимо невідомі функції Ф та ζ в циліндричних координатах у вигляді наступних рядів:

$$\zeta(r, \theta, t) = \sum_{l=0}^{m} \cos(l\theta) \sum_{k=1}^{n} d_{kl}(t)\zeta_k(r), \tag{4.1}$$

$$\Phi(r, \theta, z, t) = \sum_{l=0}^{m} \cos(l\theta) \sum_{k=1}^{n_2} \dot{d}_{kl}(t)\varphi_k(r, z) \tag{4.2}$$

При цьому буде виконана кінематична умова, якщо між базисними функціями $\varphi_k(r, z)$ та $\zeta_k(r)$ на вільній поверхні існує такий зв'язок:

$$\left.\frac{\partial \varphi_k(r,z)}{\partial \mathrm{n}}\right|_{z=H} = \zeta_k(r). \tag{4.3}$$

Функції $\psi_{kl} = \varphi_{kl}(r, z)\cos(l\,\theta)$ мають задовольняти рівнянню Лапласа.

З динамічної та кінематичної умов маємо

$$\frac{\partial \Phi}{\partial t} = -g\zeta, \quad \frac{\partial^2 \Phi}{\partial t^2} = -g\frac{\partial \zeta}{\partial t} = -g\frac{\partial \Phi}{\partial \mathbf{n}}. \tag{4.4}$$

Припускаючи гармонічний характер зміни коефіцієнтів $d_{kl}(t)$ за часом $d_{kl}(t) = D_{kl}\exp(i\omega_{kl}t)$, отримаємо з (4.4)

$$\frac{\partial \psi_{kl}}{\partial \mathbf{n}} = \frac{\omega_{kl}^2}{g}\psi_{kl}. \tag{4.5}$$

Таким чином, сформульовано спектральну крайову задачу відносно ψ_{kl} [14]

$$\nabla^2\psi_{kl} = 0, \mathbf{P}\in\Omega\,, \frac{\partial\psi_{kl}}{\partial\mathbf{n}} = 0,\ \mathbf{P}\in S_1,\ \frac{\partial\psi_{kl}}{\partial\mathbf{n}} = \frac{\omega_{kl}^2}{g}\ \psi_{kl},\ \mathbf{P}\in S_0. \tag{4.6}$$

Для розв'язання спектральної крайової задачі застосовано метод граничних елементів (МГЕ).

Зауважимо, що в поданнях (4.1)-(4.2) можна також використовувати множники $\sin(l\theta)$.

5 Метод граничних елементів

Для застосування методу граничних елементів в прямому формулюванні використовуємо третю формулу Гріна [15]

$$2\pi\psi_{kl}(\mathbf{P}_0) = \iint_S \frac{\partial\psi_{kl}}{\partial\mathbf{n}}\frac{1}{|\mathbf{P}-\mathbf{P}_0|}dS - \iint_S \psi_{kl}\frac{\partial}{\partial\mathbf{n}}\frac{1}{|\mathbf{P}-\mathbf{P}_0|}dS, \tag{5.1}$$

де $|\mathbf{P}-\mathbf{P}_0|$ – декартова відстань між точками $\mathbf{P}, \mathbf{P}_0$, $S = S_1 \cup S_0$. З використанням крайових умов спектральної задачі (4.6) отримуємо

$$2\pi\psi_{kl} + \iint_{S_1}\psi_{kl}\frac{\partial}{\partial\mathbf{n}}\left(\frac{1}{|\mathbf{P}-\mathbf{P}_0|}\right)dS_1 - \frac{\omega_{kl}^2}{g}\iint_{S_0}\frac{\psi_{kl}}{|\mathbf{P}-\mathbf{P}_0|}dS_0 + \iint_{S_0}\psi_{kl}\frac{\partial}{\partial\mathbf{n}}\left(\frac{1}{|\mathbf{P}-\mathbf{P}_0|}\right)dS_0 = 0, \mathbf{P}_0\in S_1,$$

$$2\pi\psi_{kl} + \iint_{S_1}\psi_{kl}\frac{\partial}{\partial\mathbf{n}}\left(\frac{1}{|\mathbf{P}-\mathbf{P}_0|}\right)dS_1 + \frac{\omega_{kl}^2}{g}\iint_{S_0}\frac{\psi_{kl}}{|\mathbf{P}-\mathbf{P}_0|}dS_0 = 0, \mathbf{P}_0\in S_0. \tag{5.2}$$

У разі оболонок обертання та з використанням подання $\psi_{kl} = \varphi_{kl}(r,z)\cos(l\,\theta)$ приходимо до одновимірної системи сингулярних інтегральних рівнянь у вигляді

$$2\pi\varphi_{kl}(r_0,z_0) + \int_\Gamma \varphi_{kl}(r(z),z)\Theta\,(z,z_0)r(z)d\Gamma - \frac{\omega_{kl}^2}{g}\int_0^R \varphi_{kl}(\rho,H)\Xi(\mathbf{P},\mathbf{P}_0)\rho d\rho = 0, \mathbf{P}_0\in S_1, \tag{5.3}$$

$$2\pi\varphi_{kl}(r_0,H) + \int_\Gamma \varphi_{kl}(r(z),z)\Theta\,(z,z_0)r(z)d\Gamma - \frac{\omega_{kl}^2}{g}\int_0^R \varphi_{kl}(\rho,H)\,\Xi(\mathbf{P},\mathbf{P}_0)\rho d\rho = 0, \mathbf{P}_0\in S_0.$$

$$\Theta(z,z_0) = \frac{4}{\sqrt{a+b}}\left\{\frac{1}{2r}\left[\frac{r^2-r_0^2+(z_0-z)^2}{a-b}E_l(k) - F_l(k)\right]n_r + \frac{z_0-z}{a-b}E_l(k)n_z\right\},$$

$$\Xi(P,P_0) = \frac{4}{\sqrt{a+b}}F_l(k),\ a = r^2+r_0^2+(z-z_0)^2,\ b = 2rr_0.$$

В (5.3) введені узагальнені еліптичні інтеграли за формулами

$$E_l(k) = (-1)^l(1-4l^2)\int_0^{\pi/2}\cos 2\,b_1 l\theta\sqrt{1-k^2\sin^2\theta}\,d\theta, \tag{5.4}$$

$$F_l(k) = (-1)^l\int_0^{\pi/2}\frac{\cos 2b_1 l\theta d\theta}{\sqrt{1-k^2\sin^2\theta}}d\theta, \quad k^2 = 2b/(a+b). \tag{5.5}$$

Для обчислення інтегралів (5.4)-(5.5) використовується метод, запропонований в [16], заснований на використанні середнього арифметико-геометричного значення. Для розв'язання системи сингулярних рівнянь (5.3) застосовується метод граничних елементів зі сталою апроксимацією густини вздовж елементу [13], [17].

6 Аналіз числових результатів

Для тестування запропонованого методу здійснено порівняння отриманих числових результатів з даними, наведеними в [18]. Як і в [18], розглядаються як V-подібні, так і Λ-подібні конічні резервуари з R_1 = 1м і α = π/3 з рідиною. Вважаємо, що R_2 менший радіус конуса.

Розглянуті перші частоти з хвильовими числами l= 0, 1, 2, оскільки вони є найнижчими власними частотами, що визначають гідродинамічне навантаження. Результати порівняння надані в таблиці 6.1. для різних значень R_2

При числових розрахунках обиралось 120 граничних елементів вздовж конічної частити, 100 елементів вздовж радіусу вільної поверхні, та 100 елементів вздовж радіусу днища. Подальше збільшення кількості елементів не привело до суттєвої зміни результатів.

Результати, отримані запропонованим одновимірним МГЕ, гарно узгоджуються з даними [18]. Деяка розбіжність даних спостерігається при R_2=0.2м для Λ-подібних конічних резервуарів. При цьому, в [18] зроблено зауваження відносно невисокої точності полу-аналітичного методу саме в цьому випадку.

Надалі саме 120 граничних елементів використовується вздовж як циліндричної, так і конічної поверхонь для дослідження коливань рідини в коаксіальних оболонках.

Таблиця 6.1. Частоти плескань в конічних резервуарах

	V-подібні					Λ-подібні				
R_2,м	0.2	0.4	0.6	0.8	0.9	0.2	0.4	0.6	0.8	0.9
l =0, k =1										
[18]	3.386	3.386	3.382	3.139	2.187	24.153	10.014	6.665	4.550	2.683
МГЕ	3.389	3.390	3.391	3.192	2.200	20.027	10.034	6.669	4.545	2.678
l =1, k =1										
[18]	1.304	1.302	1.254	0.934	0.542	11.332	5.629	3.515	1.661	0.726
МГЕ	1.305	1.307	1.259	0.954	0.574	11.303	5.626	3.481	1.651	0.732
l =2, k =1										
[18]	2.263	2.263	2.255	2.015	1.361	17.760	8.967	5.941	3.724	1.923
МГЕ	2.265	2.270	2.269	2.048	1.394	17.939	8.965	5.941	3.726	1.951

Далі розв'язана спектральна гранична задача (4.6), що дозволило знайти форми $\varphi_k(r,\theta,z)$ та відповідні їм фундаментальні частоти для конструкцій, зображених на рис.1.

Специфіка цих конструкцій полягає в тому, що вільна поверхня має форму кільця. Таку ж саме форму має вільна поверхня в при розгляданні тороїдальних оболонок, плескання рідини в таких оболонках досліджено в [11].

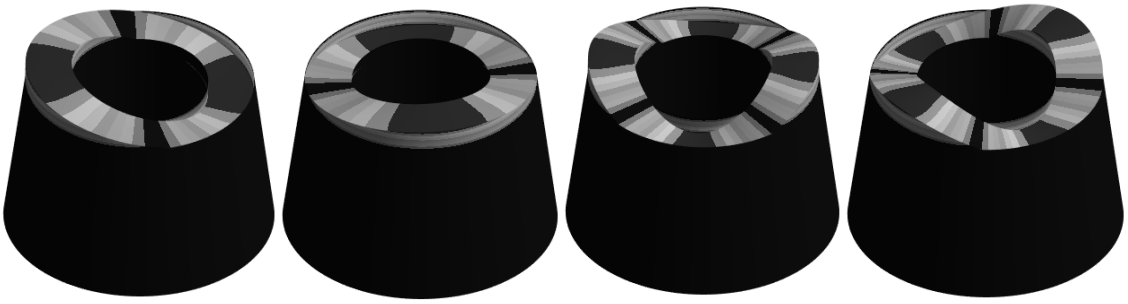
Значення нижчих восьмі частот плескань коаксіальних циліндрично-конічних оболонкових конструкцій наведені в таблиці 6.2.

Таблиця 6.2. Частоти плескань рідини в коаксіальних оболонках, Гц

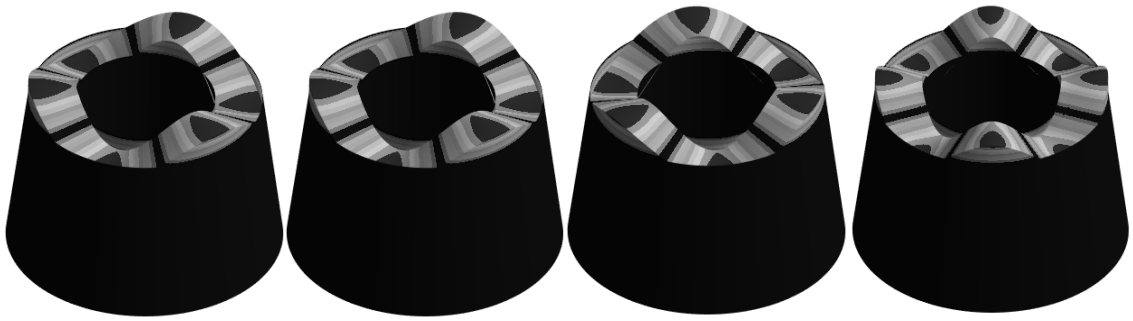
№	1	2	3	4	5	6	7	8
Оболонкова конструкція, рис.1а)								
частота	0,6277	0,6277	0,8892	0,8892	1,0779	1,0779	1,2355	1,2355
Оболонкова конструкція, рис.1б)								
частота	0,5512	0,5512	0,8153	0,8153	1,0027	1,0027	1,1548	1,1548

Зауважимо, що наявні кратні частоти плескань. Вони відповідають множнику $\sin(l\,\theta)$ в рівняннях (4.1)-(4.2). Відповідні форми плескань вільної поверхні зображені на рис. 6.1-6.2. Частоти плескань обох конструкцій відрізняються незначно, але для конструкцій з меншим радіусом вільної поверхні вони є більшими. Ця різниця зменшується із зростанням хвильового числа.

Найнижчі частоти відповідають першому, другому та третьому хвильовим числам. Це відповідає даним розрахунків, наведеним а роботах [5,7,10], стосовно плескань рідини в конічних та циліндричних оболонках.

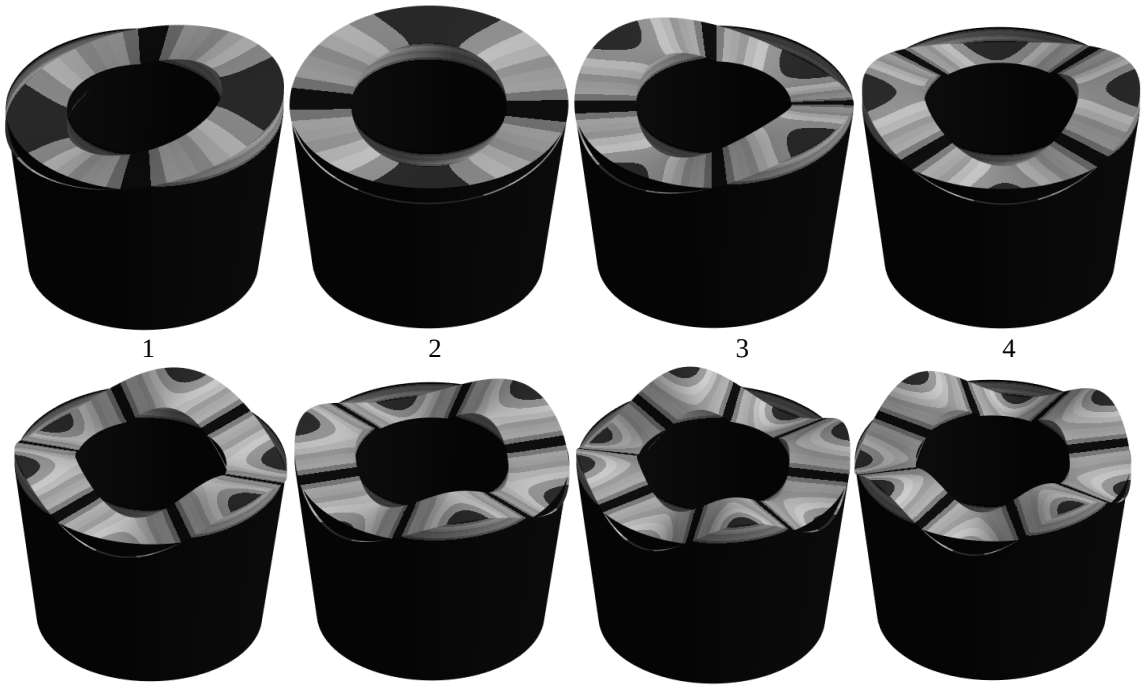


1 2 3 4



5 6 7 8

Рис. 6.2 Форми плескань $\varphi_k(r,\theta,H)$ вільної поверхні конструкції 1а).



1 2 3 4

5 6 7 8

Рис. 6.3 Форми плескань $\varphi_k(r,\theta,H)$ вільної поверхні конструкції 1б).

Таким чином, розв'язано спектральну задачу щодо визначення частот та форм коливань рідини в коаксіальних оболонкових конструкціях. Це дає змогу дослідити рух рідини в паливних баках та резервуарах при дії зовнішніх навантажень.

Висновки

Запропоновано метод визначення частот ти форм коливань рідини в складених оболонках обертання. Метод граничних елементів вперше застосовано для розв'язання спектральної крайової задачі в складених оболонках обертання. Цей підхід буде використовуватись при комп'ютерному моделюванні динамічної поведінки резервуарів з рідиною та дослідженні стійкості руху рідини в паливних баках ракет-носіїв складної форми. У подальшому передбачається дослідження коливань пружних коаксіальних оболонок з рідиною, з використанням різних композитних матеріалів [19].

СПИСОК ЛІТЕРАТУРИ

1. Gnitko V., Naumenko V., Rozova L. & Strelnikova E. Multi-Domain Boundary Element Method for Liquid Sloshing Analysis of Tanks with Baffles. *Journal of Basic and Applied Research International*, Vol. 17(1), P. 75–87. 2016. https://www.ikppress.org/index.php/JOBARI/article/view/3788

2. Balas O.-M., Doicin C. V. and Cipu E. C. Analytical and Numerical Model of Sloshing in a Rectangular Tank Subjected to a Braking, *Mathematics*, Vol. 11, P. 949-955, 2023. DOI:10.3390/math11040949
3. Liu J., Zang Q., Ye W., Lin G. High performance of sloshing problem in cylindrical tank with various barrels by isogeometric boundary element method, *Engineering Analysis with Boundary Elements*, Vol.114, P.148-165, 2020. DOI:10.1016/j.enganabound.2020.02.014.
4. Gnitko V., Karaiev A., Degtyariov K., Strelnikova E. Singular boundary method in a free vibration analysis of compound liquid-filled shells, *WIT Transactions on Engineering Sciences*, Vol.126, P.189-200, 2019. WIT Press, DOI:10.2495/BE420171.
5. Strelnikova E., Kriutchenko D., Gnitko V. Tonkonozhenko A. Liquid Vibrations in Cylindrical Tanks with and Without Baffles Under Lateral and Longitudinal Excitations. *International Journal of Applied Mechanics and Engineering*, Vol. 25(3), P.117-132, 2020. DOI:10.2478/ijame-2020-0038
6. Tong, C. Shao Y., Bingham H. B. & Hanssen, FC. W. An Adaptive Harmonic Polynomial Cell Method with Immersed Boundaries: Accuracy, Stability and Applications. *International Journal for Numerical Methods in Engineering*, Vol. 122, P. 2945–2980, 2021. https://doi.org/10.1002/nme.6648
7. 1brahim R. A., *Liquid Sloshing Dynamics. Theory and Applications*. Cambridge University Press, 984 p., 2005.
8. Pradeepkumar K., Selvan V., Satheeshkumar K. Review of Numerical Methods for Sloshing. *International Journal for Research in Applied Science & Engineering Technology*. Vol.8, Issue XI, 2020, doi.org/10.22214/ijraset.2020.32116.
9. Zheng Jh., Xue, MA., Dou, P. et al. A review on liquid sloshing hydrodynamics. *J Hydrodyn* Vol. 33, P. 1089–1104, 2021. https://doi.org/10.1007/s42241-022-0111-7
10. Strelnikova E., Kriutchenko D., Gnitko V. Liquid Vibrations in Cylindrical Quarter Tank Subjected to Harmonic, Impulse and Seismic Lateral Excitations. *Journal of Mathematics and Statistical Science*. Vol.5, P. 31-41, 2019. http://www.ss-pub.org › 2019/03 › JMSS18122001.
11. Karaiev A., Strelnikova E. Liquid Sloshing in Circular Toroidal and Coaxial Cylindrical Shells. *In: Ivanov, V., Pavlenko, I.,* Liaposhchenko, *O., Machado, J., Edl, M. (eds) Advances in Design, Simulation and Manufacturing III. DSMIE 2020. Lecture Notes in Mechanical Engineering. Springer, Cham.* 2020. https://doi.org/10.1007/978-3-030-50491-5_1
12. Murawski K. Technical Stability of Very Slender Rectangular Columns Compressed by Ball-And-Socket Joints without Friction, *Int. Journal of Structural Glass and Advanced Materials Research*, Vol. 4(1), P. 186-208, 2020. DOI: 10.3844/sgamrsp.2020.186.208
13. Krutchenko D. V., Strelnikova E. A., Shuvalova Y. S. Discrete singularities method in problems of seismic and impulse impacts on reservoirs. *Вісник Харківського національного університету імені В.Н. Каразіна, сер. «Математичне моделювання. Інформаційні технології. Автоматизовані системи управління»*, вип. 35, С. 31-37, 2017, http://lib.kart.edu.ua/bitstream/123456789/13113/1/Krutchenko.pdf.
14. Raynovskyy I. A. and Timokha A. N. Sloshing in Upright Circular Containers: Theory, Analytical Solutions, and Applications. 155p., 2020. CRC Press/Taylor and Francis Group, https://doi.org/10.1201/9780429356711
15. Brebbia, C.A. The birth of the boundary element method from conception to application. *Engineering Analysis With Boundary Elements*, Vol. 77, P. iii-x, 2017. https://doi.org/10.1016/j.enganabound.2016.12.001.
16. Karaiev, A, Strelnikova, E. Axisymmetric polyharmonic spline approximation in the dual reciprocity method. *Z Angew Math Mech*. Vol. 101, e201800339, 2021. DOI:10.1002/zamm.201800339.
17. Naumenko V., Strelnikova H. Singular integrals accuracy of calculations in two-dimensional problems using boundary element methods, *Engineering Analysis with Boundary Elements*, Vol. 26, Issue 1, P. 95-98, 2002. https://doi.org/10.1016/S0955-7997(01)00041-8.
18. Gavrilyuk I., Hermann M., Lukovsky I., Solodun O., Timokha A. Natural Sloshing frequencies in Truncated Conical Tanks, *Engineering Computations*, Vol. 25, no. 6, P. 518 – 540, 2008. DOI: 10.1108/02644400810891535
19. Sierikova O, Strelnikova E, Gnitko V, Degtyarev K. Boundary Calculation Models for ElasticProperties Clarification of Three-dimensional Nanocomposites Based on the Combination of Finite and Boundary Element Methods. *IEEE 2nd KhPI Week on Advanced Technology (KhPIWeek)* P. 351–356. 2021. doi: 10.1109/KhPIWeek53812.2021.9570086

REFERENCES

1. V. Gnitko, V. Naumenko, L Rozova. & E. Strelnikova, "Multi-Domain Boundary Element Method for Liquid Sloshing Analysis of Tanks with Baffles". *Journal of Basic and Applied Research International*, 2016, Vol. 17(1), P. 75–87, https://www.ikppress.org/index.php/JOBARI/article/view/3788
2. O.-M., Balas C. V. Doicin and E. C. Cipu, "Analytical and Numerical Model of Sloshing in a Rectangular Tank Subjected to a Braking", *Mathematics*, 2023, Vol. 11, P. 949-955, DOI:10.3390/math11040949
3. J. Liu Q. Zang, W. Ye, G. Lin, "High performance of sloshing problem in cylindrical tank with various barrels by isogeometric boundary element method", *Engineering Analysis with Boundary Elements*, 2020, Vol. 114, P. 148-165, DOI:10.1016/j.enganabound.2020.02.014
4. V. Gnitko, A. Karaiev, K.Degtyariov, E.Strelnikova, "Singular boundary method in a free vibration analysis of compound liquid-filled shells", *WIT Transactions on Engineering Sciences*, 2019, Vol. 126, P. 189-200, WIT Press, DOI:10.2495/BE420171.
5. E. Strelnikova, D. Kriutchenko, V. Gnitko, A. Tonkonozhenko, "Liquid Vibrations in Cylindrical Tanks with and Without Baffles Under Lateral and Longitudinal Excitations", *International Journal of Applied Mechanics and Engineering*, Vol. 25, Issue 3, P. 117-132, 2020, DOI: 10.2478/ijame-2020-0038.
6. C.Tong, Y. Shao, H. B. Bingham, & FC. W. Hanssen, "An Adaptive Harmonic Polynomial Cell Method with Immersed Boundaries: Accuracy, Stability and Applications. *International Journal for Numerical Methods in Engineering*, 2021, Vol. 122, P. 2945–2980. https://doi.org/10.1002/nme.6648
7. R. A. 1brahim, *Liquid Sloshing Dynamics. Theory and Applications*. Cambridge University Press. 2005, 984 p.
8. K. Pradeepkumar, V. Selvan, K.Satheeshkumar, "Review of Numerical Methods for Sloshing", *International Journal for Research in Applied Science & Engineering Technology*, Vol. 8, Issue XI, 2020, doi.org/10.22214/ijraset.2020.32116.
9. Jh. Zheng, MA. Xue, P. Dou, et al. " A review on liquid sloshing hydrodynamics. *J Hydrodyn* 2021, Vol. 33, P. 1089–1104. https://doi.org/10.1007/s42241-022-0111-7
10. E. Strelnikova, D. Kriutchenko, V. Gnitko, "Liquid Vibrations in Cylindrical Quarter Tank Subjected to Harmonic, Impulse and Seismic Lateral Excitations", *Journal of Mathematics and Statistical Science*, 2019, Vol. 5, P. 31-41. http://www.ss-pub.org › 2019/03 › JMSS18122001.
11. A. Karaiev, E. Strelnikova, "Liquid Sloshing in Circular Toroidal and Coaxial Cylindrical Shells", In: Ivanov, V., Pavlenko, I., Liaposhchenko, O., Machado, J., Edl, M. (eds) Advances in Design, Simulation and Manufacturing III. DSMIE 2020. Lecture Notes in Mechanical Engineering. Springer, Cham, 2020, https://doi.org/10.1007/978-3-030-50491-5_1
12. K. Murawski, "Technical Stability of Very Slender Rectangular Columns Compressed by Ball-And-Socket Joints without Friction", *Int. Journal of Structural Glass and Advanced Materials Research*, 2020, Vol. 4(1), P. 186-208, DOI: 10.3844/sgamrsp.2020.186.208.
13. D. V. Krutchenko, E. A. Strelnikova, Yu. S. Shuvalova, " Discrete singularities method in problems of seismic and impulse impacts on reservoirs", *Bulletin of VN Karazin Kharkiv National University, series «Mathematical modeling. Information technology. Automated control systems»,* 2017, vol. 35, P. 31-37. http://lib.kart.edu.ua/bitstream/123456789/13113/1/Krutchenko.pdf.
14. I. A. Raynovskyy and A. N. Timokha, *Sloshing in Upright Circular Containers: Theory, Analytical Solutions, and Applications*. CRC Press/Taylor and Francis Group, 155p., 2020. https://doi.org/10.1201/9780429356711
15. C.A Brebbia, "The birth of the boundary element method from conception to application", *Engineering Analysis With Boundary Elements*, 2017. vol. 77, pp. iii-x, https://doi.org/10.1016/j.enganabound.2016.12.001.
16. A. Karaiev, E. Strelnikova, "Axisymmetric polyharmonic spline approximation in the dual reciprocity method". Z *Angew Math Mech*. Vol. 101, e201800339, 2021. DOI:10.1002/zamm.201800339.
17. V. Naumenko, H. Strelnikova, "Singular integrals accuracy of calculations in two-dimensional problems using boundary element methods", *Engineering Analysis with Boundary Elements*, Vol. 26 (1), P. 95-98, 2002. https://doi.org/10.1016/S0955-7997(01)00041-8.

