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)

ІНФОРМАЦІЙНА ГЕОМЕТРІЯ ЯК ІНСТРУМЕНТ ПІДВИЩЕННЯ ТОЧНОСТІ АЛГОРИТМІВ МАШИННОГО НАВЧАННЯ

Чепурна Олена

доцент кафедри кібербезпеки Національного університету «Одеська юридична академія», кандидат фізико-математичних наук

Черевко Євген

доцент кафедри кібербезпеки Національного університету «Одеська юридична академія», кандидат фізико-математичних наук

Розвиток систем машинного навчання вимагає дедалі точніших засобів представлення та аналізу структур даних. Одним із таких підходів є інформаційна геометрія, яка оперує поняттями статистичних многовидів, дивергенцій, метричних структур і ріманових метрик для моделювання параметричних просторів розподілів. Її методи дозволяють переходити від класичного евклідового простору до більш придатних для аналізу інформаційних просторів, де зберігається інваріантність до деформацій і логарифмічних масштабувань [1, с. 18].

Центральним об'єктом аналізу є статистичний многовид – гладкий многовид , у якому кожна точка відповідає розподілу ймовірностей , де – вектор параметрів. Визначеною на ньому метрикою є метрика Фішера, яка вводиться як:

$$g_{ij}(\theta) = \mathbb{E}[\frac{\partial \log\, p(x;\theta)}{\partial \theta_i} \frac{\partial \log\, p(x;\theta)}{\partial \theta_j}],$$

де очікування береться відносно $p(x;\theta)$. Така метрика дозволяє визначити геодезичні криві, обчислювати довжини та кути між напрямами зміни параметрів, що уможливлює побудову ефективних алгоритмів градієнтного спуску у задачах навчання [2, с. 142–143].

Іншим важливим поняттям є дивергенція Кульбака–Лейблера:

$$D_{\mathrm{KL}}(p \parallel q) = \int p(x) \log \frac{p(x)}{q(x)}\, dx,$$

яка відіграє роль функції відстані між двома розподілами, незважаючи на її несиметричність. Геометрична структура, індукована цією дивергенцією, забезпечує можливість оптимізації моделей у задачах класифікації, регресії та виявлення аномалій [3, с. 79].

У сфері кібербезпеки особливої уваги заслуговує застосування інформаційно-геометричних методів до задач виявлення вторгнень (IDS), де ймовірнісні розподіли ознак мережевого трафіку можуть розглядатися як точки на статистичному многовиді. Наприклад, зміна геодезичної відстані між

базовим розподілом нормального трафіку та поточним розподілом може свідчити про відхилення, що наближається до аномального режиму [4, с. 33].

У сучасних підходах дедалі активніше інтегруються методи інформаційної геометрії в алгоритми навчання на багатовимірних даних. Наприклад, у роботі [5, с. 11–22] описані геометричні метрики які можна використовувати як частину механізму оптимізації в багаторівневих моделях. Такі підходи вже знаходять практичне застосування в розподілених інтелектуальних системах, зокрема в енергетичних мережах, де необхідна здатність до адаптивного реагування на аномалії в режимі реального часу [6, с. 9–11].

Додаткову роль у формуванні геометрії статистичного простору відіграє концепція двоїстих зв'язностей (Dual Affine Connections), яка дозволяє моделювати не лише симетричні, а й асиметричні зв'язки між розподілами. Це актуально в системах, де має місце неповна інформація або різнотипні джерела даних (наприклад, кіберфізичні системи з мультисенсорними потоками) [7, с. 213–215].

Нормативний та методологічний контекст також формує запит на використання інформаційної геометрії в системах оцінювання ризиків. У межах структури NIST Cybersecurity Framework 2.0 [8] можуть бути інтегровані геометричні моделі як частина інструментарію для ідентифікації критичних відхилень, зокрема в аналітиці поведінки користувачів та обчислювальних систем.

