створення рівнів доступу до інформаційних ресурсів, багатофакторну автентифікацію персоналу, ізоляцію критично важливих систем управління від відкритих мереж передачі даних, дублювання серверної інфраструктури, використання захищених мобільних центрів управління та створення альтернативних каналів передачі інформації, підвищення рівня знань із кібербезпеки персоналу ТІ, використання систем штучного інтелекту для аналізу ризиків щодо можливих кіберзагроз.

Концепцію безпеки ТІ України слід будувати на основі системного підходу як багаторівневу модель організаційних, міжвідомчих, технічних, наукових, інформаційних та кібербезпекових заходів, які створюють надійні умови використання ТІ України.

1. Ковальов К. Є. Сучасні виклики та загрози для критичної інфраструктури України під час воєнного стану. *Приватне та публічне право*. – 2025. – № 1. – С.75-80. DOI: https://doi.org/10.32782/2663-5666.2025.1.12
2. Коваль К. П., Тєлєгін О. О. Логістика в умовах війни: ключові виклики та шляхи протидії загрозам. *Проблеми і перспективи економіки та управління*. – 2025. – № 1 (41). – С. 167-178. DOI: https://doi.org/10.25140/2411-5215-2025-1(41)-167-178
3. СБУ нейтралізувала понад 14 тисяч масштабних кібератак на Україну за час повномасштабного вторгнення. URL: https://ssu.gov.ua/novyny/sbu-neitralizuvala-ponad-14-tysiach-masshtabnykh-kiberatak-na-ukrainu-za-chas-povnomasshtabnoho-vtorhnennia (дата звернення: 01.05.2026).

Graph-Based Model for Risk Assessment of Access to Corporate Databases in Network Infrastructure

UDK 004.056.5:004.7

Oleksandr Budzynskyi[1], Yurii Shchavinsky[2]

State University of Information and Communication,
[1]oleksandr.email@gmail.com, [2]y.shchavinskyi@duikt.edu.ua

Modern corporate databases are characterized by a large number of interconnected nodes, services and data exchange channels. Under such conditions, ensuring cybersecurity becomes one of the key tasks. Traditional security mechanisms are focused mainly on the analysis of individual events or network traffic, and cannot fully assess the risks of multi-stage attacks implemented by sequentially compromising network nodes. In this regard, the use of graph models becomes promising, since they allow formalizing the structure of the network infrastructure and assessing risks at the level of possible access paths to the database.

The relevance of the topic of using graph models to improve the effectiveness of corporate database protection is substantiated in many studies. In work [1], the authors showed the need to use structural graph attack models to detect complex lateral movement scenarios. In paper [2], a model for assessing the cyber-physical security

of industrial systems based on “AND/OR” attack graphs is proposed, which allows identifying critical infrastructure components and minimal ways to compromise the system. In study [3] a combination of Bayesian attack graphs with process mining is proposed for dynamic risk assessment in real time.

Unlike the above approaches, in the proposed work, the graph model is combined with an AI-based node anomaly assessment based on Isolation Forest, LSTM, and Autoencoder, as well as an exponential risk model that takes into account the cumulative impact of node criticality along the attack path to the corporate database. This allows for adaptive risk assessment in conditions of variable network activity and dynamic network segmentation. The purpose of the study is to develop a graph-based model for assessing access risks to corporate databases in network infrastructure by considering attack propagation paths, node criticality, and AI-driven anomaly detection mechanisms.

The corporate network is proposed to be represented as a directed graph $G=(V,E)$, where V is the set of network nodes (workstations, servers, routers, databases), and E is the set of edges defining possible transitions between nodes.