18. I. Gavrilyuk, M. Hermann, I. Lukovsky, O. Solodun, A. Timokha, “Natural Sloshing frequencies in Truncated Conical Tanks”, *Engineering Computations*, Vol. 25, no. 6, P. 518 – 540, 2008. DOI: 10.1108/02644400810891535
19. O. Sierikova, E. Strelnikova, V. Gnitko, K Degtyarev, “Boundary Calculation Models for ElasticProperties Clarification of Three-dimensional Nanocomposites Based on the Combination of Finite and Boundary Element Methods”, IEEE 2nd KhPI Week on Advanced Technology (KhPIWeek), P. 351–356, 2021.DOI: 10.1109/KhPIWeek53812.2021.9570086

Gnitko Vasyl *PhD, senior researcher*
A. Pidhorny Institute of Mechanical Engineering Problems
vul. Pozharskogo, 2/10, Kharkiv, 61046, Ukraine,
Degtyarev Kirill *PhD, researcher*
A. Pidhorny Institute of Mechanical Engineering Problems
vul. Pozharskogo, 2/10, Kharkiv, 61046, Ukraine
Doroshenko Volodymir *DSc, Ptofessor*
Kharkiv National University of Radio Electronics
Nauky Ave, 14, Kharkiv, 61166, Ukraine
Krutchenko Denys *PhD, junior researcher*
A. Pidhorny Institute of Mechanical Engineering Problems
vul. Pozharskogo, 2/10, Kharkiv, 61046, Ukraine

Spectral boundary value problem for coaxial shells of revolution

The main objective of this study is to develop an efficient numerical approach using boundary elements to estimate natural frequencies of liquid vibrations in composite tanks. The spectral boundary value problem for liquid tanks is to find the natural frequencies and modes of free surface sloshing. The calculation of hydrodynamic forces on the walls of tanks with liquid is an important problem for ensuring the strength and stability of movement of industrial tanks and vessels. The vibrations of shell structures, including cylindrical and conical shells connected by rings, are analyzed. The area between the shells is filled with an ideal incompressible fluid. Numerical modeling uses the superposition method in combination with the boundary element method. A numerical solution of the spectral boundary value problem regarding fluid vibrations in rigid shell structures has been carried out. Frequencies and modes are determined by solving systems of singular integral equations. For the shells of revolution, these systems are simplified to one-dimensional equations, where the integrals are calculated along curves and line segments. Efficient numerical procedures are used to calculate one-dimensional integrals with logarithmic and Cauchy features. Test calculations confirm the high accuracy and efficiency of the proposed method. The importance and practical significance of the method lies in the ability to study fluid fluctuations in real compound fuel tanks of launch vehicles under different load conditions. This makes it possible to study the movement of liquid in fuel tanks and reservoirs under the action of external loads. The elaborated method will be used in computer modeling the dynamic behavior of liquid tanks and the stability study of liquid movement in compound fuel tanks of launch vehicles. In the future, it is planned to study the vibrations of elastic coaxial shells with liquid, using various composite materials.

Keywords: *cylindrical-conical tanks, systems of singular integral equations, boundary element method, liquid sloshing.*

Надійшла у першій редакції 08.10.2023, в останній – 12.11.2023.
The first version has been received on 08.10.2023, the final version – on 12.11.2023.

DOI: https://doi.org/10.26565/2304-6201-2023-60-02

УДК 681.3

Деменкова Світлана Дмитрівна *старший викладач кафедри автоматизації хіміко-технологічних систем та екологічного моніторингу, Національний технічний університет Харківський політехнічний інститут, Харків, вул.. Кирпичова,2, 61002*
e-mail: svet1972232765@gmail.com
https://orcid.org/[0000-0003-0604-5456]

Демченко Катерина Вікторівна *к.т.н., доцент, доцент кафедри автоматизації та комп'ютерно-інтегрованих технологій Державний біотехнологічний університет, вул. Алчевських 44, м. Харків, Україна, 61002*
e-mail: yayaska@btu.kharkiv.ua
https://orcid.org/0000-0002-3168-5351

Корольова Яна Юріївна *к.т.н., доцент кафедри мультимедійних та інтернет технології і системи, Національний технічний університет Харківський політехнічний інститут, Харків, вул.. Кирпичова,2, 61002*
e-mail: yanakoroleva815@gmail.com
https://orcid.org/[0000-0003-0604-5456]

Пахомов Юрій Васильович *к.т.н., доцент кафедри комп'ютерних наук та інформаційних технологій Харківський національний університет міського господарства імені О.М. Бекетова, м. Харків, вул. Маршала Бажанова, 17, Україна, 61002*
e-mail: abc050073@gmail.com
https://orcid.org/0000-0002-2267-8600

Використання метода пошуку аномалій для виявлення мережевих атак

Стаття присвячена опису моделі виявлення мережевих вторгнень у трафіку мереж, побудованих з урахуванням стека протоколів TCP/IP. Аналізуються основні об'єкти локальної обчислювальної мережі. Описуються основні контрольовані параметри кожного типу об'єктів. У роботі розробляються методи пошуку аномалій, що ґрунтуються як на аналізі за правилами, так і на аналізі з використанням імовірнісних моделей.

Актуальність. У зв'язку з інтенсивним зростанням інформаційних технологій та їх впровадженням у різні галузі діяльності міського господарства питання інформаційної безпеки виходить на перше місце і стає дуже актуальним.

Методи дослідження. Під час вирішення поставлених завдань використовувалися методи теорії управління; методи побудови систем захисту; теорія графів; теорія ймовірності та математична статистика; методи аналізу часових рядів; методи прогнозної аналітики та обробки великих даних; методи побудови високонавантажених захищених програм. Основними методами дослідження є імовірнісне і верифікаційне моделювання.

Результати. Імовірнісне і верифікаційне моделювання мережевих атак підтвердило працездатність запропонованого підходу. Результати синтезу за допомогою САПР показали, що додаткові апаратні витрати не перевищують 20% порівняно з канонічною моделлю опису.

Висновки. Розроблена модель системи дозволяє виявляти атаки на ключові об'єкти, що моделюються. Отримані під час випробувань результати показали високу ефективність виявлення аномалій числових параметрів моделі. Для збільшення точності надалі планується перейти до моделювання поняття «сервіс» та моделювання протоколів HTTP, SMTP, POP3. Модель сесії також дозволяє виявляти існуючі та нові атаки на рівні сесії TCP, а також деякі види атак на відмову в обслуговуванні. Модель потоків мережевого трафіку дозволяє нам виявляти такі види атак, як: різні види сканування системи, установку троянських програм (бо зросте кількість байт у вихідному потоці), установку ICMP шелла (бо зросте кількість ICMP пакетів). Модель часових інтервалів дозволяє виявляти деякі види сканування системи, атаки на відмову в обслуговуванні та встановлення web-шеллу. Стаття присвячена опису моделі виявлення мережевих вторгнень у трафіку мереж, побудованих з урахуванням стека протоколів TCP/IP. Аналізуються основні об'єкти локальної обчислювальної мережі. Описуються основні контрольовані параметри кожного типу об'єктів. Розробляються методи пошуку аномалій, що ґрунтуються як на аналізі за правилами, так і на аналізі з використанням імовірнісних моделей.

***Ключові слова**: пошук аномалій, мережеві атаки, скінчені автомати, верифікація, моделювання, розподілених інформаційних мережах, імовірнісне моделювання, верифікаційне моделювання*

Як цитувати: Деменкова С. Д, Демченко К. В., Корольова Я. Ю., Пахомов Ю. В. Використання метода пошуку аномалій для виявлення мережевих атак. *Вісник Харківського національного університету імені В.Н. Каразіна, серія Математичне моделювання. Інформаційні технології. Автоматизовані системи управління*. 2023. вип. 60. С.15-26.
https://doi.org/10.26565/2304-6201-2023-60-02

How to quote: Demenkova S., Demchenko K., Koroleva Y., Pakhomov Y., "Using anomaly detection method to detect network attack", *Bulletin of V.N. Karazin Kharkiv National University, series Mathematical modelling. Information technology. Automated control systems*, vol. 60, pp.15-26, 2023. https://doi.org/10.26565/2304-6201-2023-60-02 [In Ukrainian].

1 Вступ

Сучасні методики знаходження та знешкодження кібератак у комп'ютерних системах та мереж, а також виявлення кібератак є неформальними щодо моделі такої атаки, тому для них складно оцінити обчислювальну складність, коректність, завершеність тощо. Зазвичай роздають методи виявлення атак, та зловживань. Більшість комерційних комп'ютерних систем та мереж використовують сигнатурні (експертні) методи виявлення. В промислових системах рідка використовуються системи академічних розробок в області виявлення аномалій, тому, що вони породжують дуже велику кількість помилкових спрацьовувань [1].

2 Постановка задачі

Побудова розподілених інформаційних мереж (РІМ), стійких до комп'ютерних атак, пов'язана зі значними витратами часу та ресурсів. Забезпечення працездатності РІМ залежить від їх здатності протистояти цілеспрямованим впливам, що порушують їх роботу. Для РІМ основною проблемою є низька ефективність виявлення невідомих атак та захисту від внутрішнього порушника.

У зв'язку з інтенсивним зростанням інформаційних технологій та їх впровадженням у різні галузі діяльності міського господарства питання інформаційної безпеки стає дедалі **актуальнішим**. Сьогодні більшість промислових виробництв для захисту своїх корпоративних мереж використовує якісь різні методики захисту від вторгнень, а саме міжмережеві екрани, антивірусні системи та системи виявлення вторгнень. Системи виявлення вторгнень (СВВ) – це програмні або апаратно-програмні засоби, які автоматизують події та процес їх контролю, які проходять у комп'ютерній системі або мережі, і також самі аналізують події та знаходять ознаки порушення політики безпеки. Системи виявлення вторгнень на сьогоднішній день є одним із необхідних компонентів інфраструктури безпеки корпоративної мережі для більшості організацій міського господарства.

Сучасні РІМ характеризуються надвисокими обсягами інтенсивна надходить різнорідного мережевого трафіку, у зв'язку з чим **актуальним** є розгляд систем виявлення вторгнень (СВВ), спрямованих на обробку великих даних. Математичні аспекти побудови СВВ та моніторингу РІМ для визначення внутрішнього порушника на сьогоднішній день розроблені недостатньо, а механізми прихованого моніторингу та аналізу Великих даних існують окремо. Тому побудова розподілених систем виявлення вторгнень (РСВВ) з використанням методів прихованого моніторингу та аналізу великих даних є **актуальним**.

Системи виявлення атак, залежно від використовуваної технології виявлення атак, поділяють на дві основні групи: системи, які виявляють зловмисну поведінку та аномальну поведінку. Перші покладаються на модель зловмисної поведінки (наприклад, шаблон атаки) і порівнюють модель з потоком подій. Другі покладаються на модель нормальної поведінки (наприклад профіль системи) і шукають аномальні входження в потік подій. Незважаючи на широке поширення СВВ та активні дослідження в даній галузі, існуючі системи мають ряд недоліків [1]. Наприклад, нездатність виявлення нових видів атак.

У роботі **розглядаються** системи виявлення аномальної поведінки, оскільки ця технологія дозволяє виявляти нові види атак. **Метою роботи** є розроблення моделей виявлення атак у мережевому трафіку на основі виявлення аномалії заголовків мережевих пакетів.

3 Огляд літератури

В [1] наведені таки підходи, які класифікують методи, які виявляють аномалії у системах, які виявляють атаки. Також проведено аналіз та розгляд популярних групи методів виявлення аномалій та зазначено, що методи виявлення аномалій в системах виявлення атак не дуже формалізовані для побудови моделі атаки, та в них досить складно оцінити обчислювальну складність, коректність та завершеність.

У [2] розглядається можливість автоматизації процесу побудови мережевих графіків за допомогою підходу мультипаралельної обробки, який дозволяє перетворювати алгоритми лінійної дії в паралельні алгоритми. Метою даного дослідження є скорочення часу мережевого планування для виконання IT-проектів за рахунок використання методів мультипаралельної обробки.

У [3] наведені методи побудови гетерогенних комп'ютерних систем і мереж критичного застосування також були проаналізовані вимоги до цих систем, наведено перелік та зміст комп'ютерних технологій, розроблено новий метод автоматизованого проектування гетерогенних комп'ютерних систем та мереж критичного застосування.

У [4] проведено аналіз методів тестового діагностування двовимірних однорідних мереж (ОМ), запропоновано метод модифікації автоматної моделі мережі, що забезпечує С - тестування рядків та L - тестування стовпців мережі

У [5] запропоновано використовувати системи запобігання та виявлення вторгнень для того, щоб захист мережи був комплексний. Шляхом порівняння систем було наведено виявлено їх недоліки та вимоги для наближення до так званої супер системи по запобіганню та виявленню кібератак та вторгнень.

У [6] проведено аналіз характеристик виявлення мережевих вторгнень в інформаційну систему і виявлення ознак комп'ютерних атак на підприємстві; аналіз можливих дій зі сторони зловмисників, досліджено методи та принципи встановлення оптимальної системи виявлення мережевих вторгнень; розглянуто можливості розробки та використання комп’ютеризованих систем для виявлення вторгнень до мережі і властивостей комп’ютеризованих атак на підприємстві в сучасних умовах; досліджено і розроблено рекомендації щодо впровадження таких систем виявлення атак, вторгнень та ознак кібератак для можливого подальшого встановлення їх в систему захисту інформації будь-якої організації.

У зв’язку з тім, що збільшується кількість різних комп'ютерних мережевих загроз, які призводять до фінансових втрат організацій, то в [7] показано, що дуже важний напряв у інформаційної безпеки – це розробка систем пошуку атак в комп’ютеризованих мережах. Також показані основні існуючи методи вирішення задач по виявленню атак в мережі. Розглядаються роботи, які присвячені методу вейвлет-аналізу по виявленню аномалій в мережевому трафіку та показані отримані тестові дані мережевого трафіку з аномаліями для практичного виконання, також показано практичне виконання шумоусунення сигналу для конкретизації та зменшення розміру даних, використано різноманіття методів вейвлет-аналізу для виявлення можливості появи аномалій.

У [8] показано, що ніякі методи захисту від кібератак в мережі не дають гарантію від проникнення зловмисника в комп’ютерну мережу систему та у випадку злому потрібно швидко виявити та перервати доступ, провести розслідування та виправити дірки в безпеці. Для цього треба використовувати методи, які виявляють зловживання та аномалії. Були досліджени можливості використання частотного методу, який виявляє аномалії в роботі системи шляхом аналізу ентропії журналу подій та використовується для виявлення аномалій у трафіку комп’ютерної мережі, при цьому аномалії в журналі подій на хостах можуть вказувати для перевірки на наявність несанкціонованих дій також. Дослідження були проведені на основі журналу подій в ОС Windows та показали, що можна виявити перевищення порогів безпеки щодо кількості різних повідомлень в журналі подій шляхом аналізу ентропії. Це вказує на аномалії в роботі комп’ютерної мережі. Метод, який був запропоновану можна інтегрувати у системи виявлення вторгнень, які будуть сповіщати адміністратора безпеки про зловживання та атаки.

У [9] показано, що всі комп’ютерні системи та мережи використовують системи виявлення кібератак та вторгнень до комп’ютерних мереж та інформаційних систем. Зазвичай це можуть бути або програмні, або апаратно-програмні засоби, які автоматизують процес контролю подій в комп’ютерної системі або мережі, і аналізують події для пошуку проблем безпеки.

У зв’язку зі збільшенням несанкціонованих атак у комп’ютерні мережі, системи виявлення кібератак (СВА) є важливою частиною системи безпеки організації. Існують багато методів виявлення кібератак та аномалій, але їх стійкість слабка, відсутня верифікація, дуже багато хибних спрацьовувань, характер не допомагають їх широкому використанню. Запропоновано аналіз, можливості найпоширеного типу атак – DDoS, тобто атак типу, а саме - відмовляє обслуговувати, шхяхом переривання або призупинення роботи, хост-сервера робить онлайн-сервіс недоступним для користувачів.

В [10] було запропоновано інтелектуальну систему, яка виявляє аномалій та ідентифікує пристрої розумних будинків, які застосовують колективну комунікацію. Сенс роботи запропонованої системи у отриманні результату від об'єднання розумних будинків в одну комп'ютерну мережу для підвищення безпеки для окремо розумного будинку і всієї мережі. Гарна властивість системи – це зв'язок кластерів розумних будинків один з одним для обміну інформації про профілі розумних пристроїв в білих списках кожного кластеру.

В [11] були систематизовані, узагальнені та розвинені поняття про методики і системи, які аналізують комп'ютерні мережі, які вимагають захисту. Наведений математичний апарат побудови моделі справного функціонування комп'ютерних систем, визначення загальної оцінки стану системи, якої потрібен захист. Надано загальні недоліки та напрямки подальшого розвитку комп'ютерних систем по виявленню кібератак та вторгнень. Інтелектуальна комп'ютерна система виявлення кібератак, аномалій та ідентифікації пристроїв розумних будинків із застосуванням колективної комунікації.

У [12] показано, що при розвитку комп'ютерних систем до вдосконалення деструктивного програмного забезпечення, спрямованого на різноманітні ресурси комп'ютерних систем. Дуже небезпечними є ті засоби, які підлаштовуються під реальне програмне забезпечення чи web-сервіс та знаходять шлях до персональних даних користувача, або можуть використовивать ці ресурси чи програмне забезпечення у своїх цілях. При активізації таких атак, активізується і засоби побудови спеціалізованих засобів виявлення та протидії кібератак, які будуть ефективні проти наявних та наступних кіберзагроз з невстановленими або нечітко визначеними властивостями, тобто функціонують у нечіткому, слабоформалізованому середовищі. Методики, моделі та комп'ютерні системи, основані на нечітких множинах використовуються для розробки та переробки існуючих засобів виявлення вторгнень та аномалій у комп'ютерних системах та мережах, які виникають при реалізації кіберзагроз. Метод формування лінгвістичних еталонів для комп'ютерних систем по виявленню вторгнень використовується при виявленні однією з ознак.

4 Загальна модель мережевого трафіку

Методи виявлення аномалій можна класифікувати за різними критеріями, а саме: по джерелам даних (Network-based IDS, Host-based IDS, Application-based IDS, Hybrid), по аналізу даних (експертна оцінка та машинне навчання), по способу отримання даних (сенсори, журнал подій, комбінований), по характеру отриманих даних (структурний аналіз, поведінковий аналіз).

В процесі порівняння конкретних груп методів виявлення аномалій: статистичний метод, кластерний аналіз, нейронні мережі, імунні мережі, експертні системи, метод опорних векторів, сигнатурні методи, було виявлено, що методи, які використовують підходи визначення аномалій використовують адаптивність, яка залежить від того, який метод був реалізовано. Тому вони виявляють тільки аномальну поведінку системи, але вони не класифікують цю аномалію. В перспективі при необхідності розробки нових методів виявлення аномалій, треба як можна раніше виявляти нові ще невідомі атаки, коли система знаходиться в робочому стані та в статичному, який відмінний від норми, яка задається розробленою моделлю нормальної поведінки [1].

Розглянемо трафік у звичайній мережі на основі стека протоколів TCP/IP, коли програма відправляє пакет за протоколом TCP. Типовий шлях пакета по локальній мережі виглядає наступним чином: пакет протоколу TCP з мережі Internet потрапляє у захищену локальну мережу, потім пересилається до конкретного комп'ютера у мережі (хосту). Далі пакет відправляється на конкретний порт, пов'язаний із конкретною сесією TCP.

Щоб точно змоделювати «нормальний» трафік мережі, введемо модель кожного з п'яти ключових значень (об'єктів): пакет (D), мережа (A), хост (H), порт (P), сесія (S). Кожне ключове значення K_1, K_2, K_3, K_4, K_5 можна охарактеризувати за допомогою набору параметрів $K_i(\kappa_1^i, \kappa_2^i, ..., \kappa_n^i),\ i \in (1,5).$ Пакет, що потрапляє в мережу, передається для аналізу в кожну з моделей. Спочатку у модель пакета, де перевіряється коректність полів заголовка пакета. Потім пакет передається у модель мережі, де він перевіряється на відповідність профілю мережі. Модель мережі вибирає відповідну модель нижнього рівня – модель хосту тощо. Таким чином пакет передається від моделей верхнього рівня моделям нижнього рівня. Після аналізу, кожна модель видає значення аномальності пакета (рисунок 4.1).

Кожна з моделей має два типи параметрів: прості параметри; складові параметри.

Прості параметри описують одну з характеристик моделі, наприклад, обсяг трафіку за годину або нормальну довжину пакета. Прості настройки не можуть вказувати на ключові об'єкти. Складові параметри – вказівники на логічна структуровані множини ключових об'єктів нижнього рівня, наприклад, список портів або дерево хостів.

До кожного ключового значення складається профіль. Профіль являє собою набір параметрів $P_i(p_1^i, p_2^i,..., p_j^i, q_1^i, q_2^i,..., q_k^i)$, $i \in (1,5)$. Параметри p_j^i відповідають параметрам ключових значень k_j^i, n ≤ l, а q_i – це додаткові параметри, що характеризують профіль.

