НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»

ФАКУЛЬТЕТ КІБЕРБЕЗПЕКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

28 листопада 2025 року

КІБЕРБЕЗПЕКА В СУЧАСНОМУ СВІТІ: АКТУАЛЬНІ ВИКЛИКИ

МАТЕРІАЛИ VI МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Одеська юридична академія»
Факультет кібербезпеки та інформаційних технологій
Кафедра кібербезпеки

КІБЕРБЕЗПЕКА В СУЧАСНОМУ СВІТІ: АКТУАЛЬНІ ВИКЛИКИ

МАТЕРІАЛИ VI МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

28 листопада 2025 року, м. Одеса

Одеса, 2025

MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE
National University «Odesa Law Academy»
Faculty of Cybersecurity and Information Technologies
Department of Cybersecurity

CYBERSECURITY IN TODAY'S WORLD: ACTUAL CHALLENGES

MATERIALS OF THE VI INTERNATIONAL SCIENTIFIC AND PRACTICAL CONFERENCE

November 28, 2025, Odesa

Odesa, 2025

УДК 004.056

Відповідальній редактор:

О. В. Дикий, декан факультету кібербезпеки та інформаційних технологій, кандидат юридичних наук, доцент

Матеріали видано в авторській редакції.
Повну відповідальність за достовірність та якість поданого матеріалу несуть учасники конференції, їхні наукові керівники, які рекомендували ці матеріали до друку.

Рекомендовано до друку
Вченою радою Національного університету
«Одеська юридична академія»
(протокол №3 від 29.11.2025 р.)

Матеріали Міжнародної науково-практичної конференції «Кібербезпека в сучасному світі: актуальні виклики» (м. Одеса, 28 листопада 2025 р.). Одеса, 2025. 287 с.

У конференції взяли участь студенти, аспіранти, молоді вчені, викладачі та науковці. Конференція проводиться на базі Національного університету «Одеська юридична академія».

UDC 004.056

Editor-in-chief:

O. V. Dykyi, Dean of the Faculty of Cybersecurity and Information Technologies,
Candidate of Law, Associate Professor

The materials were published in the author's edition.
Full responsibility for the reliability and quality of the submitted material
bears the participants of the conference, their scientific supervisors,
who recommended these materials for publication.

Recommended for printing
by the Academic Council of the National University
«Odesa Law Academy»
(Minutes No. 3 dated 11/29/2025)

Materials of the International Scientific and Practical Conference «Cybersecurity in the Modern World: Current Challenges» (Odessa, November 28, 2025). Odesa, 2025. 287 p.

The conference was attended by students, postgraduates, young scientists, teachers and researchers. The conference is held at the National University «Odesa Law Academy».

VI Міжнародна науково-практична конференція

«Кібербезпека в сучасному світі: актуальні виклики»

28 листопада 2025 року

ТЕМАТИЧНІ НАПРЯМКИ КОНФЕРЕНЦІЇ:

Секція 1. Алгоритмічні та технічні аспекти кібербезпеки

Секція 2. Штучний інтелект та інформаційні технології

Секція 3. Управлінські, соціальні та психологічні аспекти взаємодії з кіберпростором

Секція 4. Нормативно-правові засади кібербезпеки та захисту інформації

E-mail: kiberprostirconf@gmail.com (Для питань та тез)

VI International Scientific and Practical Conference

«Cybersecurity in today's world: actual challenges»

28 November 2025 year

THEMATIC DIRECTIONS OF THE CONFERENCE:

Section 1. Algorithmic and technical aspects of cybersecurity

Section 2. Artificial intelligence and information technologies

Section 3. Management, social and psychological aspects of interaction with cyberspace

Section 4. Regulatory and legal principles of cybersecurity and information protection

E-mail: kiberprostirconf@gmail.com (Для питань та тез)

7. Перехід до кванто стійкої криптографії.
8. Забезпечення відповідності NIST, ISO/IEC 27001, IEC 62443, NERC-CIP.

Дослідження показало, що ефективний захист ОКІ можливий лише через комплексний підхід: фреймворки управління ризиками (NIST CSF та розширені моделі), використання ШІ, МН та блокчейну, посилення людського фактору через навчання, а також співпраця держави та приватних структур. Особливий акцент має бути на енергетиці, де поєднання легасі-систем та нових технологій створює критичні ризики.

