Результати можуть використовуватися для карти кіберризиків, сегментації мережі, посилення автентифікації, централізованого оновлення, резервування критичних сервісів і журналювання подій. Модель не замінює аудит, але є інструментом попереднього оцінювання та регулярного моніторингу. Подальші дослідження доцільно спрямувати на калібрування вагових коефіцієнтів, інтеграцію з SIEM/SOC-рішеннями та адаптацію до окремих міських сервісів..

1. Nurse J.R.C., Creese S., De Roure D. Security risk assessment in Internet of Things systems. IT Professional. 2017. Vol. 19(5). P. 20-26.
2. Kandasamy K. et al. IoT cyber risk: a holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process. EURASIP Journal on Information Security. 2020. Vol. 2020. Article 8.
3. Parsons E.K. et al. A survey on cyber risk management for the Internet of Things. Applied Sciences. 2023. Vol. 13(15). Article 9032.
4. Gharaibeh A. et al. Smart cities: A survey on data management, security, and enabling technologies. IEEE Communications Surveys & Tutorials. 2017. Vol. 19(4). P. 2456-2501.

Еволюція методів виявлення шкідливих URL: від евристик до трансформерних архітектур

УДК 519.6

Петро Венгерський[1], Володимир Лесик[2]

Львівський національний університет імені Івана Франка,
[1]petro.venherskyy@lnu.edu.ua, [2]volodymyr.lesyk@lnu.edu.ua

Стрімке зростання кількості вебресурсів та кіберзагроз зумовлює актуальність задачі виявлення шкідливих URL-адрес, що використовуються для фішингу, поширення шкідливого програмного забезпечення та координації бот-мереж. Традиційні підходи, засновані на чорних списках і сигнатурному аналізі, мають обмежену ефективність через нездатність виявляти нові або модифіковані атаки [1-3].

Метою роботи є систематизація еволюції методів виявлення шкідливих URL-адрес - від евристичних підходів до сучасних моделей машинного та глибокого навчання, а також визначення перспектив подальшого розвитку інтелектуальних систем захисту.

Еволюцію технологій детекції можна розділити на кілька послідовних етапів. Технологічний прогрес у цій галузі характеризується переходом від жорстких алгоритмів до гнучких нейромережевих архітектур [3] (рис. 1).

Початковий етап базувався на використанні ручних правил і статичних баз даних, що забезпечували швидку, але обмежену за узагальненням детекцію відомих аномалій [3].

Наступним кроком стало впровадження класичного машинного навчання (ML). Алгоритми логістичної регресії, SVM та ансамблеві методи (зокрема Random Forest) автоматизували класифікацію на основі видобутих ознак URL-адрес: лексичних, хостових, контентних та зовнішніх [1,3,4]. Лексичні ознаки дозволяють здійснювати швидку класифікацію без доступу до мережевих

ресурсів [4,5], тоді як хостові та контентні характеристики забезпечують глибокий аналіз веб інфраструктури [6]. Головною перевагою цих моделей стала висока інтерпретованість та обчислювальна ефективність.

Рис.1. Узагальнена схема еволюції технологій детекції URL

Зростання обсягів даних зумовило перехід до методів глибокого навчання (DL). Архітектури згорткових (CNN) та рекурентних (LSTM) нейронних мереж дозволяють автоматично витягувати складні нелінійні залежності з URL-рядків і контенту вебсторінок [7-9]. Це зменшує залежність від ручної інженерії ознак і підвищує здатність моделей до узагальнення.

Сучасний етап розвитку представлений трансформерними архітектурами (моделі типу BERT), які забезпечують аналіз контексту та семантичних залежностей у URL-адресах [8,10]. Такі підходи демонструють найвищі показники точності (до 99,97%) [3], однак їх практичне впровадження ускладнюється жорсткими вимогами до обчислювальних ресурсів.

Паралельно також розвиваються альтернативні підходи, зокрема асоціативна класифікація та методи видобування правил, що дозволяють формувати інтерпретовані залежності між ознаками [11, 12]. Їх інтеграція з моделями глибокого навчання відкриває можливості створення унікальних гібридних систем.

Основними викликами сучасних систем є залежність від якості даних, обчислювальна складність моделей та швидка еволюція кіберзагроз [3, 13]. У зв'язку з цим перспективним напрямом є створення адаптивних систем, здатних динамічно змінювати ваги ознак і поєднувати різні підходи до аналізу [6, 14].