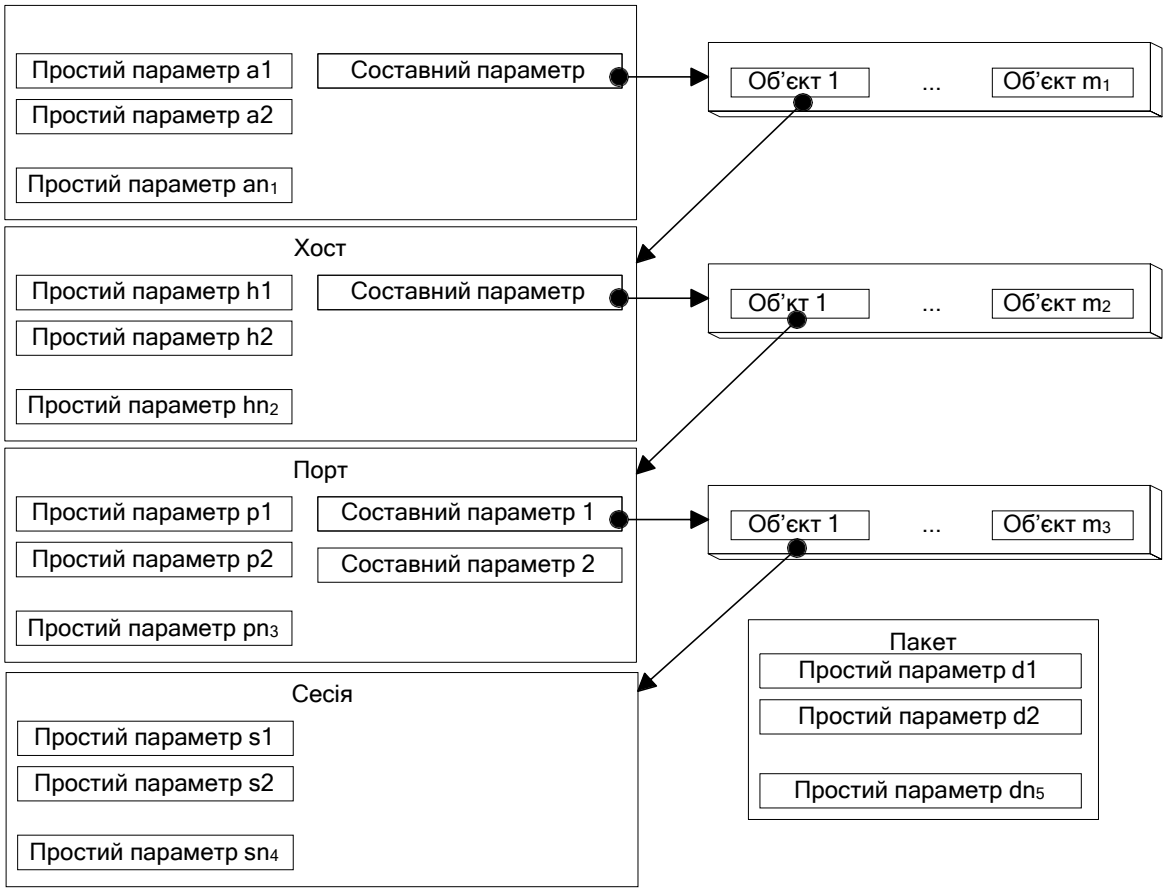


Рис.4.1 Взаємозв'язок параметрів ключових значень.

Як правило, це загальні параметри для всіх профілів: q_1 - тимчасова мітка створення профілю; q_2 – кількість пакетів у навчальній вибірці профілю; q_3 – тимчасова мітка останньої зміни профілю; q_4 – тимчасова мітка останнього аномального значення у профілі.

5 Загальна характеристика параметрів

За способом виявлення аномальних значень всі параметри всіх об'єктів *Ki* поділяються на два основні класи: чисельні; категоріальні.

До числових параметрів належать параметри, для перевірки яких використовуються статистичні та імовірнісні моделі. Наприклад, довжина пакета, обсяг переданих даних за одиницю часу, кількість пакетів у сесії тощо. Вони обчислюються за описаним нижче імовірнісним алгоритмом.

До категоріальних параметрів належать такі параметри, що можуть бути верифіковані за правилами. Ці параметри не можна оцінити у числовій формі. Наприклад, прапори TCP сесії.

Розглянемо докладніше числові параметри та методи їх аналізу. Пошук аномальних значень числових параметрів виконується з використанням імовірнісних методів. Для кожного числового параметра враховуються такі характеристики: мінімальне значення (V); максимальне значення (W); математичне очікування (M); дисперсія (D); порогове значення (Q).

Нехай є два класи пакетів: Ω_1 – клас нормальних пакетів та Ω_2 – клас пакетів, що належать мережевим атакам. Умовні щільності розподілу ймовірностей $f_1(x)$ та $f_2(x)$. Апріорна ймовірність появи об'єктів $P(\Omega_1)$ та $P(\Omega_2)$. Умовні ймовірності помилок 1-го та 2-го роду Q_1 та Q_2 можна визначити за формулами:

$$Q_1 = \int_{x_0}^{\infty} f_1(x)dx;\ Q_2 = \int_{-\infty}^{x_0} f_2(x)dx. \tag{5.1}$$

Вважатимемо, що щільності ймовірностей наших функцій підпорядковуються нормальному закону розподілу, тобто:

$$f_1(x) = (1/\sigma_1\sqrt{2\pi})e^{-(x-m_1)^2/(2\sigma_1^2)};\quad f_2(x) = (1/\sigma_2\sqrt{2\pi})e^{-(x-m_2)^2/(2\sigma_2^2)}. \tag{5.2}$$

Рішення про виявлення аномального значення приймається з використанням критерію Байєса та інтервалів довіри:

$$\frac{f_1(x)}{f_2(x)} > Q \text{ або } \frac{(x-m_1)^2/(2\sigma_1^2)}{(x-m_2)^2/(2\sigma_2^2} > Q, \tag{5.3}$$

де Q приймається експертно на етапі виявлення.

Оскільки критерій Байєса згладжує граничні значення, то додатково до критерію виконується перевірка на належність значення x, що спостерігається, до інтервалу можливих значень:

$$V \le x \le W \tag{5.4}$$

Ця модель параметра використовується для оцінки таких параметрів, як «нормальна» довжина пакета для поточної моделі та інших. Для оцінки інших числових параметрів цієї моделі недостатньо, тому були розроблені додатково дві більш складніші моделі числових параметрів: модель параметра потоків мережевого трафіку і модель параметра часових інтервалів мережевого трафіку. Розглянемо їх докладніше.

6 Модель параметра потоків мережевого трафіку

Майже у всіх об'єктів, що моделюються, можна виділити параметр, що характеризує обсяг вхідного і вихідного трафіку в одиницю часу. Побудуємо для цього параметра окрему модель і назвемо її «моделлю активності трафіку».

Трафік стосовно моделі може бути двох типів: вхідний потік (in flow) та вихідний (out flow).

З одного боку, сам собою підрахунок кількості переданих байт нам нічого не дасть. З іншого боку, при використанні інтелектуальних чи статистичних механізмів аналізу кількість переданих байт за одиницю часу набагато інформативніша. Наприклад, якщо раптом порт, який зазвичай активний тільки в робочі дні, раптом починає передавати дані у вихідні ввечері. Виходячи з викладених вище міркувань у профіль моделі активності трафіку включені наступні параметри:

–параметри вхідного потоку: - кількість переданих байт на годину, кількість переданих байт на день тижня, кількість переданих байт за день, кількість переданих байт за весь тиждень, кількість переданих байт на місяць;

- параметри вихідного потоку: - кількість переданих байт на годину, кількість переданих байт на день, кількість переданих байт на день тижня, кількість переданих байт на тиждень, кількість переданих байт на місяць.

Кожен із цих параметрів можна розглядати як числовий параметр та оцінювати одним із статистичних методів, які описані вище.

За допомогою побудованої моделі можна оцінювати активність як обсягів трафіку, так і активність кількості пакетів із заданим значенням параметра. Наприклад, збільшення кількості пакетів ICMP у мережі, в залежності від часу доби, може вказувати на встановлення ICMP-шелла.

Тому за допомогою цієї моделі числового параметра оцінюються такі параметри ключових понять: обсяг трафіку в байтах; кількість пакетів TCP; кількість пакетів ICMP; кількість пакетів UDP; загальна кількість пакетів за всіма протоколами.

7 Модель параметра часових інтервалів мережевого трафіку

Є ряд параметрів, які можна виділити у всіх об'єктів, що моделюються. Одним із таких параметрів є параметр, що характеризує час прибуття останнього пакета. Використовуючи цей параметр, можна знайти деякі види сканування портів. При їх використанні відправляються пакети на різні порти хосту, що атакуються через певні інтервали часу. Атака на відмову в обслуговуванні на web-сервері відкриває одночасно велику кількість з'єднань, тим самим переповнюючи чергу сервісу, що дозволяє виявляти такі атаки, з використанням часу прибуття останнього пакета. Під час встановлення веб-шелла інтервали між пакетами також будуть змінюватися.

Для виявлення атак, які описані вище, було запроваджено модель, що описує інтервали між пакетами: – модель часових інтервалів пакетів. Кожен із пакетів, що надходить по мережі, забезпечений тимчасовою міткою. Для цього в профілях об’єктів «Хост», «Порт» та «Сесія» введено два додаткові поля:

– час попереднього пакета (t_n) – це поле зберігає час прибуття останнього пакета і використовується для виявлення аномалій;

– інтервал до попереднього пакета (I_n) – це поле зберігає модель розподілу інтервалів часу між пакетами.

Для максимальної точності виявлення аномальних значень кожне поле зберігає відлік часу з точністю до мілісекунд.

Важливою частиною моделі є інтервали часу до попереднього пакета. Тимчасовий інтервал у свою чергою можна розглядати як числовий параметр і аналізувати за алгоритмом, який описаний вище, тобто, з урахуванням математичного очікування, дисперсії та інтервалу допустимих значень.

8 Категоріальні параметри

Категоріальні параметри не можна перевірити статистичними чи ймовірнісними методами, тому для них застосовується верифікація за правилами: – верифікаційне розпізнавання аномалій. Верифікаційне розпізнавання кожному параметру k_i^j ставить у відповідність правило R_i^j, де верхній індекс – індекс моделі (1 – мережа, 2 – хост, 3 – порт, 4 – сесія, 5 – пакет), нижній індекс – індекс параметра. Правило перевіряє належність параметра діапазону допустимих значень. У кожній ключовій моделі, крім моделі сесії, є хоча б один категоріальний параметр – це складовий параметр, з урахуванням правила якого вибирається відповідна модель нижнього рівня.

У моделі мережі є два категоріальні параметри. Перший категоріальний параметр описує діапазон адрес, що захищаються. Правило R_1^1 перевіряє, якому потоку належить пакет: вхідному, вихідному, чи це транзитний пакет. Другий параметр характеризує дерево хостів мережі, що захищається. Правило R_2^1 шукає відповідний профіль хоста, і якщо не знаходить його, повідомляє про аномалію.

Модель хоста має два категоріальні параметри. Відповідно до специфікації протоколу TCP у одному хості існує велика кількість різних портів.

Очевидно, що недоцільно зберігати профілі всіх портів. Тому модель поділяє порти на дві множини:

- серверні порти (порти, які постійно відкриті в системі та відповідають прикладним сервісам);

– клієнтські порти (порти, що динамічно генеруються системою).

На кожний серверний порт у системі заводиться окремий профіль. Для клієнтських портів моделі хоста формується загальний профіль, що характеризує загальну поведінку клієнтських портів. Перший параметр характеризує перелік серверних портів. Таким чином, при обробці серверного з’єднання правило R_1^2 шукає відповідний профіль порту для серверних з’єднань, і якщо не знаходить, генерує повідомлення про аномалію. Другий параметр характеризує загальний

профіль поведінки портів клієнтів. Правило R_2^2 ставить у відповідність клієнтським з'єднанням загальний профіль клієнтського порту.

Модель сесії, на відміну від моделей мережі і хоста, є динамічною, тобто, сесія не присутня в мережі постійно. Тому в моделі порту не зберігається профіль кожної сесії, а зберігається загальний профіль сесії. Модель порту включає два категоріальні параметри. Перший параметр – це список сесій, відкритих на даному порті на даний момент часу. Правило R_1^3 аналізованого пакету ставить у відповідність профіль сесії. Другий параметр – це загальний профіль сесії цього порту. Правило R_2^3 перетворює завершені сесії у загальному профілі сесії.

У моделях сесії та пакету є кілька категоріальних параметрів, тому розглянемо ці моделі докладніше.

9 Моделі сесії, пакета

Більшість сучасних протоколів прикладного рівня працюють з урахуванням протоколу TCP. Тому точна модель TCP сесії одна із ключових компонентів у описі «нормального поведінки» мережі. Як відомо, сесія однозначно ідентифікується наступним набором параметрів [3]: – IP адреса відправника; – IP адреса одержувача; – порт відправника; – порт отримувача.

Цей набір параметрів надалі і використовується як ідентифікатор сесій. Для обліку моделі сесії у системі до моделі порту було додано два складових параметри : список TCP сесій, аналізованих з першого пакета (таким чином, є можливість аналізу послідовності прапорів); список інших сесій. При побудові моделі сесії враховуються такі параметри: S_1 – послідовність прапорів; S_2 – вікно TCP сесії; S_3 – наявність опцій; S_4 – клієнт чи сервер; S_5 – кількість пакетів у сесії; S_6 – довжина пакетів; S_7 – кількість переданих даних у бітах за сесію; S_8 – співвідношення кількості переданих біт між клієнтом та сервером; S_9 – інтервали між пакетами.

Параметри сесії також розбиті на дві групи: категоріальні та числові. p align="justify"> Категоріальні параметри (S_1, S_2, S_3, S_4) аналізуються за допомогою набору верифікаційних правил, отриманих експериментально для кожного параметра: $R_i\,(s_i)$, i = 1...4. Числові параметри (S_5, S_6, S_7, S_8, S_9) аналізуються статистичними методами з використанням моделей, сформованих під час навчання та збережених у профілях P_i, i = 5...9.

Статистичні методи аналізу числових параметрів було описано вище, тому розглянемо докладніше аналіз категоріальних параметрів.

Верифікаційні правила сформовані експертно виходячи з аналізу специфікації протоколу TCP. Розглянемо їх докладніше.

Правило для аналізу послідовності прапорів R_1^4 ґрунтується на тому факті, що сесія TCP зазвичай має чітко визначену послідовність прапорів.

Під час встановлення сесії це SYN → SYN/ACK → ACK. Надсилання даних ACK →ACK/PUSH → …→ ACK. Завершення сесії FIN→ACK→FIN→ACK. Є й інші, допустимі стандартом послідовності прапорів, але вони у нормальній роботі мережі зустрічаються дуже рідко. Тому в побудованій моделі для аналізу параметра прапорів сесії S_1 був реалізований автомат, який перевіряє відповідність прапорів поточного пакета стану прапорів поточної сесії.

$$R_1^4(S_1 \mid S_1^{j-1}, S_1^{j-2}, ..., S_1^{j-k}, \tag{5.5}$$

де, S_1 – поточне значення першого параметра сесії для j-го пакета у цій сесії, а $R_1^4(S_1 \mid S_1^{j-1}, S_1^{j-2}, ..., S_1^{j-k}$, – значення першого параметра сесії для попередніх пакетів цієї сесії.

Правило R_2^4 здійснює аналіз параметра вікна TCP-сесії. При невдалій атаці, спрямованої на перехоплення чужої TCP-сесії, а також за деяких інших видів атак зловмиснику не вдається потрапити у вікно цієї сесії. При нормальній роботі більшості програм це зустрічається вкрай рідко. Тому пакети, які не потрапляють у вікно сесії, ми вважаємо аномальними.

$$R_2^4(S_2 \mid S_2^{j-1}, S_2^{j-2}, ..., S_2^{j-k}, \tag{5.6}$$

де, $k \in (3...5)$.

Правило призначене для аналізу параметрів опцій TCP-сесії. Це правило ґрунтується на знаннях про те, що опції зазвичай присутні лише в 1-му або 3-му пакеті сесії.

Параметр – клієнтська це сесія або серверна – сам по собі не аналізується, але він використовується при верифікаційному аналізі інших параметрів моделі. Коли у модель порту потрапляє пакет з прапором SYN і ідентифікатор цієї сесії відсутній у обох складових параметра порту, то тоді вона додається у відповідний список і сесія вважається клієнтською. Зокрема, цей параметр використовується для аналізу параметра s_1 послідовності прапорів (де враховується у який стан може перейти сервер і в яке – лише клієнт), а також, при аналізі числового параметра s_8 (співвідношення кількості переданих біт між клієнтом і сервером).

Верифікаційні правила моделі пакета перевіряють коректність полів заголовків пакетів IP та TCP. Правила формуються експертно з урахуванням специфікацій. Зокрема, перевіряються такі параметри: правило R_1^5 перевіряє, щоб IP адреса джерела не дорівнювала IP адресі одержувача; правило R_2^5 перевіряє, щоб порти джерела та одержувача не дорівнювали нулю; правило R_3^5 призначене для виявлення TCP пакетів з неприпустимими значеннями прапорів; правило R_4^5 перевіряє, щоб зарезервовані поля були заповнені нульовими значеннями; правило R_5^5 перевіряє, щоб довжина пакета була більшою або дорівнювала 40 байтам.

10. Висновки

Розроблена модель системи дозволяє виявляти атаки на ключові об’єкти, що моделюються. Отримані під час випробувань результати показали високу ефективність виявлення аномалій числових параметрів моделі. Для збільшення точності надалі планується перейти до моделювання поняття «сервіс» та моделювання протоколів HTTP, SMTP, POP3. Модель сесії також дозволяє виявляти існуючі та нові атаки на рівні сесії TCP, а також деякі види атак на відмову в обслуговуванні. Модель потоків мережевого трафіку дозволяє нам виявляти такі види атак, як: різні види сканування системи, установку троянських програм (бо зросте кількість байт у вихідному потоці), установку ICMP шелла (бо зросте кількість ICMP пакетів). Модель часових інтервалів дозволяє виявляти деякі види сканування системи, атаки на відмову в обслуговуванні та встановлення web-шеллу.

Стаття присвячена опису моделі виявлення мережевих вторгнень у трафіку мереж, побудованих з урахуванням стека протоколів TCP/IP. Аналізуються основні об'єкти локальної обчислювальної мережі. Описуються основні контрольовані параметри кожного типу об'єктів. Розробляються методи пошуку аномалій, що ґрунтуються як на аналізі за правилами, так і на аналізі з використанням імовірнісних моделей.

СПИСОК ЛІТЕРАТУРИ

1. Рубан І. В. Класифікація методів виявлення аномалій в інформаційних системах / Рубан І. В., Мартовицький В. О., Партика С. О. // Системи озброєння і військова техніка. – 2016. – №. 3. – С. 100-105. https://openarchive.nure.ua/server/api/core/bitstreams/7c434471-942c-40a7-b70c-0cc2655a42fe/content

2. Мірошник М.А. Модель мережевого планування із застосуванням методів мультипаралельної обробки інформації / Мірошник М.А., Толстолузький Є.Д. // тези 23 Міжнародна науково-технічная конференція "Проблеми інформатики та моделювання", Харків: НТУ "ХПІ", 2023. с. 75-76. https://repository.kpi.kharkov.ua/items/480d4c7b-d463-49dc-8521-c1162b16db88

3. Мирошник, М. А. Методы автоматизированного проектирования гетерогенных компьютерных систем и сетей критического применения / М. А. Мирошник, А. А. Можаев // Інформаційно-керуючі системи на залізничному транспорті. 2019. № 4. С.40-46.

DOI: https://doi.org/10.18664/ikszt.v0i4.178719.4.

4. Мирошник М. А. Синтез легкотестируемых двумерных сетей / М. А. Мирошник, Я. Ю. Королева // Інформаційно-керуючі системи на залізничному транспорті : тези стендових доповідей та виступів учасників 31-ї міжнародної науково-практичної конференції "Інформаційно-керуючі системи на залізничному транспорті" (Харків, 24-26 жовтня, 2018 р.). – 2018. – № 4 (додаток). – С. 20-21. http://lib.kart.edu.ua/handle/123456789/11689

5. Коробейнікова Т.І. Аналіз сучасних відкритих систем виявлення та запобігання вторгнень / Т.І. Коробейнікова, О.О. Цар // Національний університет «Львівська політехніка», Україна. May 2023, Грааль науки. С.317-325. DOI:10.36074/grail-of-science.12.05.2023.050, License, CC BY-SA 4.0

6. Лук'яненко Т. Ю. Методика виявлення мережевих вторгнень і ознак комп'ютерних атак на основі емпіричного підходу. / Лук'яненко Т. Ю., Поночовний П. М., Легомінова С. В. // Сучасний захист інформації. – № 2 (2022). – с.15-21. DOI: 10.31673/2409-7292.2022.021521

7. Чемерис К. М., Дейнега Л. Ю. Застосування методу вейвлет-аналізу для виявлення атак в мережах. Наука і техніка Повітряних Сил Збройних Сил України. 2022. № 1(46). С. 99-107. https://doi.org/10.30748/nitps.2022.46.14.

8. Панченко М.В. Виявлення аномалій інформаційної безпеки на основі аналізу ентропії інформаційної системи / М. В. Панченко, А. М. Бігдан, Т. В. Бабенко, Д. С. Тимофєєв. Енергетика і автоматика", №1, 2022 р. DOI 10.31548/energiya

http://journals.nubip.edu.ua/index.php/Energiya/article/viewFile/energiya2022.01.072/14743

9. Толюпа С. Засоби виявлення кібернетичних атак на інформаційні системи / С. Толюпа, Н. Лукова-Чуйко, Я. Шестак. Інфокомунікаційні технології та електронна інженерія. - №2 (2). 2021, стр. 19-31. https://science.lpnu.ua/sites/default/files/journal-paper/2022/mar/27268/stattya3stolyupanlukova-chuykoyashestak.pdf

10. . Нічепорук А.О. Інтелектуальна система виявлення аномалій та ідентифікації пристроїв розумних будинків із застосуванням колективної комунікації / А.О. Нічепорук, А.А. Нічепорук, О.С. Савенко, А.Д. Казанцев. Хмельницький національний університет // ISSN 2221-3805. Електротехнічні та комп'ютерні системи. 2021. № 34 (110) Інформаційні системи та технології Users/Administrator/Downloads/3196-Article Text-2350-1-10-20210904.pdf

11. Аналіз систем та методів виявлення несанкціонованих вторгнень у комп'ютерні мережі [Електронний ресурс] / В. В. Литвинов [та ін.] // Математичні машини і системи. К : ІПММС НАН України, 2018. № 1. С. 31-40. http://dspace.nbuv.gov.ua/handle/123456789/132008 .

12. Терейковський І. Моделі еталонів лінгвістичних змінних для систем виявлення email-спуфінг-атак / І. Терейковський, А. Корченко, П. Вікулов, І. І. Дж. Ірейфідж // Безпека інформації. - 2018. - Т. 24, № 2. - С. 99-109.

Режим доступу: http://nbuv.gov.ua/UJRN/bezin_2018.

REFERENCES

1. Ruban I. V. Classification of anomaly detection methods in information systems / Ruban I. V., Martovytskyi V. O., Partika S. O. // Armament systems and military equipment. – 2016. – no. 3. – pp. 100-105. https://openarchive.nure.ua/server/api/core/bitstreams/7c434471-942c-40a7-b70c-0cc2655a42fe/content [in Ukrainian]

2. . Miroshnyk M.A. A model of network planning with the use of multiparallel information processing methods / M.A. Miroshnyk, E.D. Tolstoluzkyi. // theses 23 International Scientific and Technical

Conference "Problems of Informatics and Modeling", Kharkiv: NTU "KhPI", 2023. – pp. 75-76. https://repository.kpi.kharkov.ua/items/480d4c7b-d463-49dc-8521-c1162b16db88 [in Ukrainian]

3. Miroshnyk M.A.. Methods of automated design of heterogeneous computer systems and networks of critical application / Miroshnyk M.A., A.A. Mozhaev // Information and control systems on railway transport. – 2019. – No. 4. – P.40-46. DOI: https://doi.org/10.18664/ikszt.v0i4.178719.4 [in Ukrainian]
4. Miroshnyk M.A. Synthesis of easily testable two-dimensional networks / M. A. Myroshnyk, Y. Yu. Koroleva // Information and control systems in railway transport: abstracts of poster reports and speeches of the participants of the 31st international scientific and practical conference "Information and control systems in railway transport" (Kharkiv, October 24-26, 2018). – 2018. – No. 4 (appendix). - pp. 20-21. http://lib.kart.edu.ua/handle/123456789/11689 [in Ukrainian]
5. Korobeynikova T.I. Analysis of modern open intrusion detection and prevention systems / T.I. Korobeynikova, O.O. Tsar // Lviv Polytechnic National University, Ukraine. May 2023, the grail of science. pp. 317-325.