Список використаної літератури:

1. Ajayi O., Alozie C., Abieba O. Enhancing Cybersecurity in Energy Infrastructure: Strategies for Safeguarding Critical Systems in the Digital Age. Trends in Renewable Energy. 2025. Vol. 11, No. 2. P. 201-212.
2. Alozie C., Chinwe E. Developing a Cybersecurity Framework for Protecting Critical Infrastructure in Organizations. Iconic Research And Engineering Journals. 2025. Vol. 8, No. 7. P. 562-576.
3. Shah S. Machine Learning for Cyber Threat Detection and Prevention in Critical Infrastructure. Journal of Global Research in Electronics and Communication. 2025. Vol. 2, No. 2. P. 1-6.
4. Aljumaiah O., Jiang W., Addula S., Almaiah M. Analyzing Cybersecurity Risks and Threats in IT Infrastructure based on NIST Framework. Journal of Cyber Security and Risk Auditing. 2025. Vol. 2025, No. 2. P. 12-26.

Ключові слова: кібербезпека, об'єкти критичної інфраструктури (ОКІ), штучний інтелект (ШІ), NIST фреймворк для кібербезпеки.
Keywords: cybersecurity, critical infrastructure facilities (CIF), artificial intelligence (AI), NIST Cybersecurity Framework (NIST CSF).

АНАЛІЗ ІНСТРУМЕНТІВ ТА ПЛАТФОРМ ДЛЯ ТРЕКІНГУ ЕКСПЕРИМЕНТІВ

Савенко Михайло

Національний університет «Одеська юридична академія»,
студент факультету кібербезпеки та інформаційних технологій

У сучасному науковому середовищі, де машинне навчання стає ключовим елементом інноваційних розробок, трекінг експериментів набуває критичного значення як засіб забезпечення відтворюваності, порівнянності та ефективності дослідницьких процесів. Трекінг експериментів охоплює систематичний збір, зберігання та аналіз метаданих, параметрів, метрик продуктивності та артефактів, що виникають під час ітеративних циклів

розробки моделей, від підготовки даних до розгортання в продуктивне середовище. Цей процес не лише полегшує виявлення оптимальних конфігурацій моделей, але й сприяє колективній роботі команд, дозволяючи уникнути дублювання зусиль і полегшуючи аудит результатів.

Одним з фундаментальних аспектів трекінгу є забезпечення відтворюваності, яка досягається через фіксацію всіх вхідних та вихідних параметрів експерименту. Уявіть типовий цикл: дослідник вибирає датасет, налаштовує гіперпараметри мережі, запускає тренування на графічному процесорі та оцінює модель за допомогою кросвалідації. Без трекінгу цей процес перетворюється на ланцюг непередбачуваних подій, де успішний результат важко повторити через зміни у версіях бібліотек чи то випадкові фактори. Сучасні платформи вирішують цю проблему, впроваджуючи автоматизовані хуки для логування, які активуються на етапі ініціалізації тренування. Такі системи не лише зберігають числові метрики, як-от точність чи функцію втрат, а й фіксують текстові описи, знімки градієнтів та навіть логи обчислень, дозволяючи провести ретроспективний аналіз.

Інтеграція трекінгу з пайплайнами автоматизації, такими як оркестрація робочих потоків, підвищує ефективність на 30-50%, оскільки дозволяє автоматизувати гіперпараметричний пошук і моніторинг дрейфу даних. Це особливо актуально для великих команд, де колаборація вимагає централізованого доступу до історії експериментів, з можливістю коментування та розподілу ролей [1].

З-посеред інших платформа **MLflow** вирізняється своєю універсальністю як відкрита система для керування життєвим циклом машинного навчання. Вона складається з кількох компонентів, де модуль трекінгу дозволяє фіксувати параметри, метрики та артефакти для кожного запуску, створюючи ієрархію проєктів і експериментів. Користувач може запустити сервер трекінгу локально або в хмарі, після чого через програмний інтерфейс логуються дані в реальному часі з можливістю фільтрації за тегами чи значеннями метрик. Перевагою MLflow є інтеграція з різними мовами програмування та фреймворками, що робить її ідеальною для гетерогенних середовищ, де команди використовують як Python, так і R [2]. На практиці це дозволяє провести серію експериментів з варіаціями архітектури, автоматично генеруючи звіти про продуктивність, без потреби ручного копіювання файлів. Дослідження артефактів життєвого циклу підкреслює, що MLflow досягає високого рівня покриття критеріїв логування та версіонування, перевершуючи базові інструменти за інтеграцією з оркестраторами, як-от Kubeflow. Однак, для великих обсягів даних, де потрібна розподілена обробка, MLflow рекомендується комбінувати з інструментами версіонування, щоб уникнути перевантаження локального сховища [3].