Еволюція методів виявлення шкідливих URL-адрес демонструє поступовий перехід від простих евристик до складних інтелектуальних моделей. Найбільш перспективним напрямом є розробка адаптивних гібридних систем, що поєднують інтерпретованість класичних методів, здатність до узагальнення моделей глибокого навчання та контекстний аналіз трансформерів, з можливістю динамічного коригування ваг ознак у реальному часі.

1. Sahoo D., Liu C., Hoi S.C.H. Malicious URL Detection using Machine Learning: A Survey. arXiv preprint. – 2017. – arXiv:1701.07179. – doi:10.48550/arXiv.1701.07179.
2. Aljabri M., Altamimi H., Albelali S., Al-Harbi M., Alhuraib H., Alotaibi N., Alahmadi A., Alhaidari F., Mohammad R., Salah K. Detecting

Malicious URLs Using Machine Learning Techniques: Review and Research Directions. IEEE Access. – 2022. – doi:10.1109/ACCESS.2022.3222307.
3. Tian Y., Yu Y., Sun J., Wang Y. From Past to Present: A Survey of Malicious URL Detection Techniques, Datasets and Code Repositories. arXiv preprint. – 2025. – arXiv:2504.16449. – doi:10.48550/arXiv.2504.16449.
4. Dhotre A. Malicious URLs Detection using Lexical Features based on Machine Learning. IJSRD. – 2023. – Vol. 11, Issue 8.
5. Joshi A., Lloyd L., Westin P., Seethapathy S. Using Lexical Features for Malicious URL Detection – A Machine Learning Approach. arXiv preprint. – 2019. – arXiv:1910.06277. – doi:10.48550/arXiv.1910.06277.
6. Hamadouche S., Boudraa O., Gasmi M. Combining Lexical, Host, and Content-based Features for Phishing Websites Detection using Machine Learning Models. EAI Endorsed Transactions on Scalable Information Systems. – 2024. – Vol. 11, no. 6. – doi:10.4108/eetsis.4421.
7. Do N., Selamat A., Krejcar O., Herrera-Viedma E., Fujita H. Deep Learning for Phishing Detection: Taxonomy, Current Challenges and Future Directions. IEEE Access. – 2022. – Vol. 10. – P. 36543–36564. – doi:10.1109/ACCESS.2022.3151903.
8. Turk F., Kilicaslan M. Malicious URL Detection with Advanced Machine Learning and Optimization-Supported Deep Learning Models. Appl. Sci. – 2025. – Vol. 15, no. 18. – Art. 10090. – doi:10.3390/app151810090.
9. Kibriya H., Amin R., Alshamrani S.S. et al. Lightweight Malicious URL Detection using Deep Learning and Large Language Models. Sci. Rep. – 2025. – Vol. 15. – Art. 43044. – doi:10.1038/s41598-025-26653-2.
10. Elsadig M., Ibrahim A.O., Basheer S., Alohali M.A., Alshunaifi S., Alqahtani H., Alharbi N., Nagmeldin W. Intelligent Deep Machine Learning Cyber Phishing URL Detection Based on BERT Features Extraction. Electronics. – 2022. – Vol. 11, no. 22. – Art. 3647. – doi:10.3390/electronics11223647.
11. Kumi S., Lim C., Lee S.-G. Malicious URL Detection Based on Associative Classification. Entropy. – 2021. – Vol. 23, no. 2. – Art. 182. – doi:10.3390/e23020182.
12. Jeeva S.C., Rajsingh E.B. Intelligent Phishing URL Detection using Association Rule Mining. Hum. Cent. Comput. Inf. Sci. – 2016. – Vol. 6. – Art. 10. – doi:10.1186/s13673-016-0064-3.
13. Alsaedi M., Ghaleb F.A., Saeed F., Ahmad J., Alasli M. Cyber Threat Intelligence-Based Malicious URL Detection Model Using Ensemble Learning. Sensors. – 2022. – Vol. 22, no. 9. – Art. 3373. – doi:10.3390/s22093373.
14. Rafsanjani A.S., Kamaruddin N.B., Behjati M., Aslam S., Sarfaraz A., Amphawan A. Enhancing Malicious URL Detection: A Novel Framework Leveraging Priority Coefficient and Feature Evaluation. IEEE Access. – 2024. – Vol. 12. – P. 85001–85026. – doi:10.1109/ACCESS.2024.3412331.