   DOI:10.36074/grail-of-science.12.05.2023.050, License, CC BY-SA 4.0 [in Ukrainian]
6. Lukyanenko, T. Yu. Methodology for detecting network intrusions and signs of computer attacks based on an empirical approach. / Lukyanenko T. Yu., Ponochevny P. M., Legominova S. V. // Modern protection of information. – No. 2 (2022). - pp. 15-21.DOI: 10.31673/2409-7292.2022.021521 [in Ukrainian]
7. Chemeris K. M., Deinega L. Yu. Application of the wavelet analysis method to detect attacks in networks. Science and technology of the Air Force of the Armed Forces of Ukraine. 2022. No. 1(46). pp. 99-107. https://doi.org/10.30748/nitps.2022.46.14 [in Ukrainian]
8. M.V. Panchenko Identification of information security anomalies based on information system entropy analysis / M. V. Panchenko, A. M. Bigdan, T. V. Babenko, D. S. Timofeev. Energy and automation", No. 1, 2022. DOI 10.31548/energiya [in Ukrainian]

   http://journals.nubip.edu.ua/index.php/Energiya/article/viewFile/energiya2022.01.072/14743
9. Tolyupa S. Means of detecting cybernetic attacks on information systems / S. Tolyupa, N. Lukova-Chuiko, Ya. Shestak. Information communication technologies and electronic engineering. - #2 (2). 2021, pp. 19-31. [in Ukrainian]

   https://science.lpnu.ua/sites/default/files/journal-paper/2022/mar/27268/stattya3stolyupanlukova-chuykoyashestak.pdf [in Ukrainian]
10. Nicheporuk A.O. An intelligent system for detecting anomalies and identifying devices of smart buildings using collective communication / A.O. Nicheporuk, A.A. Nicheporuk, O.S. Savenko, A.D. Kazantsev. Khmelnytskyi National University // ISSN 2221-3805. Electrical and computer systems. 2021. No. 34 (110) Information systems and technologies Users/Administrator/Downloads/3196-Article Text-2350-1-10-20210904.pdf [in Ukrainian]
11. Analysis of systems and methods for detecting unauthorized intrusions into computer networks [Electronic resource] / V.V. Litvinov [et al.] // Mathematical machines and systems. K: IPMMS of the National Academy of Sciences of Ukraine, 2018. No. 1. P. 31-40.

    http://dspace.nbuv.gov.ua/handle/123456789/132008 . [in Ukrainian]
12. I. Tereykovskyi. Models of standards of linguistic variables for email-spoofing-attack detection systems / I. Tereykovskyi, A. Korchenko, P. Vikulov, I. I. J. Ireifidge // Information security. - 2018. - Vol. 24, No. 2. - P. 99-109. - Access mode: http://nbuv.gov.ua/UJRN/bezin_2018. [in Ukrainian]

Demenkova Svitlana *Senior lecturer of the department of automation of chemical-technological systems and environmental monitoring, National Technical University, Kharkiv Polytechnic Institute, Kharkiv, Kirpychova St.,2, 61002*
e-mail: svet1972232765@gmail.com
https://orcid.org/0000-0003-0604-5456

Demchenko Kateryna *associate professor of the Department of Automation and Computer-Integrated Technologies, State Biotechnology University, str. Alchevsky 44, Kharkiv, Ukraine, 61002*
e-mail: yayaska@btu.kharkiv.ua
https://orcid.org/0000-0002-3168-5351

Koroleva Yana *associate professor of the department of multimedia and Internet technologies and systems, National Technical University, Kharkiv Polytechnic Institute, Kharkiv, Kirpychova St.,2, 61002*
e-mail: yanakoroleva815@gmail.com
https://orcid.org/0000-0003-0604-5456

Pakhomov Yurii *associate Professor of the Department of Computer Sciences and Information Technologies, Beketov Kharkiv National University of Urban Economy Kharkiv, str. 17, Marshala Bazhanov, Ukraine, 61002*
e-mail: abc050073@gmail.com
https://orcid.org/0000-0002-2267-8600

Using anomaly detection method to detect network attacks

The article is focused on the description of a model for detecting network intrusions in the network traffic based on the TCP/IP protocol stack. The main objects of a local area network have been analyzed. The main controlled parameters of each type of object have been described. The methods of anomaly detection based on both rule-based and probabilistic model analysis have been developed.

Relevance. Due to the intensive growth of information technologies and their implementation in various sectors of the municipal economy, the issue of information security becomes very relevant.

Research methods. In solving the tasks, the methods of control theory; methods of building security systems; graph theory; probability theory and mathematical statistics; methods of time series analysis; methods of predictive analytics and big data processing; methods of building high-load secure programs have been used. The main research methods used are probabilistic and verification modeling.

The results. Probabilistic and verification modeling of network attacks has confirmed the effectiveness of the proposed approach. The results of synthesis using CAD showed that the additional hardware costs do not exceed 20% compared to the standard description model.

Conclusions. The developed system model allows detection of attacks on key simulated objects. The results obtained during the tests showed a high efficiency of detecting anomalies in the numerical parameters of the model. In order to increase accuracy, it is planned to move on to the modeling of the concept of "service" and the modeling of HTTP, SMTP, and POP3 protocols. The session model also allows detecting existing and new TCP session-level attacks, as well as some types of denial-of-service attacks. The model of network traffic flows allows us to detect such types of attacks as: various types of system scanning, installation of Trojan programs (because the number of bytes in the output stream will increase), installation of ICMP shell (because the number of ICMP packets will increase). The time interval model allows detecting some types of system scanning, denial-of-service attacks, and web shell installation.

Keywords: *anomaly detection, network attacks, finite state machines, verification, modeling, distributed information networks, probabilistic modeling, verification modeling.*

Надійшла у першій редакції 01.11.2023, в останній – 02.12.2023.
The first version has been received on 01.11.2023, the final version – on 02.12.2023.

DOI:https://doi.org/10.26565/2304-6201-2023-60-03

УДК (UDC) 519.7, 004.8

Novikov Artem *PhD student, Department of Artificial Intelligence Systems Karazin Kharkiv National University, Svobody Sq 4, Kharkiv, Ukraine,61022*
email: artem.slick@gmail.com;
https://orcid.org/0009-0004-5914-7098

Smyrnov Vadym *Master's student, Department of Artificial Intelligence Systems Karazin Kharkiv National University, Svobody Sq 4, Kharkiv, Ukraine,61022*
e-mail:vadym.smyrnov@student.karazin.ua;
https://orcid.org/0009-0000-1743-8541

YanovskyVolodymyr *Doctor of physical and mathematical sciences; Professor of Department of Artificial Intelligence Systems*
"Institute for Single Crystals" of National Academy of Sciences, Nauky ave. 60, Kharkiv, Ukraine, 61001
e-mail:yanovsky@isc.kharkov.ua;
https://orcid.org/0000-0003-0461-749X

Shadow zones of an artificial neuron

The extremely widespread use of artificial neural networks in the diverse areas of application makes the study of their fundamental properties highly relevant. Such studies can be used to improve the properties of neural networks.
The key goal of the work: to determine the general properties of artificial neurons and detect the presence of zones where the field of output signals has a complex fractal structure in the space of all input signals.
Research methods: to explore the space of all input signals, a software that allows modelling the neuron's response to all possible input signals with a certain length in the given alphabet has been developed. With the help of the developed application the space of all input signals can be modulated and the field of output signals in this space is graphically determined. By using the capability of the software to change the scale of the input signal space, zones with a self-similar, fractal structure have been found.
Results: it has been established that when considering the overall arrangement of the neuron's input signal space, specific areas – shadow zones – are present, which exhibit a complex fractal structure of output signal field. The impact of modifying theneuron's weights and threshold on the presence and location of such zones has been established. The changes that follow an increase in the length of the input signals have been described. The fractal dimension of the structures within shadow zones has been determined.
Conclusions: the obtained general properties of neurons should significantly impact the properties of neural networks in the form of shadow zones in which the "response" of the network is extremely sensitive even to minute alterations in input signals. The presence of such zones is an extremely important factor that needs to be considered while developing neural networks.

Keywords: *artificial neuron, weights, fractals, fractal dimension, activation function, space of input signals, field of output signals.*

Як цитувати: Novikov A., Smyrnov V., Yanovsky V., Shadow zones of an artificial neuron . *Вісник Харківського національного університету імені В.Н. Каразіна, серія Математичне моделювання. Інформаційні технології. Автоматизовані системи управління*. 2023. вип. 60. С.27-35. https://doi.org/10.26565/2304-6201-2023-60-03

How to quote: Novikov A., Smyrnov V., Yanovsky V., "Shadow zones of an artificial neuron", *Bulletin of V.N. Karazin Kharkiv National University, series Mathematical modelling. Information technology. Automated control systems*, vol. 60, pp.27-35, 2023. https://doi.org/10.26565/2304-6201-2023-60-03 .

1. Introduction

Nowadays, neural networks have garnered significant attention as one of the promising domains in the advancement of artificial intelligence which has been introduced in the scientific study as a very simplified mathematical model of a natural neuron. It represented a nonlinear function, which is an activation function from a linear combination of input signals. In the research by Warren McCulloch and Walter Pitts [1], the Heaviside function played the role of the activation function, and such neurons could execute logical operations, and when organized into a neural network, they demonstrated the capability

to conduct numerical calculations. It was planned to construct neural networks based on electronic circuits, where neurons would function using binary signals. That corresponded to a certain degree with natural neurons, which could be in an excited or non-excited state. The practical implementation of such neural network was achieved by Frank Rosenblatt in the form of a perceptron [2, 3]. Rosenblatt anticipated substantial success in the advancement of artificial intelligence through neural networks.

The development of neural networks demanded the creation of more versatile neurons capable of processing numerical signals. Such neurons were proposed by Withrow and Hoff [4]. They suggested using a logistic dependence, or a sigmoid function, as an activation function. An important stage in the development of neural networks was the inception of the idea of learning neural networks, which in the form of the first learning algorithm appeared in the work of Hebb [5].

However, the M. Minsky and S. Papert [6] demonstrated the limitations of single-layer perceptrons and notably reduced attention to neural networks. The interest revived after the publication of Hopfield's works [7, 8, 9], and after the discovery and advancement of the backpropagation [10] the rapid development of learning neural networks began.

Now, the study of neural networks is becoming even more important, as we are facing an ever-increasing amount of data and data-based tasks that require complex analytical and decision-making solutions. Neural networks are used in many areas, including medicine, finance, automation, image recognition, natural language, and many others [11, 12, 13]. They have become a fundamental tool for achieving and enhancing solutions that were previously performed exclusively by humans [14].

This work researches the output field of a neuron for all possible input words of a certain length. It is demonstrated that within the input word space, there are zones – shadow zones – where the output field exhibits a fractal structure. The range of scales at which a self-similar fractal structure is observed is determined by the length of the input words n, encompassing a vast scale range $1 \div 2^{-n}$. The fractal dimension of such structures is determined. An area where shadow zones emerge within neuron weight values is pinpointed. The changes that might occur as the number of input channels of the neuron increases are discussed.

2. Formulation of the problem

Let us consider how a typical neuron responds to various input words within a certain alphabet. For the sake of simplicity, we will use a binary alphabet $A = [0,1]$. Using this alphabet, we will construct input words and generate the neuron's response or output words. The main goal of research is to determine the structure of the neuron's responses to all input words.

To answer this question, let us discuss the set of all questions and our conceptualization of them. Certainly, all questions consist of words from the alphabet A, and this set is denoted as A^*. According to Cantor's theorem, the cardinality of the set A^* is the continuum. To distinguish finite subsets, we also consider sets of words of finite length n, and for such subsets, we use the notation A_n^*. Therefore, any word $x \in A_n^*$ has a length $|x| = n$. The number of elements in A_n^* is equal to 2^n. As a result, all questions can be arranged in lexicographic order, thereby forming a completely ordered set. It is easy to see that each of these words corresponds to a particular interval of length $\frac{1}{n}$ within the unit interval (see Fig. 2.1). Within limit $n \to \infty$ each infinite word corresponds to a point in the unit interval. Thus, it can be deduced that each input word encodes a number less than one in the binary numeral system. For example, the number 0.011000111101 corresponds to the input word 011000111101. It is evident that the intervals of length $\frac{1}{n}$ correspond to numbers that have the same first n signs and differ in subsequent signs. This implies that such an interval comprises truncated numbers up to the decimal point. By agreement, if the number contains fewer signs, zeroes are appended to the record to match the agreed-upon length. Such coding method allows the complete set of questions presented as an input of a neuron to be displayed graphically.

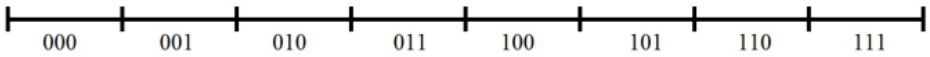


Fig. 2.1. An example of dividing a unit segment into 2^3 *subintervals of length* $1/2^3$ *is shown to determine a mutually unique correspondence with all words of length 3 in the alphabet* $A=[0,1]$. *Words of any length can be arranged in the same way.*

For simplicity's sake, we will consider a neuron with two input channels (see Fig. 2.2). Then each pair of input words that are sent to the input of the neuron corresponds to the cells of the unit square with coordinates (x, y). If the length of the input word is n, then the associated cell's side length is $\frac{1}{n}$. In fact, this square divided into cells, represents the space of all input words with a length of n. That enables the visualization of the neuron's response to every possible input word. To do this, let us assign a color to each cell based on the output value corresponding to the input words. To generate source words, the sequences in the binary alphabet are sent to the input channels. At the output, we will receive a sequence of the same length. There are two ways to achieve that. The first is to use the McCulloch-Pitts neuron [1], [16] with an activation function that corresponds to the Heaviside θ-function. The second is to use a standard neuron with a sigmoidal activation function, but set the rule that a value exceeding $1/2$ corresponds to the reaction 1, and if it is less than $1/2$, then it corresponds to the reaction 0. In both cases, the neuron's output will consist of a sequence of binary symbols with the same length as the input words.

Thus, each pair of input words relates to a cell of the size $\frac{1}{|x|}$ which is divided by the unit square (see Fig. 2.2). From a number coding perspective, such a cell corresponds to all real numbers that have the same first $|x|$ decimal places and differ in subsequent signs. In order to determine the neuron's field of reactions to all possible input words, it is enough to color each cell according to the initial sequence. Thus, a particular palette should be used. In our research, we have used the simplest palette. So, if the initial sequence is encoded with a number less than $1/2$, then the response corresponds to yellow, otherwise, it corresponds to blue. Next, we have used a program that executes such an algorithm automatically. By providing all possible words to the input of the neuron, it determines the output word and sets the color of the corresponding cell within the unit square. After processing all input words, it depicts a single painted square, i.e. the output field. A more detailed description of the program is provided in Appendix A. In short, its functionality corresponds to sending all possible pairs of input words to the neuron's input, obtaining the output sequence and coloring the corresponding cell in a certain color based on the resulting output word. As a result, we get the response field of the neuron.

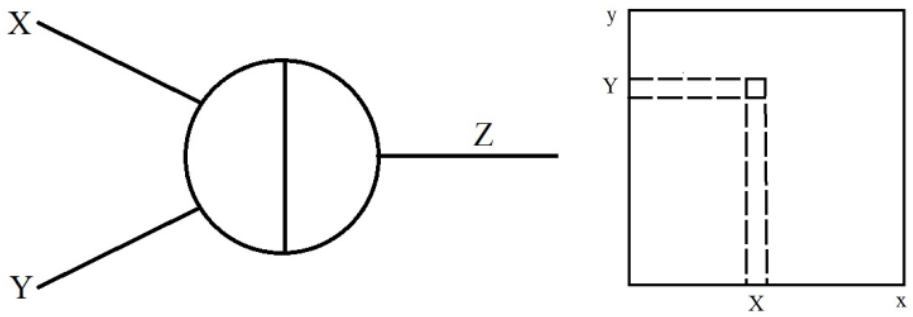


Fig 2.2. An artificial neuron with two input channels is symbolically shown on the left side. X *and* Y *inputs are binary sequences of the same length,* Z *output is a binary sequence of the same length. On the right side, the positioning of the two input sequences* X *and* Y *on the unit square is shown.*

3. Modeling results

Using the developed program (see Appendix A), the response field of an artificial neuron with a sigmoid activation function and a McCulloch-Pitts neuron with an activation function that corresponds to the Heaviside function at certain weight values can be examined. The input words had a length of 8. The resulting response field is shown in Fig. 3.1. It is easy to see the extraordinary structure of this field for both neurons. The input word space is divided into three characteristic zones, each demonstrating a unique structure of output words. The blue zone has no structures and occupies 3/4 of the unit square's area. The triangular yellow zone, lacking distintive structures, encompasses 1/8 of the unit square's areas. The final zone that occupies 1/8 of the area is structured and corresponds to the fractal structure of the response field. This class of objects is extremely common in nature and has been the subject of exensive study since the work of Mandelbrot [17]. Further, the zones in the space of input words in which the output words form fractal structures are referred to as "shadow zones". The fractal structure observed in these zones is well known as the Sierpiński carpet [17, 18]. Fractal, self-similar objects are characterized by a non-integer dimension, commonly known as fractal dimension. For example, the fractal dimension of the structure in Fig. 3.1 is $D_f = \frac{\ln 3}{\ln 2} \approx 1.59$.

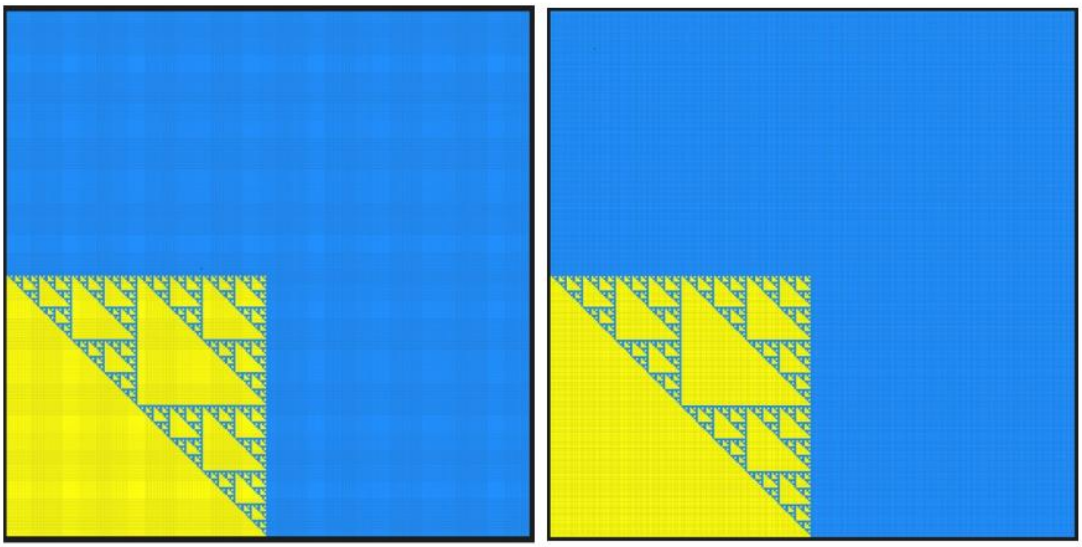


Fig 3.1. The field of responses to all possible questions with a length of 8. On the left, the field of responses of a McCulloch-Pitts neuron is depicted ($\omega_x = 1, \omega_y = 1, \sigma = -0.5$), and a regular neuron with a sigmoid activation function ($\omega_x = 1, \omega_y = 1, \sigma = -0.2$) is presented on the right.

Thus, the response of a regular neuron to all possible input words has shadow zones with fractal structures, and that has extremely interesting consequences. Indeed, if the questions are located in the non-fractal zones, the neuron's response remains unchanged with small alterations in the input words. Conversely, in the shadow zones, even a minor modification to the last character of the input word can result in a drastic change of the neuron's response. For instance, assuming that blue indicates "Yes", and yellow indicates "No", a modification in the last character of the input word may change the response from "Yes" to "No". In other words, such sensitivity can be considered as the manifestation of chaos in the neuron's responses. This is a distinct form of chaos that does not stem from random influences on the neuron, but is its internal property and refers to deterministic chaos [19, 20].

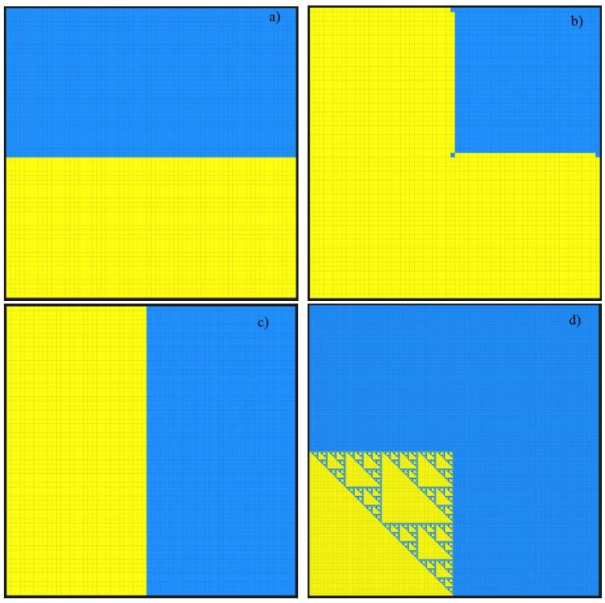


Fig. 3.2. All typical response fields of the neuron observed during simulation at different values of the neuron's weights are shown, excluding trivial cases of one color only.

Let us consider how typical the appearance of shadow zones with fractal structures is. To achieve thats, we have determined the neuron weights associated with the presence or absence of shadow zones. The result of such check can be depicted graphically. Fig. 3.2 shows all possible response fields of the neuron (excluding the trivial case where the entire space of input words is yellow*)*,denoted as *a), b), c),* and *d)* corresponding to different weight values obtained from the simulation. The first three response fields do not have shadow zones and, consequently, fractal structures, while the fourth field demonstrates a typical example with a shadow zone. It is important to note that case *b)* depends on the length of the input words. Namely, the small squares positioned near the corners of the big blue square have the size $\frac{1}{2^n}$.That is, as the length of the input words increases, the squares decrease in size and become less noticeable. No other structures have been observed in the simulation. Analyzing the square in the coorqdinate axes (ω_1, ω_2), we have determined the weights that result in the structures of the response field depicted in Fig. 3.2. The results of this analysis are shown in Fig. 3.3. The range of weights from 0 to 1 shows the weights at which fractal structures are observed. This zone is highlighted in green in Fig. 3.3. Thus, in the case of a threshold $\sigma = 0.2$, it covers 0.69 of the plane of the considered weight change. The non-fractal structures encompass 0.31 of the square area.

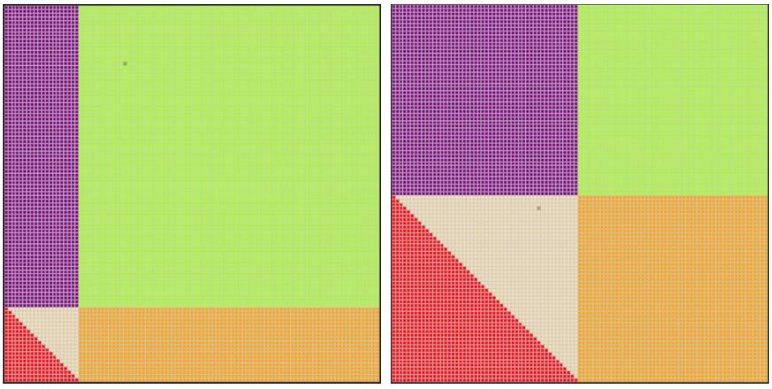


Fig. 3.3. The regions of the neuron's weights ω_1, ω_2 in which response fields have been observed. The green area represents the neuron weight values where the shadow zones appear. The purple area corresponds to the field of answers - a), orange - b), light brown - c), and red - all yellow answers.

On the left side, it shows the range of neuron weights when the threshold is set to $\sigma = 0.2$. On the right side, it illustrates the range of neuron weights with a threashold $\sigma = 0.5$. The influence of the

threshold on the sizes of the corresponding squares is noticeable. There is practically no difference in choosing the sigmoid or Heaviside activation function.

It can be seen, that when the weights change within the $[0,1]$ interval, shadow zones occur twice as frequently. Altering the threshold results in changing of all zone planes. Therefore, increasing the threshold makes the size of the green zone decrease. The case when the threashold is set to $\sigma = 0.5$ is shown in Fig. 3.3 on the right side. Decreasing the threshold, conversely, expands the area of the green zone as shown in Fig. 3.3 on the left side. The symmetrical structure of the square divisions remains intact, only a shift along the diagonal of the square is observed. This allows predicting the changes occuring with alterations in the threshold. Data approximation reveals a linear relationship between the area of the green zone in the unit square of the weights and the threshold value. It can be concluded that the existence of shadow zones with a fractal structure of the response field in the input word space is a common characteristic of neurons.

4. Conclusion

Thus, it has been proven that the presence of shadow zones within the input word space, displaying output words with a fractal structure, is an internal characteristic of artificial neurons. The fractal dimension of the resulting fractal structures is equal to $D_f = \frac{\ln 3}{\ln 2} \approx 1.59$. The region of weights where shadow areas are observed in the neuron's response field is determined. The area of the weight range where shadow zones are observed depends on the threshold of the neuron. As the length of the input words increases, the fractal structure persists and extends to extremely small scales ranging from 1 to 2^{-n}. This generates zones of extreme sensitivity of the neuron's responses to even the slightest alterations in input words. In those zones, a reversal of the answer can happen even when the last character in the input word is changed.