Іншою потужною платформою є **Weights & Biases**, яка орієнтована на візуалізацію та колаборацію в процесі трекінгу. Ця система автоматично відстежує метрики під час тренування, генеруючи інтерактивні панелі з графіками втрат, матрицями плутанини та гістограмами гіперпараметрів, що полегшує інтерпретацію складних траєкторій. Користувачі можуть створювати «свіпи» – масові запуски з варіаціями параметрів, – і миттєво порівнювати результати через паралельні криві, виявляючи оптимальні точки. У контексті командної роботи Weights & Biases надає робочі простори для спільного редагування з нотифікаціями про завершення експериментів та інтеграцією з системами контролю версій [4]. Ця платформа вирізняється обробкою програмних артефактів, дозволяючи фіксувати залежності та середовища, що критично для відтворюваності в мультиплатформових проєктах. Попри хмарну орієнтацію, яка забезпечує масштабованість, користувачі відзначають потребу в локальних опціях для чутливих даних, де конфіденційність переважає зручність [5].

Платформа **Neptune.ai** акцентована на метаданих як на основі трекінгу. Вона пропонує централізоване сховище для датасетів, моделей і логів експериментів. Через програмний інтерфейс дослідник може маркувати запуски тегами, додавати кастомні метрики та прикріплювати артефакти, як-от: знімки моделей чи то звіти. Візуальний дашборд дозволяє будувати кастомні запити, фільтрувати експерименти за продуктивністю або часом виконання, з можливістю експорту в формати для подальшого аналізу. Neptune.ai здатна значно знизити помилки в постекспериментальних задачах, досягаючи 7% рівня помилок проти 48% без інструментів, завдяки інтуїтивному інтерфейсу для порівнянь [3]. Ця платформа корисна для академічних середовищ, де потрібно документувати процеси для публікацій, але вимагає навчання для повного використання автоматизованих пайплайнів.

Інструмент **Sacred** пропонує мінімалістичний підхід до конфігурації та логування, інтегруючись безпосередньо в скрипти тренування. Він фіксує конфігурації як YAML-файли, автоматично генерує ідентифікатори для запусків і дозволяє моніторити метрики через бази даних чи файли [6]. Sacred вирізняється можливістю редагування конфігурацій без перезапуску коду, що прискорює ітерації, та інтеграцією із системами моніторингу для реального часу. Недоліком є обмежена візуалізація, що робить його доповненням до графічних платформ [1].

Платформа **ClearML**, як частина екосистеми MLOps, автоматизує трекінг через «магічні» хуки, що активуються без значних змін у коді, фіксуючи все від ресурсів до артефактів [2]. Вона підтримує віддалене виконання на кластерах, з дашбордом для моніторингу кількох запусків паралельно. ClearML здатна на високу автоматизацію колекції, аж до 64% непрямої

фіксації, що зменшує навантаження на розробників [1]. У промислових проєктах це дозволяє масштабувати експерименти на тисячі ядер, але вимагає налаштування сервера для приватних розгортань.

Інструмент **DVC** (Data Version Control) розширює традиційний контроль версій на дані та моделі через трекінг метафайлів, які посилаються на хеші файлів. Він інтегрується з Git для повного відтворення пайплайнів, дозволяє кешувати проміжні результати та порівнювати версії датасетів [7]. Це робить його ідеальним для відкритих проєктів, де прозорість коду є пріоритетом.

Платформа **Comet.ml** фокусується на оптимізації, пропонуючи інструменти для автоматизованого трекінгу гіперпараметрів та A/B-тестування моделей. Вона генерує звіти з тепловими картами продуктивності і дозволяє виявляти кореляції між параметрами. Її сильними сторонами є обробка залежностей та інтеграція з моніторингом для постпродакшну. Користувачі цінують мобільність інтерфейсу, але критикують вартість для великих команд [5].

Для прозорості трекінгу розроблено інструмент **PyPads**, який забезпечує неінтрузивне логування без змін у коді, фіксує контекст виконання через декоратори. Він створює структуровані логи з метаданими, доступними для аналізу в Jupyter [8]. PyPads корисний в освітніх проєктах, де студенти потребують детального трасування.