Водночас українське правове поле, зокрема Закон України «Про основні засади забезпечення кібербезпеки України» [9], визначає принципи захисту інформаційних ресурсів, які можуть бути вдосконалені через використання математично строго обґрунтованих методів виявлення ризиків.

Враховуючи зростаючу складність кіберзагроз та обмеженість класичних статистичних методів при роботі з великомасштабними даними високої розмірності, інформаційна геометрія відкриває нові напрямки для досліджень. Одним із перспективних напрямів є подальше формалізоване вивчення геометрії статистичних многовидів для побудови інваріантних моделей виявлення аномалій у середовищах з нестабільною розподільчою структурою. Зокрема, це стосується OT/ICS-архітектур, розподілених систем контролю та адаптивних систем в енергетичній, транспортній та телекомунікаційній інфраструктурах.

Окремий інтерес становить застосування інформаційно-геометричних моделей у поєднанні з байєсівськими і варіаційними методами для поліпшення стійкості до атак типу Adversarial, що особливо актуально у сфері безпеки автономних систем. Також доцільно розглядати інтеграцію рімановых метрик та геодезичних дивергенцій до структур Explainable AI (XAI), що дозволить інтерпретувати поведінку критичних моделей у кібербезпекових системах.

З практичної точки зору, доцільним є впровадження окремих компонентів інформаційної геометрії у нормативні та методологічні рамки управління ризиками, а також у проєктування процедур виявлення аномалій у системах реагування CERT-типу. Такий підхід дозволить підвищити як точність виявлення інцидентів, так і адаптивність до нових сценаріїв загроз.

Узагальнено використання інформаційної геометрії як структурного підходу в задачах аналізу даних та побудови безпечних систем відкриває простір для міждисциплінарних досліджень, що поєднують кібербезпеку, диференціальну геометрію, статистику та теорію інформації.

Список використаних джерел:

1. Amari S. Information Geometry and Its Applications. Springer. 2016. 381 p. DOI: 10.1007/978-4-431-55978-8.
2. Nielsen F. An Elementary Introduction to Information Geometry. Entropy. 2020. Vol. 22. No. 10. P. 1100. DOI: 10.3390/e22101100.
3. Cover T.M., Thomas J.A. Elements of Information Theory. 2nd ed. Wiley. 2006. 784 p. ISBN: 978-0471241959.
4. Derhab A., Bouras A. Multivariate correlation analysis and geometric linear similarity for real-time intrusion detection systems. Security and Communication Networks. 2015. Vol. 8. No. 4. P. 1193–1212. DOI: 10.1002/sec.1074.
5. Cherevko Y., Chepurna O., Kuleshova Y. On Information Geometry Methods for Data Analysis. Geometry Integrability and Quantization. 2024. Vol. 29. P. 11–22. DOI: 10.7546/giq-29-2024-11-22.
6. Chen Y., Li C., Xu Z. Information Geometry Based Anomaly Detection for Cyber–Physical Systems. IEEE Transactions on Industrial Informatics. 2020. Vol. 16. No. 9. P. 6193–6202. DOI: 10.1109/TII.2019.2952914.
7. Lauritzen S.L. Statistical Manifolds. In: Differential Geometry in Statistical Inference. Institute of Mathematical Statistics. 1987. P. 163–216. DOI: 10.1214/lnms/1215454097.
8. National Institute of Standards and Technology. The NIST Cybersecurity Framework 2.0. 2024. URL: https://www.nist.gov/cyberframework
9. Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII. Відомості Верховної Ради України. 2017. № 45. Ст. 403. URL: https://zakon.rada.gov.ua/laws/show/2163-19

Ключові слова: інформаційна геометрія, статистичні многовиди, геодезичні відстані, Riemann-метрика, виявлення аномалій, машинне навчання, кібербезпека, дивергенція, інтерпретованість моделей, захист критичної інфраструктури

Keywords: information geometry, statistical manifolds, geodesic distance, Riemannian metric, anomaly detection, machine learning, cybersecurity, divergence, model interpretability, critical infrastructure protection

ЗМІСТ