It is evident that increasing the number of input channels of an artificial neuron does not influence the existence of shadow zones in the input word space, but visualizing these zones becomes more challenging due to the expanded dimensionality of the space of all possible input questions or words, which aligns with the number of input channels of the neuron. Consequently, visualizing shadow zones and their corresponding fractal structures becomes impossible for four or more input channels. With three input channels, this problem can still be solved. Certainly, when maintaining the weight of the third input channel and the input word constant, we can observe the aforementioned fractal structures on the response field to input words that are transmitted through two channels. Geometrically, that image corresponds to a certain intersection of a unit cube divided into corresponding colored cubes of smaller sizes, namely 2^{-n}. With a larger number of input channels, it is possible to detect such fractal structures without the visualization, by using special mathematical algorithms. Such algorithms are used in the study of strange attractors in dissipative nonlinear dynamical systems in high-dimensional spaces.

Appendix A

In our study of artificial neurons we have been using a custom-built web application designed to model and visualize the behavior of two different neuron models: SigmoidNeuron and ThresholdNeuron (McCulloch-Pitts neuron). This web application has been developed using the React library for building user interfaces and TypeScript for enhanced code quality.

The interface (see Fig. 5.1) provides separate settings fields for each neuron model. It allows adjusting such parameters as signal weights (w1, w2) and bias (threshold). Additionally, users have the opportunity to set the length of the question, thereby affecting the number of combinations of inputs for the neurons. For instance, a question of length 2 generates $(2 * 2)^2 = 16$ combinations of x1 and x2.

Fig. 5.1. The application interface.

Upon clicking the "Generate" button, the application generates a table representing all possible combinations of inputs. The square visualization component represents the table, plotting x1 values horizontally from left to right and x2 values vertically from bottom to top (see Fig. 5.2). Each cell in the table corresponds to a specific combination of x1 and x2 inputs. The application sends these inputs to the neurons, resulting in a sequence of zeros and ones as the output. If the output sequence exceeds the average value of the table, the cell is colored blue, representing a positive response ("yes"). Otherwise, the cell is colored yellow, indicating a negative response ("no").

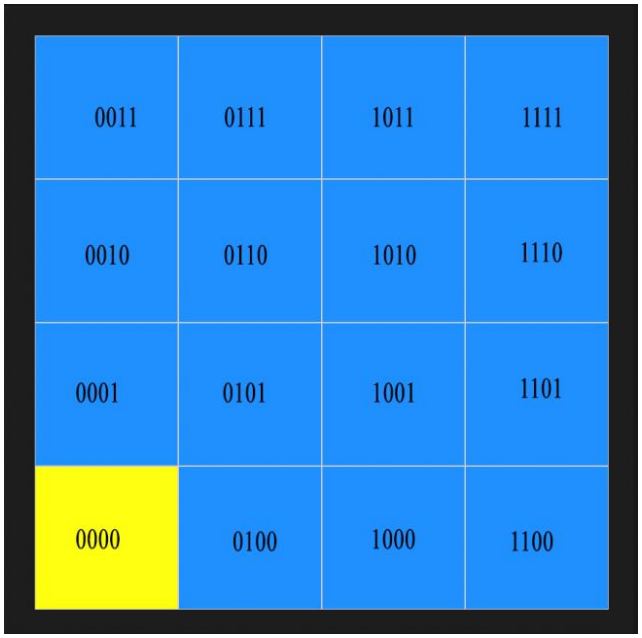


Fig. 5.2. Example of values arranging in the table for question of length 2.

Application has the following workflow:

1. User configures neuron model settings.
2. User sets the question length.
3. User clicks "Generate" to create a table of binary combinations.
4. The application processes each cell, sending inputs to the neurons and determining the output sequence.
5. Cell coloring reflects the decision outcome: blue for "yes," yellow for "no."
6. The final output is a square grid of cells, where each cell corresponds to a specific question and its color indicates the neuron's response.

This web application serves as a powerful tool for providing a visual understanding of the decision-making processes of artificial neurons, offering valuable insights into their behavior based on different configurations and input patterns.

REFERENCES

1. W. S. McCulloch and W. Pitts, "A logical calculus of the ideas immanent in nervous activity," *Bulletin of Mathematical Biophysics*, vol. 5, no. 4, pp. 115–133, 1943.https://doi.org/10.1007/BF02478259
2. F. Rosenblatt, "The Perceptron: A Probabilistic Model for Information Storage and Organization in the Brain," *Psychological Review*, vol. 65, no. 6, pp. 386–408, 1958.https://doi.org/10.1037/h0042519
3. F. Rosenblatt, *Principles of Neurodynamics*. Washington, DC: Spartan Books, 1962.https://doi.org/10.2307/1419730
4. B. Widrow and M. E. Hoff, "Adaptive switching circuits," in 1960 *IRE WESTCON Conference Record*. New York, 1960.https://doi.org/10.7551/mitpress/4943.003.0012
5. D. O. Hebb, The organization of behavior; a neuropsychological theory. New York: Wiley, 1949.
6. M. L. Minsky and S. A. Papert, Perceptrons. Cambridge, MA: MIT Press, 1969.https://doi.org/10.1016/s0361-9230(99)00182-3
7. J. J. Hopfield, "Neural networks and physical systems with emergent collective computational abilities," *Proceedings of National Academy of Sciences*, vol. 79, no. 8, pp. 2554–2558, April 1982.https://doi.org/10.1073%2Fpnas.79.8.2554
8. J. J. Hopfield, "Neural with graded response have collective computational properties like those of two-state neurons," *Proceedings of the National Academy of Sciences*, vol. 81, no. 10, pp. 3088-3092, May 1984.https://doi.org/10.1073/pnas.81.10.3088
9. J. J. Hopfield, "Learning algorithms and probability distributions in feed-forward and feed-back networks,"*Proceedings of the National Academy of Sciences*, vol. 84, no. 23, pp. 8429-8433, December 1, 1987.
10. D. E. Rumelhart, G. E. Hinton, and R. J. Williams, "Learning Internal Representations by Error Propagation," *Parallel Distributed Processing*, vol. 1, pp. 318–362. Cambridge, MA: MIT Press, 1986.https://doi.org/10.7551/mitpress/5236.003.0012
11. Y. Wu and J. Feng, "Development and application of artificial neural network," *Review of Wireless Personal Communications*, vol. 102, no. 2, pp. 1645-56, 2018.https://doi.org/10.1007/s11277-017-5224-x
12. A. Sharma and A. Chopra, "Artificial neural networks: Applications in management," *Review of Journal of Business and Management*, vol. 12, no. 5, pp. 32-40, 2013.https://doi.org/10.1371%2Fjournal.pone.0212356
13. J. Jiang, P. Trundle, and J. Ren, "Medical image analysis with artificial neural networks," *Review of Computerized Medical Imaging and Graphics*, vol. 34, no. 8, pp. 617-31, 2010.https://doi.org/10.1016/j.compmedimag.2010.07.003
14. A. Abraham, "Artificial Neural Networks," in *Handbook of Measuring System Design*, 1st ed., vol. 3, John Wiley & Sons, 2005. http://dx.doi.org/10.1002/0471497398.mm421
15. G. Cantor, "Über eine elementare Frage der Mannigfaltigskeitslehre," *Jahresbericht der Deutschen Mathematiker-Vereinigung*, vol. 1, pp. 75–78, 1891.[in German]http://eudml.org/doc/144383
16. P. Halmos, *Naive Set Theory*. Princeton, NJ: D. Van Nostrand Company, 1960. Reprinted by Springer-Verlag, New York, 1974.
17. B. B. Mandelbrot, *The Fractal Geometry of Nature*. New York: W. H. Freeman and Co., 1982.
18. M. F. Barnsley and H. Rising, *Fractals Everywhere*. Boston: Academic Press Professional, 1993.
19. R. M. Crownover, *Introduction to Fractals and Chaos*. University of Missouri-Columbia: Jones and Bartlett Publishers, Boston, London, 1995.
20. H. G. Schuster, *Deterministic Chaos: An Introduction*. Weinheim: Physik-Verlag, 1984.

Зони тіні штучного нейрона

Новіков Артем Олександрович *аспірант кафедри штучного інтелекту та програмного забезпечення Харківський національний університет імені В.Н. Каразіна; майдан Свободи, 6, м. Харків, Україна, 61022*

Смирнов Вадим Максимович *студент магістратури кафедри штучного інтелекту та програмного забезпечення Харківський національний університет імені В.Н. Каразіна; майдан Свободи, 6, м. Харків, Україна, 61022*

Яновський Володимир Володимирович *доктор фізико-математичних наук; професор штучного інтелекту та програмного забезпечення Інститут монокристалів, Національна Академія Наук Україн; пр. Науки 60, м. Харків, Україна, 61001*

Надзвичайна поширеність використання штучних нейронних мереж у самих різноманітних напрямках застосувань робить дослідження їх фундаментальних властивостей надзвичайно актуальним. Таки властивості можуть бути використані для покращення властивостей нейронних мереж.

Мета роботи полягає в визначенні загальних властивостей штучних нейронів та виявлені наявності у просторі всіх вхідних сигналів зон, де поле вихідних сигналів має складну фрактальну структуру.

Методи дослідження: для дослідження простору всіх вхідних сигналів було розроблено програмне забезпечення, яке дозволило моделювати реакцію нейрона на всі можливі вхідні сигнали певної довжини у деякому вхідному алфавіті. За допомогою цього забезпечення було з модульовано простір всіх вхідних сигналів та графічно визначено поле вихідних сигналів у над цим простором. Використовуючи можливість програмного забезпечення змінювати масштаб спостереження простору вхідних сигналів було здійснено пошук зон з самоподібною, фрактальною структурою.

Результати: У роботі визначено, що у випадку загального положення у просторі всіх вхідних сигналів нейрону існують зони - зони тіні, в яких поле вихідних сигналів має складну фрактальну структуру. Визначено вплив зміни ваг та порогу нейрону на існування та розташування таких зон. Виявлено зміни які спостерігаються зі збільшенням довжини вхідних сигналів. Встановлено фрактальну розмірність структур в зонах тіні.

Висновки: отримані загальні властивості нейронів повинні суттєво впливати на властивості нейронних мереж у вигляді наявності зон тіні в яких "відповідь" мережі є надзвичайно чутливою навіть до малих змін вхідних сигналів. Наявність таких зон є надзвичайно важливим фактором який потрібно враховувати при створенні неронних мереж.

Ключові слова: *штучний нейрон, ваги, фрактали, фрактальна розмірність, функція активації, простір вхідntх сигналів, поле вихідних сигналів.*

Надійшла у першій редакції 23.10.2023, в останній – 28.11.2023.
The first version has been received on 23.10.2023, the final version – on 28.11.2023.

DOI: https://doi.org/10.26565/2304-6201-2023-60-04

УДК (UDC) 000.00

Петрушенко Даніїл Олександрович *вчене звання, посада на мові статті*
Харківський національний університет імені В.Н. Каразіна,
майдан Свободи, 4, Харків, Україна, 61022
e-mail: xa12850385@student.karazin.ua
https://orcid.org/0009-0004-1335-2897

Бикова Тетяна Володимирівна *к.т.н., доцент кафедри теоретичної та прикладної системотехніки,*
Харківський національний університет імені В.Н. Каразіна,
майдан Свободи, 4, Харків, Україна, 61022
e-mail: tetiana.bykova@karazin.ua;
https://orcid.org/0000-0003-0484-5388

Актуальні проблеми побудови комп'ютерних мереж

Актуальність: У зв'язку зі зростаючим використанням комп'ютерів та Інтернету в сучасному світі, побудова комп'ютерних мереж є важливим завданням. Однак, існують різні проблеми, які потрібно вирішувати для побудови ефективних та безпечних мереж.

Мета: Дана стаття присвячена огляду актуальних проблем побудови комп'ютерних мереж та методів їх розв'язання.

Методи дослідження: Для написання даної статті було проведено аналіз літературних джерел та розглянуто досвід практичної роботи з побудови комп'ютерних мереж.

Результати: У результаті аналізу було виявлено, що основними проблемами побудови комп'ютерних мереж є безпека, масштабованість, відмовостійкість, ефективність та відповідність до вимог користувачів. Для їх розв'язання було розглянуто різні технології та інструменти для побудови та адміністрування мереж.

Висновки: Побудова комп'ютерних мереж є важливою задачею у сучасному світі, існує кілька проблем, які потрібно вирішувати для забезпечення ефективної та безпечної роботи мережі. Для їх розв'язання використовуються різноманітні методи, які допомагають покращити якість та надійність роботи мереж. В цій статті були розглянуті окремі проблеми побудови комп'ютерних мереж, а також приклад рішення однієї з них, а саме аналіз навантаженості мережі

Ключові слова: *комп'ютерні мережі, безпека, масштабованість, відмовостійкість, ефективність, захист, шифрування, брандмауери, протоколи, алгоритми, дублювання.*.

Як цитувати: Петрушенко Д.О., Бикова Т.В. Актуальні проблеми побудови комп'ютерних мереж. *Вісник Харківського національного університету імені В.Н. Каразіна, серія Математичне моделювання. Інформаційні технології. Автоматизовані системи управління*. 2023. вип. 60. С.36-45. https://doi.org/10.26565/2304-6201-2023-60-04

How to quote: Petrushenko D., Bykova T., "Actual problems of building computer networks", *Bulletin of V.N. Karazin Kharkiv National University, series Mathematical modelling. Information technology. Automated control systems*, vol. 60, pp.36-45, 2023. https://doi.org/10.26565/2304-6201-2023-60-04 [In Ukrainian].

1 Актуальність

Актуальність даної статті полягає в тому, що зростаюче використання комп'ютерів та Інтернету в сучасному світі призводить до збільшення значення побудови ефективних та безпечних комп'ютерних мереж. Однак, на сьогоднішній день існує ряд проблем, пов'язаних з побудовою мереж, таких як безпека, масштабованість, відмовостійкість, ефективність та відповідність до вимог користувачів. Розуміння цих проблем та методів їх розв'язання може допомогти в розробці та побудові більш надійних та ефективних комп'ютерних мереж, що є важливим завданням для багатьох компаній та організацій у всіх сферах діяльності.

Додатково, розвиток технологій та збільшення кількості підключених до мереж пристроїв зумовлює появу нових викликів та проблем. Наприклад, збільшення кількості підключених пристроїв до мережі вимагає від побудованих мереж масштабованості та ефективності, а також додаткових засобів для захисту мережі від зловмисників та шкідливого програмного забезпечення.

Крім того, існує проблема стійкості мережі до відмов, яка важливою для високо навантажених мереж, таких як мережі провайдерів інтернет-послуг. Неправильна побудова мережі може призвести до недоступності даних та послуг, що може призвести до серйозних наслідків для користувачів.

Отже, зважаючи на зростаючу важливість комп'ютерних мереж у сучасному світі, розуміння актуальних проблем та методів їх розв'язання має велике значення для розробників та користувачів мереж. Відповідність мережі до вимог користувачів, ефективність та безпека є ключовими чинниками, які слід враховувати при побудові комп'ютерних мереж.

2 Мета

Метою дослідження є аналіз актуальних проблем побудови комп'ютерних мереж, вивчення методів та технологій, що використовуються для розв'язання цих проблем, а також визначення важливості ефективної побудови мережі та її стійкості до відмов. Крім того, метою є розгляд основних чинників, які впливають на ефективність та безпеку комп'ютерних мереж, таких як масштабованість, маршрутизація, захист від зловмисників та інших загроз. Результати дослідження можуть бути корисні для розробників мереж, адміністраторів мереж та користувачів, які бажають зрозуміти, як побудувати ефективну та безпечну комп'ютерну мережу.

3 Методи дослідження

Для досягнення мети дослідження будуть використовуватися наступні методи дослідження:

1. Аналіз наукової літератури та документації, що стосується побудови комп'ютерних мереж.
2. Огляд існуючих технологій та інструментів для побудови та адміністрування мереж.
3. Вивчення технологій та методів масштабування мереж.
4. Аналіз методів маршрутизації, визначення найбільш оптимальних шляхів передачі даних.
5. Вивчення принципів захисту мереж від зловмисників та інших загроз.
6. Розгляд практичних прикладів побудови мереж та їх ефективності.

Використання цих методів дослідження дозволить отримати глибокий розуміння актуальних проблем побудови комп'ютерних мереж та знайти оптимальні шляхи їх вирішення.

4 Аналіз існуючих методів побудови комп’ютерних мереж.

Коли справа доходить до побудови комп’ютерних мереж, існує кілька існуючих методів, які зазвичай використовуються. Одним із найбільш традиційних методів є використання ієрархічної архітектури мережі, яка базується на еталонній моделі, що називається моделлю взаємодії відкритих систем (OSI) [1]. Цей метод включає в себе поділ мережі на різні рівні, кожен із яких виконує свою особливу функцію, і все ще широко використовується сьогодні. Однак цей метод має деякі обмеження, такі як негнучкість і складність масштабування [2].

Ще один метод, який набув популярності в останні роки, — хмарні мережі, які включають використання технологій хмарних обчислень для побудови та керування мережами. Цей метод базується на ідеї забезпечення зручного мережевого доступу до загального пулу обчислювальних ресурсів [3]. Хмарна мережа пропонує кілька переваг, таких як масштабованість, гнучкість і економічна ефективність, але вона також має деякі недоліки, такі як проблеми безпеки та потенційні проблеми з продуктивністю [4].

Програмно-визначена мережа (SDN) є відносно новим методом побудови комп’ютерних мереж, який привернув значну увагу в останні роки [5]. Цей метод передбачає відокремлення площини керування мережею від її площини даних, що забезпечує більш централізоване та програмоване керування мережею [6]. SDN пропонує кілька переваг, таких як підвищена гнучкість і масштабованість, але вона також має деякі проблеми, такі як потреба в спеціальних навичках і потенційні ризики безпеки [7][8]. Незважаючи на ці проблеми, SDN стає все більш популярним і, як очікується, відіграватиме значну роль у майбутньому комп’ютерних мереж.

5 Існуючі технології та інструменти для побудови та адміністрування мереж

Існує безліч технологій та інструментів для побудови та адміністрування комп'ютерних мереж. Нижче розглянемо деякі з них:

- Cisco Networking Academy: це програма, розроблена компанією Cisco, що дозволяє здобути практичні знання з побудови та адміністрування мереж. Програма пропонує онлайн-курси з

побудови мереж, налаштування маршрутизаторів та комутаторів, а також курси з кібербезпеки та мережевого проектування.

- Wireshark: це безкоштовний інструмент для аналізу мережевого трафіку. Він дозволяє переглядати та аналізувати пакети, що проходять через мережу, та визначати проблеми з її роботою.

- Microsoft Azure: це хмарна платформа від Microsoft, яка дозволяє побудувати та керувати мережами в хмарі. Вона має вбудовані інструменти для моніторингу та керування мережами, а також можливість налаштування віртуальних приватних мереж.

- Docker: це інструмент для контейнеризації додатків, який дозволяє запускати та керувати додатками в різних середовищах. Цей інструмент може бути використаний для побудови та керування мережевими додатками.

- Nagios: це безкоштовний інструмент для моніторингу мереж та серверів. Він дозволяє контролювати різні параметри мережі, такі як доступність серверів, використання ресурсів та швидкість передачі даних.

Оглядаючи існуючі технології та інструменти, можна знайти оптимальний варіант для побудови та адміністрування мережі з урахуванням конкретних потреб користувачів.

6 Проблема масштабування та її вирішення

Однією з ключових проблем побудови комп'ютерних мереж є масштабування. Мережі повинні бути здатні розширюватися для забезпечення зростаючих потреб користувачів та підтримки нових функціональних вимог. Далі будуть описані найефективніші методи масштабування, які наразі використовуються у більшості сучасних комп’ютерних мережах.

6.1. Горизонтальне та вертикальне масштабування

Горизонтальне та вертикальне масштабування - це два основних методи масштабування комп'ютерних мереж.

Вертикальне масштабування означає збільшення потужності обладнання, що використовується в мережі. Це може бути досягнуто шляхом додавання нових процесорів, пам'яті, жорстких дисків або інших компонентів до існуючих серверів. Якщо ресурси на сервері вичерпані, його можна замінити більш потужним. Вертикальне масштабування є дорожчим за горизонтальне, оскільки нове обладнання зазвичай дорожче, ніж просто додавання нових серверів.

Горизонтальне масштабування передбачає збільшення кількості серверів у мережі. Це може бути досягнуто шляхом додавання нових серверів або машин до мережі, які можуть виконувати різні функції. Горизонтальне масштабування зазвичай дешевше за вертикальне, оскільки можна використовувати більш дешеві компоненти, а також через те, що можна використовувати віртуалізацію та контейнеризацію для ефективнішого використання ресурсів сервера.

Кожен з цих методів масштабування має свої переваги та недоліки, і вибір методу залежить від конкретних потреб мережі та обмежень бюджету.

6.2. Віртуалізація

Віртуалізація - це технологія, яка дозволяє запускати багато віртуальних комп'ютерів на одному фізичному сервері. Вона є ключовою технологією для будь-якої інфраструктури, що масштабується. Завдяки віртуалізації можна ефективно використовувати ресурси серверів, зменшити кількість фізичних серверів та спростити процеси адміністрування.

У контексті побудови комп'ютерних мереж віртуалізація може бути використана для створення віртуальних мереж з окремими віртуальними машинами, що запускаються на різних серверах. Це забезпечує більшу гнучкість в плану розгортання та управління мережами, що масштабуються.

Однією з основних переваг віртуалізації є можливість відокремлення ресурсів, що забезпечує високу рівень ізоляції та безпеки. Крім того, віртуалізація дає можливість швидко створювати та розгортати нові віртуальні машини, що робить процес розширення мережі більш простим та ефективним.

Проте, віртуалізація має свої недоліки. Вона може вплинути на продуктивність, особливо якщо використовуються віртуальні машини з високими вимогами до ресурсів. Також, віртуалізація потребує великої кількості ресурсів на господарському сервері, що може збільшити вартість побудови та управління мережами.

6.3. Горизонтальне та вертикальне масштабування

Кластеризація - це технологія, що дозволяє об'єднувати декілька комп'ютерів в єдину систему, яка працює як один цілий. Кожен комп'ютер у кластері називається вузлом і має свою власну пам'ять та процесор. Управління вузлами здійснюється з центрального вузла, який координує роботу всієї системи.

Кластеризація дозволяє покращити продуктивність системи, забезпечити надійність та зменшити вартість. Завдяки розподіленому обчисленню та резервному копіюванню даних на кількох вузлах, кластери дозволяють збільшити швидкість обробки інформації та забезпечити безперебійну роботу системи.

6.4. Хмарні технології

Хмарні технології дозволяють користувачам використовувати обчислювальні ресурси з розподіленої мережі серверів, що дозволяє підвищити масштабність та забезпечити високу доступність.

Хмарні технології - це технології, що дозволяють користувачам отримувати доступ до обчислювальних ресурсів, програмного забезпечення та сервісів через Інтернет. За допомогою хмарних технологій можна зберігати та обробляти дані, виконувати різні обчислювальні процеси, а також розгортати та керувати інфраструктурою.

Однією з найбільш важливих переваг хмарних технологій є їх масштабованість та гнучкість. За потреби можна легко збільшувати або зменшувати кількість ресурсів, що використовуються, тим самим забезпечуючи оптимальне використання обчислювальної потужності. Крім того, за допомогою хмарних технологій можна забезпечити високу доступність та надійність системи, а також захист від зламів та крадіжок даних.

За допомогою хмарних технологій можна створювати та розгортати різноманітні додатки, віртуальні машини, веб-сайти та інші ресурси, що використовуються в Інтернеті. Крім того, хмарні технології дозволяють економити на обладнанні та інфраструктурі, оскільки вони забезпечують доступ до обчислювальних ресурсів в режимі "віддаленого доступу".

6.5. Протоколи маршрутизації

Протоколи маршрутизації є важливою складовою будь-якої комп'ютерної мережі. Вони використовуються для визначення найкоротшого шляху між вузлами мережі та передачі даних від одного вузла до іншого. Деякі з найпоширеніших протоколів маршрутизації включають:

- OSPF (Open Shortest Path First) - цей протокол маршрутизації використовується для маршрутизації в мережах IP. Він визначає найкоротший шлях між джерелом та призначенням, використовуючи метрики, такі як пропускна здатність та вартість маршруту.
- BGP (Border Gateway Protocol) - цей протокол маршрутизації використовується для маршрутизації між різними автономними системами (AS). Він дозволяє визначати найкоротший шлях між AS та встановлювати маршрути між ними.
- RIP (Routing Information Protocol) - цей протокол маршрутизації використовується для маршрутизації в невеликих мережах. Він використовує відстань як метрику та може підтримувати до 15 маршрутів.
- EIGRP (Enhanced Interior Gateway Routing Protocol) - цей протокол маршрутизації використовується для маршрутизації в мережах IP. Він використовує кілька метрик, таких як пропускна здатність та затримка, для визначення найкоротшого шляху між джерелом та призначенням.

