1. Sternak T., Runje D., Granoša D., Wang C. Automating Prompt Leakage Attacks on Large Language Models Using Agentic Approach – 2025. – URL: https://arxiv.org/pdf/2502.12630
2. Agarwal D., Fabbri A., Risher B., Laban P., Joty S., Wu C.-S. Prompt Leakage Effect and Mitigation Strategies for Multi-turn LLM Applications // Proceedings of the 2024 Conference on Empirical Methods in Natural Language Processing: Industry Track. – Miami, Florida, USA, 2024. – C. 1255–1275. – URL: https://aclanthology.org/2024.emnlp-industry.94/
3. Cao B., Li C., Cao Y., Ge Y., Wang T., Chen J. You Can't Steal Nothing: Mitigating Prompt Leakages in LLMs via System Vectors // Proceedings of the 2025 ACM SIGSAC Conference on Computer and Communications Security (CCS '25). – Taipei, Taiwan, 2025. – URL: https://arxiv.org/abs/2509.21884
4. Wu G., Zhang Z., Zhang Y., Wang W., Niu J., Wu Y., Zhang Y. I Know What You Asked: Prompt Leakage via KV-Cache Sharing in Multi-Tenant LLM Serving // Network and Distributed System Security Symposium (NDSS) 2025. – San Diego, CA, USA, 2025. – URL: https://www.ndss-symposium.org/ndss-paper/i-know-what-you-asked-prompt-leakage-via-kv-cache-sharing-in-multi-tenant-llm-serving/
5. Wang Z., Zhang R., Liu Y., Liu C., Zhao Q., Li H., Xu G. Black-Box Skill Stealing Attack from Proprietary LLM Agents: An Empirical Study // arXiv. – 2026. – URL: https://arxiv.org/abs/2604.21829

Еволюція стратегії ЄС щодо протидії іноземному втручанню та маніпулюванню інформацією (FIMI)

УДК 327:004.056

Сергій Кондратюк

Державний університет інформаційно-комунікаційних технологій, s.kondratiuk@duikt.edu.ua

У період 2015-2026 рр. стратегія Європейського Союзу у сфері протидії іноземним маніпуляціям і втручанням (FIMI) пройшла глибоку еволюцію — від поодиноких реакцій на дезінформаційні кампанії до створення узгодженої, багаторівневої екосистеми проактивної протидії. У березні 2015 р. на саміті ЄС у Брюсселі було ухвалене рішення про необхідність протидії постійним дезінформаційним кампаніям Росії, що зумовило створення East StratCom Task Force у межах Європейської служби зовнішніх справ (EEAS).

До 2022 р. на рівні ЄС було напрацьовано базову систему захисту від FIMI. Вона включала Платформу EUvsDisinfo; План дій проти дезінформації 2018 р., який формалізував FIMI як гостру внутрішню загрозу демократії ЄС; та Кодекс практики щодо дезінформації. Важливим етапом стало створення у середині 2016 р. Центру аналізу гібридних загроз ЄС (EU Hybrid Fusion Cell) у складі EEAS для аналізу розвідувальної інформації та OSINT. У квітні 2017 р. в Гельсінкі засновано Європейський центр передового досвіду з протидії гібридним загрозам (Hybrid CoE) — міжнародний хаб для країн ЄС та НАТО.

Внаслідок повномасштабної російської агресії проти України у 2022 р. гібридні загрози стрімко загострилися. FIMI еволюціонували у складні багатовимірні операції. Ключовим чинником стало використання Кремлем концепції «асиметрії витрат» — організація надзвичайно дешевих інформаційних кампаній із залученням ботів, місцевих проксі та ШІ, для захисту від яких потрібні були колосальні ресурси з боку європейських урядів. Крім того, у 2025–2026 рр. посилилася синергія російських дестабілізаційних кампаній та китайських «тактик відхилення». Важливим тригером змін стали резолюції Європарламенту (зокрема Russiagate–2024), які викрили внутрішні вразливості, механізми «корумпування» європейських політичних еліт та нелегальне фінансування радикальних партій.

Після 2022 р. ЄС перейшов до комплексної, проактивної стратегії, в основі якої лежать такі механізми:

1.Координаційна рамка та оперативне реагування. Запроваджений у 2022 р. інструментарій EU Hybrid Toolbox діє як координаційна рамка для узгодження застосування різних механізмів, таких як Cyber Diplomacy Toolbox (кіберсанкції) та заходи протидії FIMI. У травні 2024 р. Рада ЄС затвердила Гібридні команди швидкого реагування (EU Hybrid Rapid Response Teams, HRRTs) для надання оперативної вузькопрофільної допомоги державам-членам, які вперше були розгорнуті у Молдові напередодні виборів 2025 р.

