з постачальниками програмного й апаратного забезпечення, керованих послуг, які зможуть змінити кіберландшафт на користь більшої безпеки та стійкості.

Отже, Національна стратегія кібербезпеки США представила бачення федерального уряду щодо забезпечення стабільного й надійного захисту критичної інфраструктури шляхом встановлення вимог кібербезпеки для критично важливих служб, поглиблення державно-приватної співпраці, інтеграції федеральних центрів кібербезпеки, оновлення федеральних планів і процесів реагування на інциденти, модернізації системи федерального захисту.

1. National cybersecurity strategy. March 2023. *The White House.* URL: https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf
2. Cybersecurity Performance Goals (CPGs). October 2022. *CISA*. URL: https://www.cisa.gov/cybersecurity-performance-goals-cpgs
3. Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1. April 16, 2018. *NIST*.
4. National Cyber Incident Response Plan. Update Public Comment Draft. December 2024. *CISA*. URL: https://www.cisa.gov/sites/default/files/2025-01/NCIRP%20Update%20Public%20Comment%20Draft%20508c__0.pdf

Проєктування нейромережевого фільтра фішингових повідомлень

УДК 004.056.55

Владислав Назаров
Національний університет «Одеська політехніка,
tasknavigator@stud.op.edu.ua

З розвитком месенджерів і збільшенням електронної кореспонденції традиційні спам-фільтри неефективні від складних фішингових атак. Статистичні й SVM-фільтр втрачають лінгвістичні ознаки, не враховуючи зовнішні посилання [1], нейромережеві моделі вимагають значних ресурсів, мають затримки [2].

Метою роботи є розробка розподіленої мікросервісної архітектури фільтра, інтегрованого в месенджери та поштові сервіси, для швидкого й безперервного виявлення фішингу з мінімальною затримкою.

Запропонована система поєднує NLP-аналіз, ранжування чинників ризику і нейромережеву класифікацію. Конфіденційність забезпечується завдяки виключенню втручання людини та аналізу повідомлень лише в оперативній пам’яті, без збереження їх змісту.

Система реалізована як комплекс автономних мікросервісів, що взаємодіють через асинхронну чергу RabbitMQ (таб.1).

Вхідні повідомлення надходять через REST-шлюз та послідовно обробляються NLP-модулем, сервісом формування чинників ризику і нейромережевими класифікаторами.

Таблиця 1

Опис компонентів системи та їх функціональні взаємодії

Компонент	Опис та функціональні взаємодії	Технологія	Продуктивність
Інтеграційний шлюз API	Приймає повідомлення (месенджери, SMTP/IMAP), встановлює SSL/TLS, передає запити в чергу RabbitMQ.	FastAPI, Docker, SSL/TLS	500 запитів/с
Брокер повідомлень	Асинхронна передача даних між контейнерами, гарантія доставки («at least once»),горизонтальнемасштабування	RabbitMQ 3.x, Docker	SLA ≤ 50 мс на доставку
NLP-модуль	NLP-аналіз тексту (токенізація, шаблони, URL), формування ознак аналізу ризиків.	Python 3.8+, spaCy, regex	1 000 повідомлень/с; 98% точн
Модуль ранжування ризиків	Перетворення ознак на числовий вектор (Rm, Tm, Ez, Rz), кешування Redis,підготовка даних для класифікації	C++17, PyBind11, Redis	< 1 мс на повідомлення
Сигмоїдна нейромережа	Одношарова модель (MSE-втрати), класифікація ймовірності фішингу, GPU-прискорення,передача рез-ів моніторингу	TensorFlow 2.x, CUDA-GPU	Помилка ≤ 10^{-3}; 200 ітерацій ≈ 5 хв
Порогова модель	Лінійна порогова модель, адаптивне оновлення Rz, швидка класифікація, передача результатів	NumPy 1.22+, C++	< 0,1 мс на класифікацію; похибка ≈ $0{,}5 \cdot 10^{-3}$
Моніторинг та логування	Збір метрик продуктивності, затримок та помилкових спрацьовувань; зворотний зв'язок	ELK Stack, Prometheus, Grafana	Затримка збору метрик ≤ 200 мс

1. Khamis S.A., Foozy C.F.M., Ab Aziz M.F., Rahim N. Header based email spam detection framework using Support Vector Machine (SVM) technique. *Advances in Intelligent Systems and Computing*. 2020. P. 57–65.

2. Petliak N., Bezkorovalnyi Y. Analysis of modern methods of detection of phishing e-mails.Herald of Khmelnytskyi National University.2024.Issue 5