Метамодель **EMMM** пропонує уніфікований фреймворк для трекінгу, який стандартизує метадані через абстрактну модель, що інтегрується з наявними платформами. Вона визначає сутності як експерименти, активи та залежності, дозволяє кросплатформову міграцію. Важливою є її роль у зменшенні фрагментації і забезпеченні семантичної узгодженості. У майбутніх розробках це може стати основою для API-стандартів [9].

Подальший розвиток трекінгу стосується інтеграції з AutoML, де інструменти автоматично генерують експерименти, фіксуючи еволюцію пошуку. У проєктах з великими мовними моделями трекінг розширюється на моніторинг токенів та етичних метрик, запобігаючи упередженням.

Наявні інструменти формують екосистему, де трекінг не є ізольованою функцією, а частиною інтегрованого ланцюга, що підвищує наукову цінність досліджень. Їх вибір залежить від масштабу проєкту з акцентом на відкриті рішення для академії та хмарні для індустрії.

Список використаних джерел:

1. Hewage D., Meedeniya D. Machine Learning Operations: A Survey on MLOps Tool Support. *Arxiv.* 2022. Vol. 2202. P. 1-12. DOI: https://doi.org/10.48550/arXiv.2202.10169
2. Ruggeri D., Tazza G., Vidács L. Introducing MLOps to Facilitate the Development of Machine Learning Models in Agronomy: A Case Study. *IEEE Access.* 2025. DOI: https://doi.org/10.1109/ACCESS.2025.3586691

3. Berberi L., Kozlov V., Alibabaei Kh., Sanchis B. MLflow and its usage. *AI4EOSC Platform: Users' Workshop.* 2023. DOI: https://doi.org/10.13140/RG.2.2.32801.17761.
4. W&B Models. URL: https://docs.wandb.ai/models.
5. Idowu S., Strüber D., Berger T. Asset management in machine learning: A survey. IEEE/ACM 43rd International Conference on Software Engineering: Software Engineering in Practice (ICSE-SEIP). 2021. P. 51-60. DOI: https://doi.org/10.1109/ICSE-SEIP52600.2021.00014
6. Idowu S., Osman O., Strüber D. et al. Machine learning experiment management tools: a mixed-methods empirical study. *Empir Software Eng*. 2024. Vol. 29, 74. DOI: https://doi.org/10.1007/s10664-024-10444-w
7. Barrak A., Eghan E. E., Adams B. On the co-evolution of ml pipelines and source code-empirical study of dvc projects. *IEEE International Conference on Software Analysis, Evolution and Reengineering (SANER).* 2021. March. P. 422-433. IEEE. DOI: https://doi.org/10.1109/SANER50967.2021.00046.
8. Weißgerber T., Amor M. B., Fellicious C. et al. PyPads. *Datenbank Spektrum*. 2024. Vol. 24. P. 53-62. DOI: https://doi.org/10.1007/s13222-023-00459-w.
9. Idowu S., Strüber D., Berger T. EMMM: A Unified Meta-Model for Tracking Machine Learning Experiments. *48th Euromicro Conference on Software Engineering and Advanced Applications (SEAA).* 2022. P. 48-55. DOI: https://doi.org/10.1109/SEAA56994.2022.00016.

Ключові слова: вебдизайн, вебпрограмування, візуалізація, колір.
Keywords: web design, web programming, visualization, color.

Науковий керівник: к.т.н., доцент Трофименко О.Г.

АРХІТЕКТУРНІ ТА АЛГОРИТМІЧНІ ВИКЛИКИ НАВЧАННЯ ASR-МОДЕЛЕЙ ДЛЯ РОЗПІЗНАВАННЯ УКРАЇНСЬКОГО МОВЛЕННЯ

Антіпіна Надія

Національний університет «Одеська юридична академія»,
студентка факультету кібербезпеки та інформаційних технологій

На відміну від класичних задач класифікації, розпізнавання мовлення має свої характерні особливості. У системах розпізнавання мовлення (ASR-системах) модель має навчитися перетворювати довгу послідовність звукових фреймів у значно коротшу послідовність символів без чіткої відповідності довжин між вхідними та вихідними послідовностями. Щоб вирішити цю проблему, додається алгоритм CTC (Connectionist Temporal Classification), який допомагає моделі самостійно навчитися вирівнювати аудіопослідовності змінної довжини з відповідними текстовими транскрипціями змінної довжини без необхідності зазначення точних часових проміжків кожного символу [1]. Також під час роботи з великими нейронними мережами виникає ризик перенавчання, коли через недостатню кількість прикладів система

ЗМІСТ