2.Двоєдина система внутрішньої безпеки. З 2025 р. захист від FIMI забезпечується комплексним підходом. Стратегія ProtectEU (квітень 2025) відповідає за «жорстку» безпеку: захист критичної інфраструктури, протидію саботажу та використанню організованої злочинності. Водночас Європейський щит демократії (European Democracy Shield, листопад 2025) забезпечує «м'яку» безпеку, створюючи Європейський центр демократичної стійкості, захищаючи інформаційний простір і незалежні медіа.

3.Доктрина стримування FIMI. Концептуальним зрушенням, закріпленим у 4-му звіті EEAS (березень 2026), стало впровадження Доктрини стримування (FIMI Deterrence Playbook). Це парадигмальний зсув від простого спростування фейків до демонтажу самої тіньової інфраструктури. ЄС спрямовує санкції та правоохоронні інструменти проти посередників, PR-агентств та розробників ботнетів, атакуючи ланцюги постачання, щоб зробити гібридні операції фінансово невигідними.

4.Аналітика на базі ШІ. Європейська служба зовнішніх справ активно використовує системи штучного інтелекту для моніторингу та ідентифікації патернів скоординованої неавтентичної поведінки в реальному часі. Однак зловмисники також масштабують генерацію фейків (у 2025 р. 27% проаналізованих інцидентів містили ШІ-контент), перетворюючи це на постійну технологічну гонку.

Висновки. Еволюція стратегії Європейського Союзу відображає перехід від фрагментарних реактивних ініціатив до комплексної моделі проактивного стримування. Сучасна архітектура поєднує юридичну відповідальність платформ, єдині координаційні протоколи та розбудову соціальної стійкості. Протидія маніпуляціям інформацією сьогодні стала фундаментальною

складовою захисту демократичної цілісності та безпеки всієї європейської спільноти.

1. European Council Conclusions on external relations (19 March 2015). https://www.consilium.europa.eu/en/press/press-releases/2015/03/19/conclusions-russia-ukraine-european-council-march-2015/
2. FIMI and disinformation as global threats. EUvsDisinfo, 30.01.2026. https://euvsdisinfo.eu/fimi-and-disinformation-as-global-threats/
3. 4th EEAS Report on Foreign Information Manipulation and Interference Threats : [Annual report] / European External Action Service (EEAS). Brussels, 2026. 12 March. URL: https://www.eeas.europa.eu/sites/default/files/2026/documents/EEAS%204th%20Threat%20Report_web%20version_1.pdf
4. European Commission. Communication from the Commission on ProtectEU: a European Internal Security Strategy. COM(2025) 148 final. April 2025.
5. European Commission. Joint Communication on the European Democracy Shield. November 2025.
6. Annual Report 2025 / The Soufan Center. New York, 2026. 24 p. URL: thesoufancenter.org (дата звернення: 10.05.2026).
7. EUvsDisinfo. (2020, April 22). “To Challenge Russia’s Ongoing Disinformation Campaigns”: The Story of EUvsDisinfo. https://euvsdisinfo.eu/to-challenge-russias-ongoing-disinformation-campaigns-the-story-of-euvsdisinfo/

Методологія збагачення подій SIEM результатами аналізу мережевого трафіку засобами машинного навчання

УДК 004.056.5

Юрій Коровайченко[1], Євгеній Педченко[2], Сергій Гахов[3]

Державний університет інформаційно-комунікаційних технологій,
[1]y.korovaichenko@duikt.edu.ua, [2]e.pedchenko@duikt.edu.ua,
[3]s.gakhov@duikt.edu.ua

Операційні центри безпеки в реальній корпоративній інфраструктурі стикаються з протиріччям: платформи моніторингу подій безпеки, такі як SIEM (IBM QRadar, Wazuh, Rapid7 InsightIDR, Palo Alto XSIAM) - консолідують сотні тисяч, або навіть мільйони подій на добу, але реальне покриття мережевого рівня при цьому залишається неповним. Більшість кореляційних правил спирається на стандартні джерела подій, а саме: журнали кінцевих точок та застосунків. Мережевий потік або передається як сирий NetFlow без подальшої обробки, або взагалі залишається поза полем кореляційного аналізу. На практиці це означає, що аналітик першої лінії вимушений працювати з