This model makes it possible to describe potential attack propagation routes and formalize the relationships between infrastructure components. To evaluate the state of nodes, a combined AI-based approach using Isolation Forest, LSTM, and Autoencoder models is applied. The anomaly level of a node is determined by the following expression:

$$q_v(t) = \sigma(\alpha s_{IF}(v,t) + \beta s_{LSTM}(v,t) + \gamma s_{AE}(v,t)), \quad (1)$$

where s_{IF}, s_{LSTM}, and s_{AE} are the outputs of machine learning models, $\sigma(\cdot)$ is the sigmoid normalization function, and $q_v(t) \in [0,1]$ characterizes the suspiciousness level of a node. α+β+γ=1 - model impact factors

The probability of spreading an attack between adjacent nodes u-v of the network is defined as:

$$p_{u,v}(t) = \sqrt{q_u(t) \cdot q_v(t)} \quad (2)$$

Accordingly, the probability of attack traversal along a path $\pi$is calculated as the product of transition probabilities:

$$P(\pi,t) = \prod_{(u,v)\in\pi} p_{uv}(t) \quad (3)$$

Unlike conventional approaches, the proposed model makes it possible to assess not individual incidents but the risk of reaching a critical resource through a sequence of interconnected network nodes. For integrated risk assessment, an exponential risk model is proposed:

$$R(\pi,t) = P(\pi,t) \cdot I(DB) \cdot \exp(\lambda \sum_{v\in\pi} I(v)) \quad (4)$$

where $I(v)$ denotes the criticality of a node, and λ is the sensitivity coefficient of the model, $I(DB)$ – database criticality

With an exponential function, even a small increase in the number of critical nodes can significantly increase the overall risk level. Model analysis shows that the most

dangerous routes are critical infrastructure nodes. Reducing the number of alternative database access paths significantly reduces the overall risk of system compromise. The results obtained confirm the effectiveness of the graph approach for assessing the risks of accessing corporate databases. The proposed model provides a comprehensive analysis of the network infrastructure, takes into account the structural features of the attack propagation and can be applied in SOC and SIEM systems for automatic management of cybersecurity policies. Prospects for further research include integrating the model into real corporate networks, using industrial datasets, and optimizing the parameters of the artificial intelligence model to increase the accuracy of risk assessment.

1. Stergiopoulos G.. Gritzalis D.. Limnaios E.,. Cyber-Attacks on the Oil & Gas Sector: A Survey on Incident Assessment and Attack Patterns. *IEEE Access* – 2020. p. 1-37. URL: http://doi.org/10.1109/ACCESS.2020.3007960
2. Barrère M., Hankin C., Nicolaou N., Eliades D., Parisini T. Measuring cyber-physical security in industrial control systems via minimum-effort attack strategies. *Journal of Information Security and Applications* - 2020. V. 52. - p. 1-5. URL: http://doi.org/52. 17. 10.1016/j.jisa.2020.102471
3. Vitale F.,, Guarino S., Perone S., Rak M., Mazzocca N. Dynamic Risk Assessment by Bayesian Attack Graphs and Process Mining. *Accepted to the 2026 IEEE International Conference on Cyber Security and Resilience.* 20 Apr 2026. p. 1-6. URL: https://doi.org/10.48550/arXiv.2604.18080

Архітектурний підхід Policy-as-Code для захисту LLM-інференс пайплайнів від атак prompt injection

УДК 004.056.5, 004.822

О.П. Вахула[1],

[1]Національний університет «Львівська політехніка», Львів;
oleksandr.p.vakhula@lpnu.ua

Інтеграція великих мовних моделей (LLM) у корпоративні системи обробки інформації відкриває нові вектори атак, що не охоплюються класичним апаратом статичного аналізу. Атаки типу *prompt injection* дозволяють зловмисникам маніпулювати поведінкою моделі через структурований вхід природною мовою, обходячи системні інструкції або витягуючи конфіденційні дані. Регуляторні вимоги - зокрема EU AI Act (статті 12, 13, 15) та директива NIS2 - висувають додаткову вимогу: кожне автоматизоване рішення у сфері безпеки має бути *аудитопридатним та простежуваним*, що принципово несумісне з «чорноскриньковими» ML-класифікаторами загального призначення.[1,2]

Існуючі підходи до фільтрації промптів поділяються на два полюси: прості ключово-словникові фільтри з детермінованою, але негнучкою логікою і ML-класифікатори, що забезпечують семантичне розуміння ціною непрозорості та ресурсомісткості. Жоден із підходів не задовольняє одночасно критеріям точності, швидкодії та аудитопридатності. Розрив між цими полюсами визначив