7. Принципи захисту мереж від зловмисників та інших загроз

Захист комп’ютерних мереж від зловмисників та інших загроз є критично важливим аспектом сучасної комп’ютерної техніки. Існують фундаментальні принципи, які повинні бути реалізовані для забезпечення безпеки комп’ютерних мереж. Одним із таких принципів є впровадження надійних політик паролів і процедур аутентифікації. Це передбачає встановлення надійних паролів, які важко вгадати, і впровадження багатофакторної аутентифікації, щоб гарантувати, що лише авторизовані користувачі можуть отримати доступ до мережі [9]. Впроваджуючи ці заходи, ризик несанкціонованого доступу до мережі значно знижується, а мережа стає краще захищеною.

Регулярне оновлення та виправлення програмного та апаратного забезпечення є ще одним важливим принципом захисту комп’ютерних мереж. Це передбачає підтримку всього

програмного та апаратного забезпечення в актуальному стані за допомогою останніх виправлень безпеки та оновлень, щоб гарантувати оперативне усунення будь-яких вразливостей [10]. Відмова від оновлення та виправлення програмного та апаратного забезпечення може зробити мережу відкритою для атак зловмисників та інших зловмисників [11]. Завдяки регулярному оновленню та виправленню програмного та апаратного забезпечення мережа краще захищена від відомих вразливостей і загроз.

Проведення регулярних перевірок безпеки та оцінки ризиків також є важливими для захисту комп'ютерних мереж. Це включає в себе регулярний перегляд заходів безпеки на місці та виявлення будь-яких потенційних вразливостей або слабких місць у мережі [12]. Проводячи регулярні аудити безпеки та оцінки ризиків, організації можуть проактивно виявляти потенційні загрози безпеці та вживати заходів для їх пом'якшення, перш ніж їх можна буде використовувати [13]. Відмова від проведення регулярних перевірок безпеки та оцінки ризиків може зробити мережу вразливою до атак та інших загроз безпеці [14]. Дотримуючись цих фундаментальних принципів, організації можуть краще захистити свої комп'ютерні мережі від зловмисників та інших загроз і забезпечити безпеку своїх даних і систем [15][16].

7.1 Сформульовані принципи захисту

Нижче зазначені загальні рекомендації, яких потрібно притримуватись при побудові та налаштуванні комп'ютерної мережі:

- Аутентифікація і авторизація: Користувачі повинні проходити процедуру аутентификации для входу в мережу, і їхні дії повинні бути авторизовані на основі рівня доступу.
- Шифрування даних: Шифрування може бути застосовано для захисту конфіденційної інформації в мережі від несанкціонованого доступу.
- Встановлення мережевої політики: Мережева політика повинна бути встановлена для контролю доступу до мережі, а також для визначення правил використання мережевих ресурсів.
- Захист від вірусів і шкідливих програм: Мережа повинна бути захищена від вірусів і шкідливих програм, що можуть вбудовуватися в мережу через інтернет, електронну пошту або зовнішні носії даних.
- Система виявлення інтрузій: Система виявлення інтрузій повинна бути встановлена, щоб виявляти будь-які ненормальні активності в мережі, які можуть вказувати на потенційну загрозу.
- Захист від DoS атак: Захист від атак DoS (атак, що спрямовані на перевантаження мережі або окремих комп'ютерів) повинен бути встановлений, щоб запобігти перериванням роботи мережі.
- Резервне копіювання і відновлення: Резервне копіювання даних в мережі повинно бути встановлено, щоб запобігти втраті даних в разі виникнення проблем.
- Навчання користувачів: Навчання повинно включати основні принципи безпеки мережі, які включають в себе створення надійних паролів, уникнення підозрілих електронних листів та посилань, використання антивірусного програмного забезпечення та відмова від відкритих мереж Wi-Fi. Крім того, користувачі повинні знати про найновіші загрози та техніки атак, щоб бути готовими до них.

8 Аналіз навантаженості мережі

Аналіз навантаженості системи - це процес вимірювання та оцінки продуктивності та ефективності системи в умовах збільшення обсягу роботи, зростання кількості користувачів або інших факторів, що можуть вплинути на її функціонування. Цей аналіз може допомогти виявити проблеми та відшукати методи їх вирішення. Цей етап є дуже важливою задачей при побудові комп'ютерної мережі.

8.1 Практичний приклад аналізу навантаженості мережі

Для того, щоб побачити, як на практиці проводиться аналіз мережі, розглянемо комп'ютерну мережу офісної багатоповерхової будівлі, яка має 5 поверхів, де 1-4 це офісні приміщення, а на 5-му знаходяться технічні приміщення.

Комп'ютери на каждому поверсі зібрані в окремі VLAN. Маршрутизатором виступає Cisco 1841. Комутатор ядра Cisco 3650. На кожному поверсі розміщені комутатори доступу Cisco Catalist 2960. Бездротову мережу роздають точки доступу Cisco 3702I. Маршрутизатор роздає на кожнен поверх різні підмережі:

Таблиця 1.1 Список підмереж

Поверхи	VLAN	IP-адреси
1 поверх	vlan 10	192.168.10.0/24(динамічні адреси)
2 поверх	vlan 20	192.168.20.0/24(динамічні адреси)
3 поверх	vlan 30	192.168.30.0/24(динамічні адреси)
4 поверх	vlan 40	192.168.40.0/24(динамічні адреси)

Підмережа для керування мережевими пристроями vlan 50, 192.168.50.0/24 (статичні адреси). Підмережа для керування точками доступу та контроллером wifi vlan 14, 192.168.14.0/24(динамічні адреси). Підмережа офісного wifi vlan 15, 192.168.15.0/24(динамічні адреси). Підмережа гостьового wifi vlan 16, 192.168.16.0/24(динамічні адреси).

Визначившись з параметрами мережі, ми можем перейти до її побудови. Для цього використовуємо кросплатформний інструмент візуального моделювання Cisco Packet Tracer. Результат побудови мережі можете побачити на наступній ілюстрації:

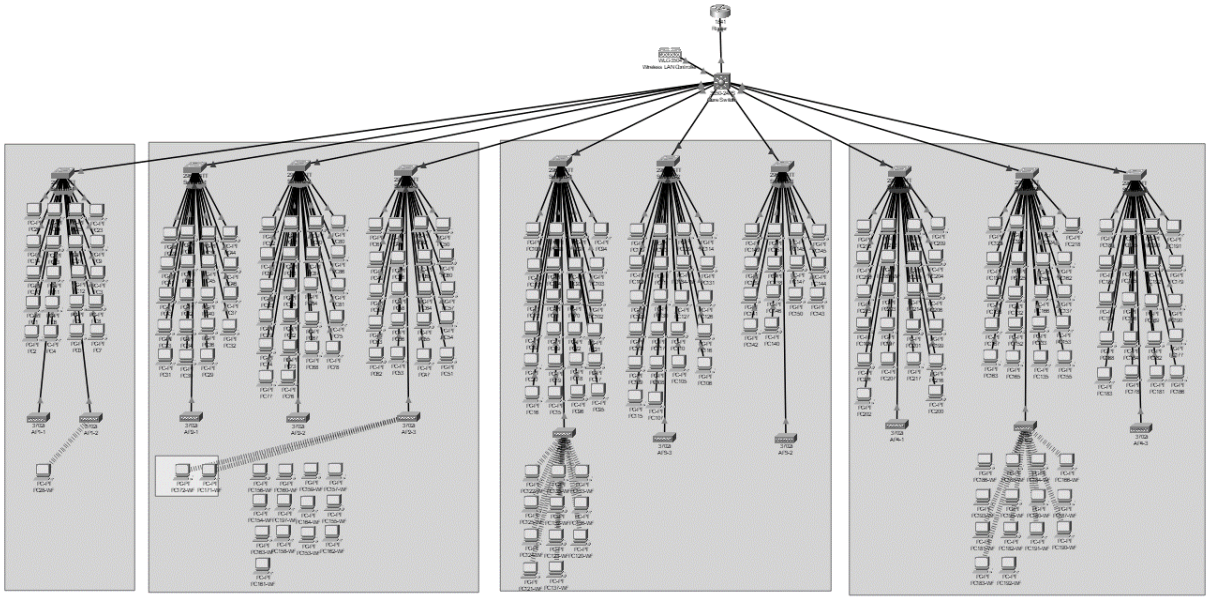


Рис.1.1 Комп'ютерна мережа офісної будівлі

Після опису мережі, з якій будемо працювати в даній роботі перейдемо безпосередньо до аналізу її можливої навантаженості та проведемо модельні експерименти. Спочатку потрібно переконатись у правильності з'єднання вузлів в одному VLAN та перевірити їх доступність. Для цього скористаємось командою ping. Перевіримо для прикладу з'єднання між PC199 та PC217, результат перевірки позитивний:

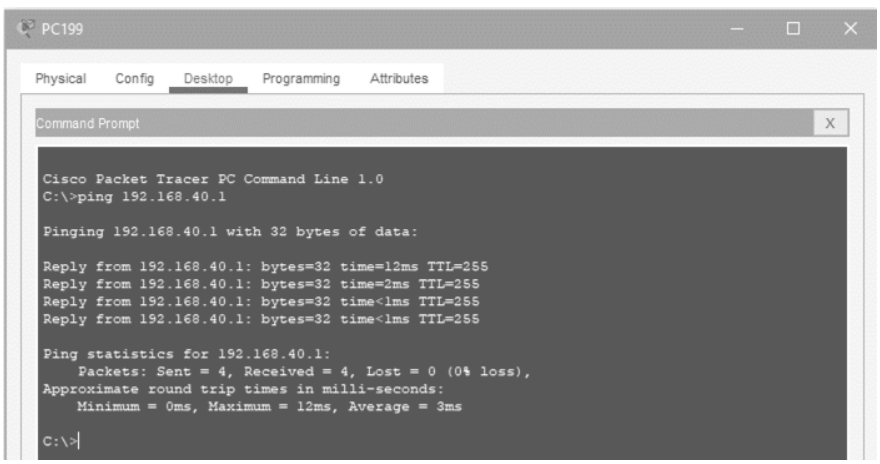


Рис.1.2 Результати експеримента

Наступним кроком проведемо схожий експеримент, але з більшою кількістю пакетів. Для цього я використовую вбудовану утиліту Traffic Generator, вкажемо розмір пакета – 1000 байт, а далі будемо збільшувати з кожним кроком на 1000, поки пакет не досягне максимального розміру, який дорівнює 1000 байт. Вікно налаштувань проілюстровано на рисунку 1.3:

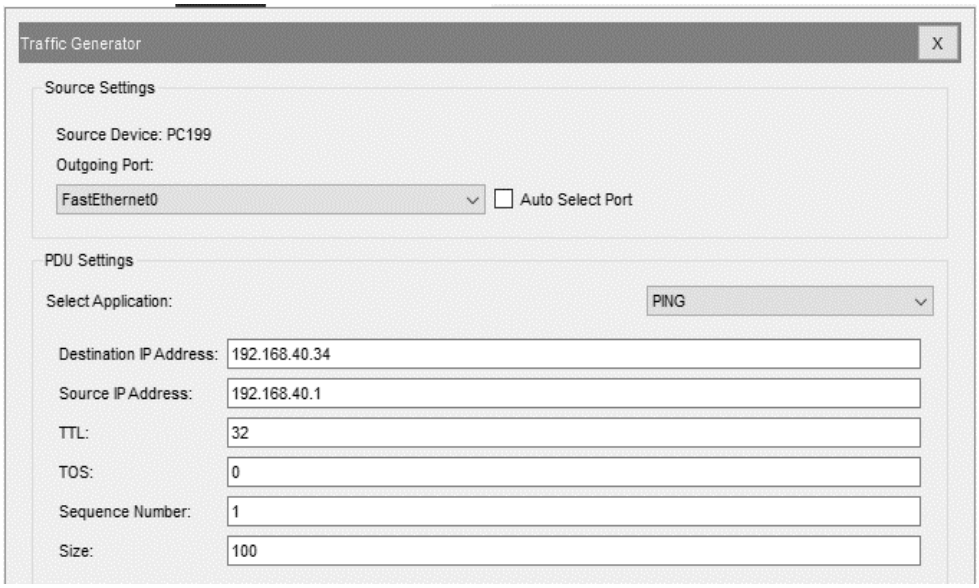


Рис.1.3 Утиліта Packet Tracer

Отримані результати ви можете побачити в таблиці:

Таблиця 1.1 Список підмереж

Номер експерименту	Розмір пакетів, байт	Пакетів втрачено всього, шт
1	1000	0
2	2000	0
3	3000	0
4	4000	0
5	5000	1
6	6000	1
7	7000	1
8	8000	1
9	9000	2
10	10000	2
11	11000	2
Номер експерименту	Розмір пакетів	Пакетів втрачено всього, шт
12	12000	3
13	13000	3
14	14000	4
15	15000	5

Отримані результати кажуть нам про те, що при максимальних навантаженнях ми отримуємо відмови, а саме при розмірі пакету від 14000 відмови були під час всіх експериментів

8.1 Вирішення проблеми навантаженності мережі

Існує кілька способів вирішення проблеми навантаженості мережі, зокрема:

- Підвищення пропускної здатності мережі: це можна зробити шляхом встановлення нових комутаторів, маршрутизаторів та іншого мережевого обладнання з вищою швидкістю передачі даних.

- Використання технологій компресії даних: це дозволяє зменшити розмір передаваних даних, що зменшує навантаження на мережу.

- Розширення мережі: це можна зробити шляхом додавання нових вузлів до мережі або підключення до мережі додаткових мережевих ресурсів, таких як хмарні ресурси.

- Оптимізація мережевого трафіку: це включає в себе використання різних технологій, таких як кешування, балансування навантаження та використання різних протоколів маршрутизації для зменшення навантаження на мережу.

- Обмеження доступу до мережі: це можна зробити шляхом встановлення обмежень на швидкість передачі даних для окремих користувачів або груп користувачів.

- Оптимізація даних: це включає в себе зменшення обсягу даних, які передаються по мережі, за допомогою різних методів, таких як стиснення даних, оптимізація протоколів та використання бінарних форматів даних.

- Використання мережевих протоколів, що підтримують QoS (Quality of Service): це дозволяє встановлювати пріоритети для різних видів даних, що передаються по мережі, і забезпечувати високу якість обслуговування для важливих даних.

9 Підсумовування проблем побудови комп'ютерних мереж

Під час дослідження проблеми побудови комп'ютерних мереж було оглянуто та проаналізовано існуючі методи та технології побудови та адміністрування комп'ютерних мереж, варіанти масштабування, захисту мереж від зловмисників та інших загроз та виявлення варіантів вирішення цих проблем і їх особливості (переваги та недоліки).

Також була розглянута проблема навантаженості комп’ютерної мережі, використовуючи практичний приклад, а також наведені варіанти вирішення цієї проблеми

СПИСОК ЛІТЕРАТУРИ

1. СЕРГІЄНКО О. М. Навчально-методичний посібник. Київ: ЕНМП, 2020. 415 с. https://kppk.com.ua/ELLIB/ebook/Segrienko/KM/page6.html
2. Тарантін А. О. АТЕСТАЦІЙНА РОБОТА. Харків: ХНУРЕ, 2019. 90 с. https://openarchive.nure.ua/bitstreams/639aa5aa-119b-4419-a4fd-ba64b2b5cf33/download
3. ВАКАЛЮК Т.А. Хмарні технології в освіті. Житомир: ЖДУ імені Івана Франка 2016, 72 с. https://lib.iitta.gov.ua/706333/1/%D0%9F%D0%BE%D1%81_%D0%A5%D0%A2%D0%9E.PDF
4. Коваленко А. А. Моделі та методи синтезу і реконфігурації архітектур комп'ютерних систем і мереж об'єктів критичного застосування. Харків: Нац. техн. ун-т "Харків. політехн. ін-т"., 2018. – 40 с. https://repository.kpi.kharkov.ua/handle/KhPI-Press/37686
5. БЕРКМАН Л.Н. ПРОГРАМНО-КОНФІГУРОВАНІ МЕРЕЖІ, 2014, 154 с. http://con.dut.edu.ua/index.php/communication/article/view/1152/1087
6. Олифер В., Олифер Н. Компьютерные сети. Принципы, технологии, протоколы : Учебник для вузов. Питер: 5-е изд. СПб, 2016. 992 с. http://www.its.kpi.ua/itm/lgloba/Lists/publications/Attachments/15/(11)--TUD_IBIS_Shill_Globa_NTUU_KPI_camera_ready.pdf
7. Лосев Ю. І., Руккас К. М., Шматков С. І. Комп’ютерні мережі: навч. посіб. / за редакцією Ю. І. Лосева. Харків : ХНУ імені В. Н. Каразіна, 2013. 248 с. https://www.springer.com/gp/book/9783642031205
8. Стеценко І.В. Моделювання систем: навч. посіб. Черкаси: ЧДТУ, 2010. 399 с. https://www.springer.com/gp/book/9783642031205
9. . Амато В. Основы организации сетей Cisco : в 2 кн. / Амато В. – М. : Вильямс, 2002. – 512 с. Кн. 1
10. Амато В. Основы организации сетей Cisco : в 2 кн. / Амато В. – М. : Вильямс, 2002. – 464 с.
11. Сейдаметова З. С. Облачные сервисы в образовании – 2011. – №9. – С. 75–141.
12. З. С. Сейдаметова, С. Н. Сейтвелиева Информационные технологии в образовании. – 2011. – №9. – С. 105–111.

13. Сейдаметова З. С. Облачные технологии и образование / Сейдаметова З. С., Аблялимова Э. И., Меджитова Л. М., Сейтвелиева С. Н., Темненко В. А. [под общ. ред. З. С. Сейдаметовой]. – Симферополь: "ДИАЙПИ", 2012. – 204 с.
14. Семеріков С. О. Хмарні технології навчання: витоки / О. М. Маркова, С. О. Семеріков, А. М. Стрюк. Інформаційні технології і засоби навчання. 2015. №2 (46). С. 29-44. Режим доступу до журн. : http://journal.iitta.gov.ua/index.php/itlt/article/view/1234/916#.VfFO4NLtmko.
15. Стрюк А. М. Система хмаро орієнтованих засобів навчання як елемент інформаційного освітньо-наукового середовища ВНЗ [Електронний ресурс]
16. Стрюк А. М., Рассовицька М. В. Інформаційні технології і засоби навчання. 2014. №4 (42). С. 150-158. Режим доступу до журн.: http://journal.iitta.gov.ua/index.php/itlt/article/view/1087/829.

REFERENCES

1. SERHIENKO O. M. Educational and methodological manual. Kyiv: ENMP, 2020. 415 p. https://kppk.com.ua/ELLIB/ebook/Segrienko/KM/page6.html [In Ukrainian]
2. Tarantin A. O. ASSESSMENT WORK. Kharkiv: Khnure, 2019. 90 p. https://openarchive.nure.ua/bitstreams/639aa5aa-119b-4419-a4fd-ba64b2b5cf33/download [In Ukrainian]
3. VAKALYUK T.A. Cloud technologies in education. Zhytomyr: Ivan Franko State University, 2016, 72 p. [In Ukrainian] https://lib.iitta.gov.ua/706333/1/%D0%9F%D0%BE%D1%81_%D0%A5%D0%A2%D0%9E.PDF
4. Kovalenko A. A. Models and methods of synthesis and reconfiguration of architectures of computer systems and networks of critical application objects. Kharkiv: National technical Kharkiv Polytechnic University, 2018. – 40 p. https://repository.kpi.kharkov.ua/handle/KhPI-Press/37686
5. Berkman L.N. SOFTWARE-CONFIGURED NETWORKS, 2014, 154 p. http://con.dut.edu.ua/index.php/communication/article/view/1152/1087 [In Ukrainian]
6. Olifer V., Olifer N. Computer networks. Principles, technologies, protocols: A textbook for universities. Peter: 5th ed. St. Petersburg, 2016. 992 p. [in Russian] http://www.its.kpi.ua/itm/lgloba/Lists/publications/Attachments/15/(11)--TUD_IBIS_Shill_Globa_NTUU_KPI_camera_ready.pdf
7. Losev Yu. I., Rukkas K. M., Shmatkov S. I. Computer networks: training. manual / edited by Yu. I. Losev. Kharkiv: V.N. Karazin KhNU, 2013. 248 p. https://www.springer.com/gp/book/9783642031205 [In Ukrainian]
8. Stetsenko I.V. Modeling of systems: training. manual Cherkasy: ChDTU, 2010. 399 p. https://www.springer.com/gp/book/9783642031205 [In Ukrainian]
9. . Amato V. Fundamentals of Cisco network organization: in 2 books. / Amato V. – M.: Vyliamc, 2002. – 512 p. - Kn. 1 [in Russian]
10. Amato V. Fundamentals of Cisco network organization: in 2 books. / Amato V. – M.: Vyliamc, 2002. – 464 p. [in Russian]
11. Seydametova Z. S. Cloud services in education - 2011. - No. 9. – P. 75–141. [in Russian]
12. Z. S. Seydametova, S. N. Seitvelyeva Information technologies in education. – 2011. – No. 9. – pp. 105–111. [in Russian]
13. Seydametova Z. S. Cloud technologies and education / Seydametova Z. S., Ablyalymova E. I., Medzhitova L.M., Seitvelyeva S.N., Temnenko V.A. ed. Z. S. Seydametova]. – Simferopol: "DIAIPY", 2012. – 204 p. [In Ukrainian]
14. Semerikov S. O. Cloud learning technologies: origins / O. M. Markova, S. O. Semerikov, A. M. Struyuk // Information technologies and means of education. – 2015. – No. 2 (46). - P. 29-44. – Log access mode. : http://journal.iitta.gov.ua/index.php/itlt/article/view/1234/916#.VfFO4NLtmko. [In Ukrainian]
15. A. M. Striuk. The system of cloud-based learning tools as an element of the informational educational and scientific environment of universities [Electronic resource] [In Ukrainian]

16. /AND. M. Striuk, M. V. Rassovytska // Information technologies and teaching tools. – 2014. – No. 4 (42). - P. 150-158. – Log access mode. : http://journal.iitta.gov.ua/index.php/itlt/article/view/1087/829. [In Ukrainian]

Petrushenko Daniil *student*
V. N. Karazin Kharkiv National University, 4 Svobody Sq., Kharkiv, 61022, Ukraine;

Bykova Tetiana *Associate Professor of the Department of Theoretical and Applied System Engineering,*
V. N. Karazin Kharkiv National University, 4 Svobody Sq., Kharkiv, 61022, Ukraine;

Actual problems of building computer networks

Relevance: In connection with the growing use of computers and the Internet in the modern world, the construction of computer networks is an important task. However, there are various challenges that need to be addressed in order to build efficient and secure networks.

Purpose: This article is devoted to an overview of current problems of building computer networks and methods of their solution.

Research methods: To write this article, an analysis of literary sources was carried out and the experience of practical work in building computer networks was considered.

Results: As a result of the analysis, it was found that the main problems of building computer networks are security, scalability, fault tolerance, efficiency and compliance with user requirements. To solve them, various technologies and tools for building and administering networks were considered.

Conclusions: Building computer networks is an important task in today's world, there are several problems that need to be solved to ensure efficient and secure network operation. Various methods are used to solve them, which help to improve the quality and reliability of networks. This article considered individual problems of building computer networks, as well as an example of a solution to one of them, namely, network load analysis

Keywords: computer networks, security, scalability, fault tolerance, efficiency, protection, encryption, firewalls, protocols, algorithms, duplication.

Keywords: *computer networks, security, scalability, fault tolerance, efficiency, protection, encryption, firewalls, protocols, algorithms, duplication..*

Надійшла у першій редакції 01.10.2023, в останній – 10.11.2023.
The first version has been received on 01.10.2023, the final version – on 10.11.2023.

DOI: https://doi.org/10.26565/2304-6201-2023-60-05

УДК (UDC) 004.94

Тележенко Денис Олександрович *аспірант*
Харківський національний університет імені В.Н. Каразіна,
майдан Свободи, 4, Харків-22, Україна, 61022
e-mail: denisque75@gmail.com
https://orcid.org/0000000283778517

Прогнозування та аналітика у віртуальних розподілених системах: Використання моделей машинного навчання та аналітичних інструментів

Дана наукова стаття присвячена розробці концептуальної моделі синтезу архітектури віртуальних розподілених систем (ВРС). У статті розглядаються ключові аспекти віртуальних розподілених систем, включаючи апаратне забезпечення, гіпервізори, віртуальні машини та модулі управління. Висвітлюються методологічні принципи синтезу архітектури, починаючи від аналізу системних вимог, проектування архітектури, реалізації та тестування, закінчуючи оцінкою та оптимізацією продуктивності ВРС. У статті підкреслюється важливість кожного етапу в цьому процесі, наголошується на необхідності глибокого розуміння системних вимог і вибору відповідних технологій. Особливу увагу в статті приділено ролі гіпервізорів і віртуальних машин у ВРС, їх підключенню до апаратного забезпечення та можливостям управління ресурсами. Ця стаття буде корисною для дослідників і практиків у сфері віртуалізації та обчислювальних систем, які розробляють або оптимізують віртуальні розподілені системи.

Актуальність. Стаття присвячена важливими питаннями, пов'язаними з прогнозуванням та оптимізацією віртуальних розподілених систем, що є ключовим елементом сучасних технологічних інфраструктур. З розвитком обчислювальних технологій та штучного інтелекту, зростає потреба у ефективному управлінні ресурсами та підтримці високої пропускної спроможності в обчислювальних системах.

Мета. Метою цієї наукової роботи є дослідження та аналіз застосування алгоритмів машинного навчання, зокрема LSTM (Long Short-Term Memory) та механізму уваги, для прогнозування та оптимізації віртуальних розподілених систем. Стаття прагне детально розглянути, як ці технології можуть покращити управління ресурсами, забезпечити більш високу ефективність та пропускну спроможність систем, а також проаналізувати, як вони допомагають виявляти потенційні проблеми та оптимізувати розподіл ресурсів, спираючись на точні прогнози та аналіз історичних даних.

Методи дослідження. У даній роботі використовуються різноманітні методи дослідження, які включають теоретичний аналіз та практичне застосування алгоритмів машинного навчання, особливо архітектури LSTM (Long Short-Term Memory) і механізму уваги, для оцінки їх ефективності у прогнозуванні поведінки віртуальних розподілених систем. Методологія включає збір та аналіз великих обсягів даних з віртуальних систем, проведення експериментальних тестувань для оцінки пропускної спроможності та ефективності ресурсів, а також застосування статистичних інструментів для оцінки точності прогнозів.

Результати. Результати дослідження показують, що застосування алгоритмів LSTM (Long Short-Term Memory) та механізму уваги значно покращує здатність віртуальних розподілених систем до ефективного прогнозування та управління ресурсами. Експерименти та аналіз даних виявили, що ці техніки дозволяють точніше аналізувати та передбачати шаблони використання ресурсів, що веде до оптимізації розподілу навантаження та підвищення загальної пропускної спроможності систем. Також було зазначено, що інтеграція механізму уваги з LSTM дозволяє більш детально розуміти довготривалі залежності в даних, що сприяє більш точному прогнозуванню та реагуванню на зміни у використанні ресурсів.

Висновки. Використання алгоритмів LSTM та механізму уваги в значній мірі покращує прогнозування та управління ресурсами віртуальних розподілених систем, відкриваючи нові можливості для їх оптимізації та підвищення ефективності.

Ключові слова: *віртуальні розподілені системи (ВРС), синтез архітектури,* LSTM*, прогнозування навантаження, Input Gate, Forget Gate, Output Gate, механізм уваги.*

Як цитувати: Тележенко Д. О. Прогнозування та аналітика у віртуальних розподілених системах: Використання моделей машинного навчання та аналітичних інструментів. *Вісник Харківського національного університету імені В.Н. Каразіна, серія Математичне моделювання. Інформаційні технології. Автоматизовані системи управління*. 2023. вип. 60. С.46-51. https://doi.org/10.26565/2304-6201-2023-60-05

How to quote: Telezhenko D., “Forecasting and analytics in virtual distributed systems: Using machine learning models and analytical tools”, *Bulletin of V.N. Karazin Kharkiv National University, series Mathematical modelling. Information technology. Automated control systems*, vol. 60, pp.46-51, 2023. https://doi.org/10.26565/2304-6201-2023-60-05 [In Ukrainian]

1. Вступ

У сучасному світі, де обсяги даних та їх складність зростають з кожним днем, віртуальні розподілені системи стають невід'ємною частиною багатьох технологічних процесів. Ці системи відіграють ключову роль у різноманітних галузях, від обчислювального хмарного сервісу до штучного інтелекту та великих даних. Однак, разом з розвитком технологій, зростає і потреба у ефективних інструментах для прогнозування та аналізу поведінки цих систем. Надійність, ефективність та безпека віртуальних розподілених систем залежить від здатності точно прогнозувати їх поведінку у відповідь на змінні умови та запити. [1]

У цій статті ми розглядаємо застосування алгоритму Long Short-Term Memory (LSTM) у контексті віртуальних розподілених систем, що є значущим внеском у сферу комп'ютерних наук і технологій. Наукова новизна полягає в адаптації та інтеграції LSTM для прогнозування та оптимізації поведінки віртуальних розподілених систем, що є важливим аспектом у сучасному світі, де обсяги даних зростають надзвичайно швидко. Віртуальні розподілені системи стають основою численних технологічних процесів, від хмарних обчислень до аналізу великих даних, і їх надійність, ефективність та безпека безпосередньо залежать від точності та ефективності прогнозування їх поведінки.

Сучасні методи машинного навчання та аналітичні інструменти відкривають нові горизонти у цій області. Вони дозволяють не лише збирати та аналізувати величезні обсяги даних, а й робити точні прогнози щодо поведінки системи. Цей підхід допомагає виявити потенційні проблеми до їх виникнення, оптимізувати ресурси та підвищити ефективність роботи системи. [2]

В цій роботі ми зосереджуємося на детальному аналізі використання LSTM в різноманітних сценаріях, що включають прогнозування навантаження на сервери та оптимізацію розподілу ресурсів у віртуальних розподілених системах. Ми демонструємо, як LSTM може використовуватися для точного прогнозування поведінки системи, що сприяє підвищенню ефективності та надійності. Окрім цього, ми досліджуємо інтеграцію механізму уваги (attention mechanism) з LSTM, що дозволяє моделі більш точно фокусуватися на релевантних даних, враховуючи специфіку розподілених систем.

Завдяки цьому аналізу можна буде краще оцінити, яким чином сучасні технології машинного навчання та аналітики можуть вдосконалити процеси управління та оптимізації віртуальними розподіленними системами.

2. Застосування алгоритму LSTM в віртуальних розподілених системах.

Оптимізація ресурсів в обчислювальних віртуальних розподілених системах за допомогою машинного навчання є ключовою для забезпечення максимальної ефективності та пропускної спроможності у великомасштабних розподілених обчисленнях. Така система може аналізувати використання ресурсів додатками, щоб визначити найкращий додатковий ресурс для кожного. Для даної задачі можна використовувати алгоритм LSTM (Long Short-Term Memory). [3] Це архітектура рекурентної нейронної мережі (RNN), яка широко використовується в глибокому навчанні. Він чудово вловлює довготривалі залежності, що робить його ідеальним для завдань прогнозування послідовності. [4] Прогнозування навантаження на сервери є важливим аспектом управління ресурсами в хмарних обчисленнях та віртуальних розподілених системах.

Основним поняттям алгоритму LSTM є клітинний стан (cell state), що допомагає моделі LSTM в навчанні та запам'ятовуванні інформації протягом довгих послідовностей. Клітинний стан в LSTM схожий на конвеєр, який працює через всю послідовність вхідних даних та переносить інформацію у часі. [5] Він дозволяє LSTM вибірково додавати чи видаляти інформацію з клітинного стану, використовуючи спеціалізовані структури, що називаються гейтами. Три основні компоненти, які складають клітину LSTM, це:

- **Гейт вводу (Input Gate):** Цей гейт визначає, яку інформацію з поточного вводу слід додати до клітинного стану. Він бере поточний вхід та попередній прихований стан як вхідні дані, обробляє їх через сигмоїдну функцію активації, щоб отримати значення між 0 та 1 (0 означає "відкинути", а 1 означає "зберегти"), а потім через тангенс гіперболічний активації, щоб отримати нові кандидатські значення для клітинного стану. Ці значення потім множаться на вихід гейту вводу, щоб визначити, що додати до клітинного стану.

- **Гейт забуття (Forget Gate):** Гейт забуття визначає, яку інформацію з попереднього клітинного стану слід забути чи зберегти. Він бере попередній прихований стан та поточний вхід, обробляє їх аналогічно гейту вводу та виробляє значення між 0 та 1, щоб визначити, які частини попереднього клітинного стану слід забути (0) або зберегти (1).
- **Гейт виведення (Output Gate):** Гейт виведення визначає, яку інформацію з поточного клітинного стану слід використовувати для створення виведення клітини LSTM. Він бере поточний вхід та попередній прихований стан, обробляє їх і комбінує з клітинним станом для створення поточного прихованого стану. Прихований стан потім передається наступному кроку часового ряду, і його також можна використовувати як виведення LSTM, якщо це потрібно. [6]

Модель LSTM може бути описана математично за допомогою набору рівнянь, що керують її роботою:

$$it = \sigma(W_i \cdot [h_{t-1}] + b_i) \tag{2.1}$$

Гейт вводу (Input Gate). Визначає, яка нова інформація зберігається у стані клітини. Де it визначає, яка нова інформація повинна бути додана до стану клітини

$$ft = \sigma(W_f \cdot [h_{t-1}] + b_f) \tag{2.2}$$

Гейт забуття (Forget Gate). Цей гейт вирішує, яка інформація буде відкинута зі стану комірки. Де ft використовується для визначення, яка інформація з попереднього стану клітини C_{t-1} повинна бути "забута" або відкинута.

$$\begin{aligned} \hat{C}_t &= tanh(W_C \cdot [h_{t-1}] + b_C) \\ C_t &= f_t \cdot C_{t-1} + i_t \cdot \hat{C}_t \end{aligned} \tag{2.3}$$

Представляє нові кандидатські значення, які можуть бути додані до стану. Де $\hat{C}_t$ кандидат на оновлення стану клітини, що створює список кандидатів на оновлення, що можуть бути додані до стану клітини. C_t – оновлення стану клітини, що поєднує інформацію з гейту забуття та вхідного гейту для оновлення стану клітини.

$$\begin{aligned} o_t &= \sigma(W_o \cdot [h_{t-1}] + b_o) \\ h_t &= o_t \cdot tanh(C_t) \end{aligned} \tag{2.4}$$

Гейт виведення (Output Gate). Цей гейт контролює вивід стану клітини. Де, o_t визначає, яка частина стану клітини повинна бути виведена на наступний шар або використана як вихід. h_t – це фактичний вихід одиниці LSTM, що базується на оновленому стані клітини та вихідному гейті.

У цих рівняннях $\boldsymbol{\sigma}$ - це сигмоїдна активаційна функція, яка перетворює вхідні значення у діапазон від 0 до 1, а $\boldsymbol{tanh}$ - гіперболічний тангенс, який нормалізує значення у діапазон від -1 до 1. Ваги W та зміщення b визначають силу зв'язків між різними одиницями у мережі та їх вплив на гейти та стан клітини. А $[h_{t-1}]$ означає вихід LSTM-одиниці з попереднього кроку часу. Це ключовий елемент у рекурентних нейронних мережах, який дозволяє мережі "пам'ятати" інформацію з минулих кроків.

3. Прогнозування навантаження на сервери у віртуальних розподілених системах.

Прогнозування навантаження на сервери у віртуальних розподілених системах є критичним аспектом для підтримки та розподілу завдань. LSTM (Long Short-Term Memory), у поєднанні з механізмом уваги (attention mechanism), становить передовий підхід у цій галузі. [7] Механізмом уваги це техніка, яка дозволяє моделі зосереджуватися на певних частинах вхідної послідовності при генерації певної частини вихідної послідовності. Цей механізм особливо корисний у завданнях, пов'язаних із послідовними даними, такими як обробка природної мови або аналіз часових рядів. Механізм уваги дозволяє моделі призначати різні ваги різним частинам вхідних даних, вказуючи, скільки "уваги" слід приділити кожній частині під час виконання обчислення.

Цей процес допомагає моделі вловлювати залежності та важливі особливості у даних, особливо в сценаріях, де вхідна послідовність є довгою, а різні частини послідовності по-різному впливають на результат. Наприклад, у перекладі мов механізм уваги допомагає моделі зосередитися на відповідних словах у джерельному реченні при перекладі певного слова на цільову мову. Механізм уваги у машинному навчанні можна описати за допомогою формул, які ілюструють, як модель визначає, на яку частину вхідних даних зосередити увагу.

Розрахунок оцінок уваги:

$$e_{t,i} = f(decoder\_state_t, encoder\_state_i) \tag{3.1}$$

де, $e_{t,i}$ це оцінка уваги для i-го елементу вхідної послідовності на часовому кроці t. Функція f може бути, наприклад, добутком векторів або мережею перцептронів.

$$\alpha_{t,i} = \frac{exp(e_{t,i})}{\sum_{j=1}^{T_x} exp(e_{t,j})} \tag{3.2}$$

Нормалізовані ваги уваги $\alpha_{t,i}$ визначають, скільки "уваги" слід приділити кожному елементу вхідних даних.

$$context_t = \sum_{j=1}^{T_x} \alpha_{t,i} \times encoder\_outputi \tag{3.3}$$

Контекстний вектор $context_t$ утворюється як зважена сума вихідних даних кодувальника, де ваги визначаються на основі ваг уваги.

Ці кроки уможливлюють моделі динамічно вибирати, на яку частину вхідної послідовності зосередити увагу при генерації кожного елементу вихідної послідовності, покращуючи здатність моделі обробляти довгі та складні послідовності даних.

4. Архітектура прогнозування навантаження на сервери у віртуальних розподілених системах.

На рисунку 4.1 зображена архітектура прогнозування навантаження на сервери у віртуальних розподілених системах. Розглянемо призначення різних компонентів архітектури ня на сервери у віртуальних розподілених системах:

- Символ 1 (рис. 4.1), містить вхідний набір даних, який містить інформацію про навантаження на сервери віртуальних розподілених систем (час, дані заліза, навантаження, температуру і т.д.).
- Символ 2 (рис. 4.1), процес нормалізує або масштабує дані таким чином, щоб всі значення знаходились у певному діапазоні, зазвичай від 0 до 1. Це полегшує тренування моделі, оскільки масштабовані дані зазвичай сприяють кращій збіжності.
- Символ 3 (рис. 4.1), SMOTE (Synthetic Minority Over-sampling Technique): цей метод використовується для боротьби з дисбалансом класів у наборі даних. Він створює синтетичні приклади міноритарного класу для вирівнювання кількості прикладів між класами, що допомагає уникнути упередженості моделі до домінуючого класу.
- Символ 4 (рис. 4.1), перетворення, де дані перетворюються (reshaping) для подачі у LSTM шари. LSTM мережі потребують вхідних даних у формі тривимірного масиву (зазвичай [приклади, часові кроки, ознаки]), тому дані мають бути переформатовані відповідно.
- Символ 5 (рис. 4.1), набір для навчання (Train Dataset) – це частина даних, яка використовується для тренування моделі. Вона проходить через LSTM шари для вивчення залежностей в часі та ідентифікації шаблонів.
- Символ 6 (рис. 4.1), позначає LSTM модель.
- Символ 7 (рис. 4.1), позначає ворота забування (forgate gate) в LSTM, які вирішують, яку інформацію з попереднього стану слід відкинути.
- Символ 8 (рис. 4.1), позначає ворота модуляції вхідних (input modularity gate) даних в LSTM, які регулюють внесок нової інформації в стан комірки
- Символ 9 (рис. 4.1), позначає ворота вводу (input gate) в LSTM, які контролюють, яка нова інформація додається до стану комірки.

- Символ 10 (рис. 4.1), позначає стан комірки в LSTM, який зберігає інформацію про весь час тренування.

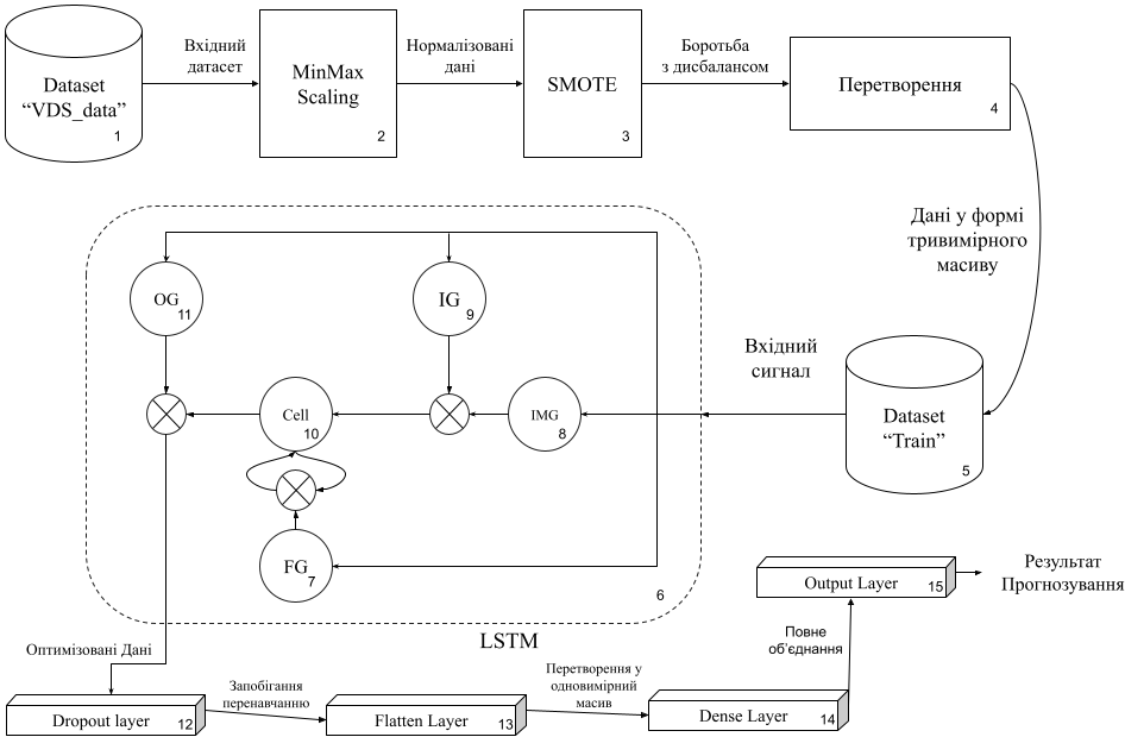


Рис. 4.1 Архітектура прогнозування навантаження на сервери у віртуальних розподілених системах

- Символ 11 (рис. 4.1), позначає ворота виводу (output gate) в LSTM, які визначають, яка інформація передається до виходу з стану комірки.
- Символ 12 (рис. 4.1), позначає шар (Dropout Layer), який запобігає перенавчанню шляхом випадкового відключення деяких нейронів під час тренування.
- Символ 13 (рис. 4.1), позначає шар (Flattern Layer), який перетворює вихідні дані з LSTM шарів у одновимірний масив для подальшої обробки.
- Символ 14 (рис. 4.1), позначає шар нейронний (Dense Layer) для подальшої обробки інформації перед передачею до вихідного шару.
- Символ 15 (рис. 4.1), позначає шар для виведення кінцевого прогнозу або результату класифікації.

Висновок.

У статті розглядається використання алгоритму LSTM (Long Short-Term Memory) для оптимізації віртуальних розподілених систем, зокрема для прогнозування навантаження на сервери. Основні нововведення та аспекти статті включають:

- Застосування LSTM в обчислювальних віртуальних розподілених системах: Підкреслюється важливість LSTM для аналізу використання ресурсів додатками і визначення оптимального розподілу ресурсів для кожного додатку.
- Ключові компоненти LSTM: Стаття детально описує клітинний стан (cell state) і його роль у навчанні LSTM, а також три головні гейти: гейт вводу (Input Gate), гейт забуття (Forget Gate) і гейт виведення (Output Gate).
- Математичний опис моделі LSTM: В статті подано набір рівнянь, які використовуються для опису роботи LSTM, включаючи процеси в гейтах та оновлення клітинного стану.
- Механізм уваги у поєднанні з LSTM: Обговорюється, як механізм уваги може покращити здатність LSTM моделей до обробки довгих та складних послідовностей даних.

Описуються процеси розрахунку оцінок уваги, нормалізації оцінок та формування контекстного вектора.

- Підсумовується, як ці технології можуть підвищити точність прогнозів у контексті віртуальних розподілених систем, сприяючи більш ефективному управлінню та розподілу ресурсів.

СПИСОК ЛІТЕРАТУРИ

1. Sarker IH, Furhad MH, Nowrozy R. Ai-driven cybersecurity: an overview, security intelligence modeling and research directions. SN Comput Sci. 2021;2:1–18.
2. Zhang C, Lu Y. Study on artificial intelligence: the state of the art and future prospects. J Industrial Inform Integr. 2021;23: 100224.
3. Aibin M (2020) LSTM for Cloud Data Centers Resource Allocation in Software-Defined Optical Networks. In: 2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON). IEEE, New York, p 0162–0167
4. IBM. (n.d.). Recurrent Neural Networks (RNN) - Overview. Retrieved from https://www.ibm.com/topics/recurrent-neural-networks
5. J. Kumar, R. Goomer, A.K. Singh, Long short term memory recurrent neural network (lstm-rnn) based workload forecasting model for cloud datacenters. Procedia Comput Sci 125, 676–682 (2018)
6. Ashawa, M., Douglas, O., Osamor, J. et al. Improving cloud efficiency through optimized resource allocation technique for load balancing using LSTM machine learning algorithm. J Cloud Comp 11, 87 (2022). https://doi.org/10.1186/s13677-022-00362-x
7. Zhu, Y., Zhang, W., Chen, Y. et al. A novel approach to workload prediction using attention-based LSTM encoder-decoder network in cloud environment. J Wireless Com Network 2019, 274 (2019). https://doi.org/10.1186/s13638-019-1605-z

Telezhenko Denys *PhD student*
V.N. Karazin Kharkiv National University, Svobody Square, 4,
Kharkiv-22, Ukraine, 61022

Forecasting and analytics in virtual distributed systems: Using machine learning models and analytical tools

This scientific article is devoted to the development of a conceptual model for the synthesis of the architecture of virtual distributed systems (VDS). The article examines key aspects of virtual distributed systems, including hardware, hypervisors, virtual machines, and management modules. The methodological principles of architecture synthesis are highlighted, starting from the analysis of system requirements, architecture design, implementation and testing, ending with the evaluation and optimization of VRS performance. The article emphasizes the importance of each stage in this process, emphasizes the need for a deep understanding of system requirements and the selection of appropriate technologies. The article pays special attention to the role of hypervisors and virtual machines in VRS, their connection to hardware and resource management capabilities. This article will be useful for virtualization and computing researchers and practitioners who are designing or optimizing virtual distributed systems. The article is devoted to important issues related to forecasting and optimization of virtual distributed systems, which is a key element of modern technological infrastructures. With the development of computing technologies and artificial intelligence, the need for effective resource management and support of high throughput in computing systems is increasing. The purpose of this scientific work is to research and analyze the application of machine learning algorithms, in particular LSTM (Long Short-Term Memory) and the attention mechanism, for forecasting and optimization of virtual distributed systems. The paper seeks to examine in detail how these technologies can improve resource management, provide higher efficiency and throughput of systems, and analyze how they help identify potential problems and optimize resource allocation based on accurate forecasts and historical data analysis. This paper uses various research methods, which include
Keywords: *virtual distributed systems (VDS), architecture synthesis, LSTM, load forecasting, Input Gate, Forget Gate, Output Gate, attention mechanism.*

Надійшла у першій редакції 01.10.2023, в останній – 07.11.2023.
The first version has been received on 01.10.2023, the final version – on 07.11.2023.

DOI: https://doi.org/10.26565/2304-6201-2023-60-06

УДК (UDC) 004.94

Тітаренко Тімур *магістр; Харківський національний університет імені В .Н. Каразіна, майдан Свободи, 4, Харків, Україна, 61022*
e-mail: tima.tytarenko.001@gmail.com
https://orcid.org/0000-0001-6417-151X

Толстолузька Олена Геннадіївна *д. т. н., с. н. с.; професор кафедри теоретичної та прикладної системотехніки; Харківський національний університет імені В.Н. Каразіна, майдан Свободи, 4, Харків-22, Україна, 61022;*
e-mail: elena.tolstoluzka@karazin.ua;
https://orcid.org/0000-0003-1241- 7906.

Узлов Дмитро Юрійович *к.т.н., доцент закладу вищої освіти кафедри теоретичної та прикладної інформатики*
Харківський національний університет імені В .Н. Каразіна, майдан Свободи, 4, Харків, Україна, 61022
e-mail: dmytro.uzlov@karazin.ua
https://orcid.org/0000-0003-3308-424X

Модель нейронної мережі для цензурування текстових даних

Актуальність: в умовах стрімкого розвитку інтернет-комунікацій та зростання обсягів текстового контенту, актуальність роботи обумовлена необхідністю забезпечення ефективного цензурування текстових даних. Особливо в онлайн середовищі, де важливо забезпечити безпеку та етичність спілкування.
Мета: забезпечити більш якісний та безпечний контент для користувачів, які залежать від надійної та безпечної інформації в Інтернеті, за допомогою розробки та впровадження нейронної мережі, яка буде здатна визначати недопустимий контент у текстових дані в реальному часі.
Методи дослідження: в ході виконання досліджень були використані методи обробки та підготовки даних, методи глибокого навчання, теорія нейронних мереж, теорія штучного інтелекту, математичний аналіз, методи аналізу інформативності, методи оцінки якості класифікації, дослідження практичного застосування. Програмне забезпечення розроблено за допомогою мови Python. Також були використані наступні бібліотеки: keras, sklearn, pandas і інші.
Результати: головним результатом роботи була розробка моделі нейронної мережі, яка цензурує текстові дані в реальному часі, модель виявляється високо масштабованою і готовою до навчання на даних інших мов.
Висновки: розглянуто проблему цензурування текстових даних. Оскільки це завдання обробки природної мови, було запропоновано та розроблено модель нейронної мережі на основі RNN, а саме LSTM. Дослідження засвідчило важливість інноваційних підходів у вирішенні проблем цензури текстових даних, а використання нейронних мереж та технологій штучного інтелекту стає перспективним напрямком для подальших досліджень та впроваджень у цій області.
***Ключові слова**: нейронні мережі, цензурування тексту, LSTM, NLP, класифікація текстових даних.*

Як цитувати: Тітаренко Т., Толстолузька О. Г., Узлов Д. Ю. Модель нейронної мережі для цензурування текстових даних. *Вісник Харківського національного університету імені В.Н. Каразіна, серія Математичне моделювання. Інформаційні технології. Автоматизовані системи управління*. 2023. вип. 60. С.52-58. https://doi.org/10.26565/2304-6201-2023-60-06

How to quote: Tytarenko T., Tolstoluzka O., Uzlov D., “The model of a neural network for text data censoring”, *Bulletin of V.N. Karazin Kharkiv National University, series Mathematical modelling. Information technology. Automated control systems*, vol. 60, pp. 52-58, 2023. https://doi.org/10.26565/2304-6201-2023-60-06 [In Ukrainian].

1. Вступ

У сучасному інформаційному суспільстві, де потоки текстової інформації невпинно зростають, важливість ефективної фільтрації та цензурування текстових даних визнається як ключова область для забезпечення безпеки, конфіденційності та етичності в онлайн середовищі. Непередбачуваність та динаміка змін у сучасному мовному просторі створюють виклик для

розробки інноваційних моделей, які здатні точно та автоматично визначати неприпустимий контент, забезпечуючи безпеку та етичність онлайн-спілкування.

2. Етичні, соціальні та технічні проблеми

- Цензура може порушити принцип свободи слова, який вважається ключовим для демократичних суспільств. Обмеження доступу до певної інформації може призвести до обмеження свободи вираження та обміну ідеями.
- Суб'єктивність виникає з того, що визначення того, що є неприйнятним або образливим, може значно варіюватися залежно від культур, групи людей чи індивідуальних переконань. Одна й та ж сама фраза чи вислів може бути сприйнятими різними людьми по-різному. Спроби визначити "неприйнятний" вміст можуть враховувати різні аспекти.
- Неспроможність визначити контекст: автоматизовані системи цензури, зокрема засновані на штучних нейронних мережах, можуть мати складнощі в розумінні контексту, що може призвести до помилкового блокування чи фільтрації текстів.
- Алгоритми цензури можуть стикатися із складнощами в розрізненні іронії, гумору, або того, як певний вислів може змінювати своє значення в залежності від контексту.
- Обхід цензури: цей аспект вказує на те, що користувачі можуть використовувати різні техніки для ухилення від систем цензури та отримання доступу до забороненого або обмеженого контенту. Обхід цензурних обмежень може стати проблемою для тих, хто намагається контролювати доступ до певного вмісту. Одним зі шляхів є використання альтернативних слів, користувачі можуть змінювати слова чи використовувати схожі терміни, щоб уникнути фільтрів. Маскування контенту, використання специфічних символів, реєстрації чи інших маскувальних технік для ухилення від фільтрів.
- Виклики в області техніки: обробка природної мови виявляється складним завданням, оскільки воно вимагає розуміння не лише синтаксичних та семантичних правил, але і врахування великого різноманіття мовних виразів та ідіом.

Використання штучного інтелекту, зокрема штучних нейронних мереж, виявляється найбільш ефективним у вирішенні викликів, пов'язаних із цензурою текстових даних. Штучні нейронні мережі володіють здатністю ефективно адаптуватися до складних структур текстів та контекстів, що робить їх особливо корисними у виявленні та фільтрації небажаного контенту. Вирішення цих викликів потребує впровадження передових методів обробки природної мови, застосування технологій машинного навчання, а також постійного навчання систем для адаптації до змін у мовному вживанні та соціальних стандартах. Безперечно, розробка та вдосконалення таких технологій повинні враховувати етичні аспекти, такі як конфіденційність даних та забезпечення свободи вираження.

3. Обґрунтування та вибір типу нейронної мережі: LSTM (Long Short-Term Memory)

- *Урахування контексту:*
  LSTM вміє зберігати та використовувати інформацію з попередніх кроків в послідовності. Це особливо важливо для аналізу тексту, де розуміння контексту та зв'язків між словами грає велику роль.
- *Уникнення проблеми зниклих градієнтів:*
  LSTM вирішує проблему зниклих градієнтів, яка може виникати при тренуванні глибоких нейронних мереж. Це робить його ефективним в роботі з великими обсягами текстових даних.
- *Робота з послідовностями різної довжини:*

LSTM може працювати з послідовностями різної довжини, що важливо для роботи текстовими даними, де речення можуть мати різну кількість слів.[1-2].

На рисунку 1 відображене схематичне представлення мережі з довгою короткостроковою пам'яттю.

Рисунок 1 – Схематичне представлення мережі з довгою короткостроковою пам'яттю

4. Архітектура нейронної мережі

На рисунку 2 в схематичному вигляді представлена розроблена архітектура нейронної мережі для цензурування текстових даних. Дамо короткий опис її компонентів.

- *Embedding Layer:*
  Використовується для перетворення словесного тексту в числовий формат, що може бути використано нейронною мережею.
- *LSTM Layer:*
  LSTM шар використовується для аналізу послідовності векторів, які представляють вбудовані слова.
- *Dropout Layer (перший):*
  Dropout шари використовуються для уникнення перенавчання шляхом випадкового "вимикання" частини нейронів під час тренування.
- *Dense Layers (перший):*
  Відповідає за обробку та витягування ключових ознак з інформації, що була згенерована попереднім LSTM шаром[3].
- *Dropout Layer (другий):*
  Використовується як і попередній *Dropout* для запобігання перенавчанню.
- *Dense Layers (другий):*

Застосовується для класифікації тексту на кілька класів. Допомагає у виразному представленні вихідної інформації для рішення задачі цензурування.

Враховуючи вищезазначені фактори, обрана архітектура LSTM забезпечує ефективне виявлення та цензурування неприпустимого контенту у текстових даних, здатність адаптуватися до різних контекстів та уникнення проблем зниклих градієнтів під час тренування.[4-5]

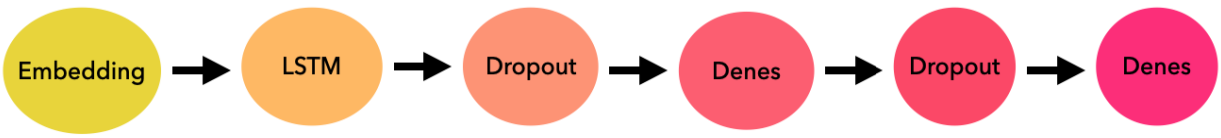


Рисунок 2 – Схематичне представлення архітектури нейронної мережі

5. Навчання нейронної мережі, та тестування

Процес навчання та тестування нейронної мережі передбачає виконання декількох кроків.

- Попередня обробка:
  Очищення даних: Вилучення непотрібних символів, HTML-тегів чи спеціальних символів.
- Розділення даних:
  Розподіл даних на тренувальний, *валідаційний* та тестовий набори для ефективного тренування та оцінки моделі.

- Токенізація та доповнення:

  Токенізація - це етап обробки тексту, під час якого вхідний текст розділяється на окремі одиниці, так звані токени. Токени можуть бути словами, фразами або іншими одиницями тексту. В контексті цензурування токенізація допомагає розділити текстові фрази на окремі слова, що стає важливим етапом перед подальшим перетворенням тексту для використання в нейронній мережі. Токенізація може бути виконана різними способами. Зазвичай вона включає в себе видалення зайвих символів, поділ тексту на окремі слова та створення токенів. Наприклад, речення «Це речення для цензурування» може бути розділене на токени: ["Це", "речення", "для", «цензурування"].[6].

  Після токенізації, текстові токени потрібно перетворити в числові значення, які можуть бути подані нейронною мережею. Цей етап називається трансформацією тексту в числові послідовності. Цей етап дозволяє побудувати числовий вектор для кожного текстового фрагменту, що є необхідним для подальшого навчання нейронної мережі.

- Імплементація моделі та навчання:

  Імплементація моделі: Імплементуємо розроблену архітектуру (рис. 2) до програмної реалізації. Після створення архітектури моделі, наступний крок - це її компіляція, тобто конфігурація процесу навчання. Компіляція включає в себе вибір оптимізатора, функції втрат та метрик, які *використовуються* для оцінки продуктивності моделі під час навчання. Після відібрання та підготовки наборів даних, модель переходить до етапу навчання. У цьому етапі використовується тренувальний набір даних, і модель намагається оптимізувати свої параметри за допомогою методу градієнтного спуску та зворотнього поширення помилки. Тренування включає в себе подачу текстових даних в мережу, оцінювання виходів, порівняння їх з очікуваними значеннями та коригування ваг моделі для покращення її точності.

- Оцінка:

  Валідація та тестування: Оцінка моделі на валідаційному наборі для налаштування параметрів та на тестовому наборі для оцінки загальної ефективності, та оцінка продуктивності навченої моделі. Для цього використовуються різні метрики, щоб отримати об'єктивне уявлення про те, *наскільки* добре модель справляється з поставленим завданням цензурування тексту[7]. На рисунку 3 наведено приклад даних на яких навчається модель.

	count	hate_speech	offensive language	neither	class	tweet
0	3	0	0	3	2	!!! RT @mayasolovely: As a woman you shouldn't complain about cleaning up your house. & as a man you should always take the trash out...
1	3	0	3	0	1	!!!!! RT @mleew17: boy dats cold...tyga dwn bad for cuffin dat hoe in the 1st place!!
2	3	0	3	0	1	!!!!!!! RT @UrKindOfBrand Dawg!!!! RT @80sbaby4life: You ever fuck a bitch and she start to cry? You be confused as shit
3	3	0	2	1	1	!!!!!!!! RT @C_G_Anderson: @viva_based she look like a tranny
4	6	0	6	0	1	!!!!!!!!!!! RT @ShenikaRoberts: The shit you hear about me might be true or it might be faker than the bitch who told it to ya 
5	3	1	2	0	1	!!!!!!!!!!!!!!!!!"@T_Madison_x: The shit just blows me..claim you so faithful and down for somebody but still fucking with hoes! 😂😂😂"
6	3	0	3	0	1	!!!!!"@__BrighterDays: I can not just sit up and HATE on another bitch .. I got too much shit going on!"
7	3	0	3	0	1	!!!!“@selfiequeenbri: cause I'm tired of you big bitches coming for us skinny girls!!”
8	3	0	3	0	1	" & you might not get ya bitch back & thats that "
9	3	1	2	0	1	" @rhythmixx_ :hobbies include: fighting Mariam" bitch
10	3	0	3	0	1	" Keeks is a bitch she curves everyone " lol I walked into a conversation like this. Smh

Рисунок 3 – Приклад даних на яких навчається модель(твіти)

Після відібрання та підготовки наборів даних, модель переходить до етапу навчання. У цьому етапі використовується тренувальний набір даних, і модель намагається оптимізувати свої параметри за допомогою методу градієнтного спуску та зворотнього поширення помилки. Тренування включає в себе подачу текстових даних в мережу, оцінювання виходів, порівняння їх з очікуваними значеннями та коригування ваг моделі для покращення її точності.

Окремий валідаційний набір даних в розробленій моделі використовується для перевірки, наскільки добре модель генералізує свої знання на нових, раніше не бачених даних. Валідація дозволяє визначити ступінь, до якої модель уникнула перенавчання (overfitting) або, навпаки, недонавчання (underfitting).

Після кожного циклу тренування, коли модель пройшла через всі дані тренувального набору, проводиться валідація на валідаційному наборі.

Результати валідації служать орієнтиром для покращення параметрів моделі та вдосконалення її продуктивності.

Цей етап є важливим для створення моделі, яка не лише ефективно працює на тренувальних даних, але і може адекватно застосовувати свої знання до нових ситуацій. Метрики моделі нейронної мережі після навчання представлено в таблиці 1.

Таблиця 1 - Метрики моделі нейронної мережі після навчання

Набір даних/метрики	Precision	AUC-ROC	Loss
Початкова точність	0.8359	0.8088	0.4790
Кінцева точність	0.8902	0.8995	0.0390

Аналізуючи результати експериментів з різними наборами гіперпараметрів для моделі, можна зробити декілька важливих висновків. Найефективнішою виявилася конфігурація з LSTM = 128, Dense = 256, Batch_size = 64, Epochs = 5 та швидкістю навчання Adam = 0.01. Цей набір параметрів дозволив досягти високої точності (Precision 0.8802) та високого показника AUC-ROC (0.8895), що свідчить про високу якість моделі в класифікації та роботу з різними класами (рис.4).

Також важливо зазначити, що збільшення кількості LSTM-шарів не завжди призводить до поліпшення результатів, а зменшення кількості може вплинути на ефективність моделі. Збільшення кількості епох не завжди призводить до покращення, а швидкість навчання може виявитися ключовим фактором: збільшення швидкості може призвести до зростання точності та AUC-ROC.

Додатково, важливо відмітити стабільність моделі при зміні швидкості навчання. Модель показала стійкість результатів при зменшенні швидкості навчання (Adam = 0.0001), що може бути корисним при роботі з великими та складними наборами даних.

У кінці, експерименти з гіперпараметрами вказують на необхідність систематичного та пристосованого підходу до вибору параметрів для кожної конкретної задачі та датасету.

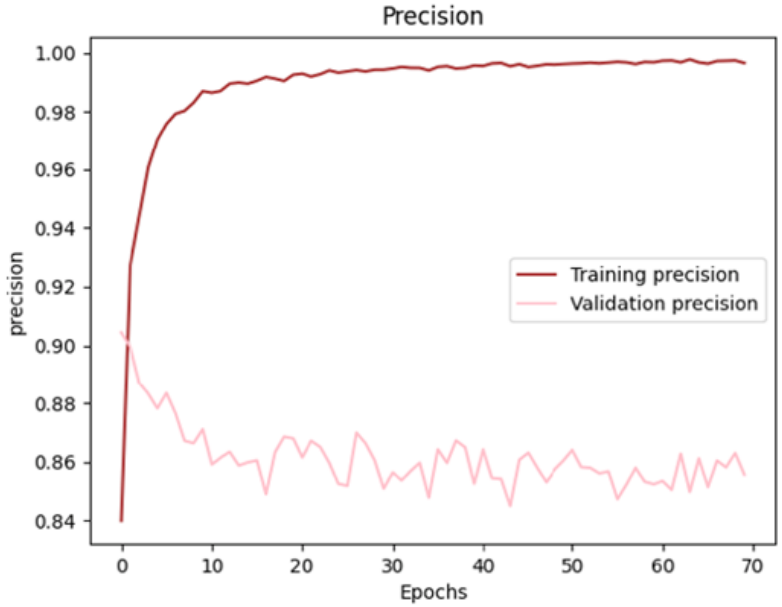


Рисунок 4 – Графік класової точності моделі

6. Висновки

Головним результатом даної роботи була розробка моделі нейронні мережі, яка цензурує текстові дані в реальному часі, модель виявляється високо масштабованою і готовою до навчання на даних інших мов. Її архітектура, з використанням LSTM-шарів та ембедінгів, дозволяє ефективно враховувати контекст та взаємодію між словами у текстах. Оскільки використовується токенізація тексту та побудова словника, модель може адаптуватися до різних мовних варіацій. Змінюючи навчальний датасет на дані іншої мови, можна досягти гарної адаптації, оскільки модель вивчає структуру мови та зв'язки між словами. Такий підхід робить модель гнучкою та застосовною до різних завдань та мовних середовищ.

Головним напрямком використання моделі є цензурування текстових даних в онлайн середовищі, де потік текстової інформації росте експоненційно, і ефективна фільтрація та цензура текстових даних стають визначальними аспектами для забезпечення безпеки, конфіденційності та етичності.

Модель демонструє високий рівень ефективності та продуктивності за рахунок розробленої архітектури, різноманіття та якість даних для навчання, та обраних гіперпараметрів. Архітектура складається з LSTM-шарів, ембедінгів та дропаут-шарів які ефективно працюють з текстовими даними, про це свідчить висока точність 88% та високий показник AUC-ROC, значення якого складає 0.8895. Дані для навчання, являють собою 25 тисяч текстових повідомлень з мережі Twitter, що попередньо оброблені, а саме видалені HTML-сутності, URL-адреса та інші непотрібні символи. Проведені експерименти та аналіз результатів дозволили визначити оптимальні гіперпараметри моделі.

Також модульна структура та архітектура програмної реалізації дозволяють легко інтегрувати та адаптувати модель для використання її на різних платформах. Як практичний приклад, модель була успішно імплементована в середовищі Telegram. Це дозволяє в реальному часі аналізувати та цензурувати текстовий контент, що надходить через цю платформу.

На етапі вибору типу моделі нейронної мережі були розглянуті та порівняні різні архітектури, такі як персептрон, багатошаровий персептрон, згорткова нейронна мережа, рекурентні нейронні мережі, зокрема, LSTM, CNN та RNN.

СПИСОК ЛІТЕРАТУРИ

1. Zhang, X. A Mathematical Model of a Neuron with Synapses based on Physiology. Nat Prec (2008). https://doi.org/10.1038/npre.2008.1703.1
2. Sima J. “Introduction to Neural Networks,” Technical Report No. V 755, Institute of Computer Science, Academy of Sciences of the Czech Republic, 1998.
3. Kröse B., and van der Smagt P. An Introduction to Neural Networks. (8th ed.) University of Amsterdam Press, University of Amsterdam, 1996.
4. Harshali M. Deep learning — 2015.
5. Yingci L. Zhonghua C. Hongkai W. Peiou L. Zongwei Z. Comparison of machine learning methods for classifying mediastinal lymph node metastasis of non-small cell lung cancer from 18F-FDG PET/CT — 2017
6. Aurélien Géron. Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow: Concepts, Tools, and Techniques to Build Intelligent Systems 3rd Edition
7. Oliver Theobald, Best Machine Learning Books for Absolute Beginners, 2021 - 50 c.

Tytarenko Tymur *Master student; V.N. Karazin Kharkiv National University, Svobody Square, 4, Kharkiv-22, Ukraine, 61022.*
e-mail: tima.tytarenko.001@gmail.com
https://orcid.org/0000-0001-6417-151X

Tolstoluzka Olena *Doctor of Engineering Sciences; Professor of Theoretical and Applied Systems Engineering Department; V.N. Karazin Kharkiv National University, Svobody Square, 4, Kharkiv-22, Ukraine, 61022.;*
e-mail: elena.tolstoluzka@karazin.ua
https://orcid.org/0000000312417906

Uzlov Dmitro *Associate Professor of the Department of Theoretical and Applied Informatics, Faculty of Mathematics and Informatics, Ph.D. V.N. Karazin Kharkiv National University, Svobody Square, 4, Kharkiv-22, Ukraine, 61022.*
https://orcid.org/0000-0003-3308-424X

The model of a neural network for text data censoring

Relevance: Given the rapid development of Internet communications and the increasing amount of textual content, an urgent need to ensure effective censorship of textual data necessitates the relevance of this research. This is especially true for the online community, where it is essential to ensure the security and ethics of communication.
Purpose: to provide better and safer content for users who depend on reliable and secure Internet information by means of developing and implementing a neural network that will be able to identify inappropriate textual content in real time.
Research methods: methods of data processing and preparation, deep learning methods, neural network theory, artificial intelligence theory, mathematical analysis, methods of information content analysis, methods of classification quality assessment, and practical application research have been used in the course of the research. The software has been developed by using the Python language.
Results: the main achievement of the work is the development of a neural network model that censors textual information in real time, the model is highly scalable and can be trained on data from other languages.
Conclusions: The problem of text data censoring has been considered. Since this is a natural language processing task, an RNN-based neural network model, namely LSTM, has been proposed and developed. The study has shown the importance of innovative approaches in solving the problems of text data censorship, and the use of neural networks and artificial intelligence technologies is becoming a promising area for further research and implementation in this area.

Keywords*: neural networks, text censorship, LSTM, NLP, text data classification.*

Надійшла у першій редакції 14.09.2023, в останній – 22.11.2023.
The first version has been received on 14.09.2023, the final version – on 22.11.2023.

ВІСНИК ХАРКІВСЬКОГО НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ імені В.Н. Каразіна

серія **«Математичне моделювання. Інформаційні технології. Автоматизовані системи управління»**

Випуски даної серії розповсюджуються у академічних та наукових колах України та за її межами з метою оперативного висвітлення досліджень у таких актуальних галузях: математичне та комп'ютерне моделювання, обчислювальний експеримент, теорія і прикладні методи обробки інформації, захист інформації, програмно-апаратні системи інформаційного або управляючого призначення, застосування математичного моделювання та системного аналізу у високих, наукоємних технологіях, враховуючи технології створення програмної продукції. Приймаються роботи, що відносяться до напрямів фізико-математичних і технічних наук (бажаний об'єм 6-18 сторінок). Усі рукописи рецензуються.

Примітка. Протягом 2024-25 рр. редакційна колегія при інших рівних умовах надаватиме перевагу роботам, що представлені англійською мовою, якщо стаття отримала схвалення при рецензуванні.

Офіційний сайт **http://periodicals.karazin.ua/mia**
http://mia.univer.kharkov.ua
Email: journal-mia@karazin.ua

Bulletin of V.N. Karazin Kharkiv National University

series **«Mathematical modeling. Information technology. Automated control systems»**

This series are distributed in academic and scientific circles of Ukraine and abroad for the purpose of timely coverage of research in the following topical areas: mathematical and computer modeling, computational experiment, theory and applied methods of information processing, information protection, software and hardware systems of control and information management, applications of mathematical modeling and system analysis in high, science-intensive technologies, including technologies of software products creation. Articles belonging to the fields of physical, mathematical and technical sciences are accepted (recommended length 6-18 pages). All submissions are peer-reviewed.

Note. For the years 2024-25, all other conditions being equal, the Editorial Board will give preference to articles submitted in English and approved by the peer-review.

Official website **http://periodicals.karazin.ua/mia**
http://mia.univer.kharkov.ua
Email: journal-mia@karazin.ua

Наукове видання

Вісник Харківського національного університету імені В. Н. Каразіна

Серія «Математичне моделювання. Інформаційні технології. Автоматизовані системи управління»

Випуск 60

Збірник наукових праць

Українською та англійською мовами

Комп'ютерне верстання О. О. Афанасьєва

Підписано до друку 15.12.2023 р.
Формат 60x84/8. Папір офсетний. Друк цифровий.
Ум. друк. арк. – 5,89.
Обл.– вид. арк. –7,36.
Наклад 50 пр. Зам. № 42/2023
Безкоштовно

Видавець і виготовлювач
Харківський національний університет імені В. Н. Каразіна
61022, м. Харків, майдан Свободи, 4
Свідоцтво суб'єкта видавничої справи ДК №3367 від 13.01.09

Видавництво Харківський національний університет імені В. Н. Каразіна
тел.: 705-24-32