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)

робить її придатною для аналізу великих обсягів даних. Простота використання – не потребує складного налаштування параметрів для досягнення стабільної якості класифікації.

Отже, використання алгоритму Random Forest у поєднанні з TF-IDF-представленням коду забезпечує збалансоване поєднання високої точності, стійкості до варіативності студентських рішень і достатньої прозорості оцінювання. Це робить обраний підхід ефективним інструментом для реалізації інтелектуальної системи автоматизованої перевірки лабораторних робіт з програмування мовою Python.

Список використаних джерел:

1. Random Forest, Explained: A Visual Guide with Code Examples. URL: https://surl.li/usfdoz (дата звернення: 10.11.2025)
2. Understanding TF-IDF (Term Frequency-Inverse Document Frequency). URL: https://surl.li/ouyept (дата звернення: 10.11.2025)
3. Intro to Model Tuning: Grid and Random Search. URL: https://surl.li/ygdymi (дата звернення: 10.11.2025)

Ключові слова: машинне навчання, алгоритм, інтелектуальна система, Random Forest
Keyword: machine learning, algorithm, intelligent system, Random Forest

Науковий керівник: доц. Логінова Н.І.

ІНТЕРНЕТ РЕЧЕЙ (IOT) ЯК ІНСТРУМЕНТ БІЗНЕС-МЕНЕДЖМЕНТУ

Літовченко Данило

студент 1 курсу факультету адвокатури та антикорупційної діяльності Національного університету «Одеська юридична академія»

Інтернет речей, або Internet of Things (IoT), перетворився на одну з ключових технологій, що формує новий тип управлінської логіки в бізнесі. У центрі цієї концепції лежить взаємодія фізичних об'єктів через мережу, що дає змогу збирати, передавати та аналізувати дані в режимі реального часу. Таке середовище даних створює нові можливості для бізнес-менеджменту, в якому швидкість прийняття рішень, точність прогнозування та оперативна адаптація стають критично важливими [1].

Сучасні компанії інтегрують IoT для оптимізації виробництва, логістики, контролю якості, автоматизації управління ресурсами та формування інтелектуальних продуктів і сервісів. Таким чином, IoT стає фундаментальним елементом цифрової трансформації й рушійною силою конкурентних переваг у глобальній економіці [2].

Даний звіт досліджує сутність IoT, механізми його роботи та ключові напрями застосування у бізнес-менеджменті. Аналіз охоплює можливості, ризики, переваги та перспективи подальшого розвитку IoT як інструменту управління. Особлива увага приділяється практичним прикладам, що демонструють реальну цінність технології для управлінських процесів.

Архітектура IoT базується на з'єднанні фізичних пристроїв через інтернет або локальні мережі, утворюючи багаторівневу систему. Основу складають сенсори, контролери, мережеві протоколи та хмарні платформи, які забезпечують збір, передобробку та аналіз даних. Кожен фізичний об'єкт виступає вузлом даних, передаючи інформацію в аналітичні платформи. Такі дані дозволяють керівникам виявляти приховані закономірності, контролювати навантаження на обладнання, прогнозувати несправності та підвищувати точність управлінських рішень [3].

Функціонування IoT забезпечується сучасними бездротовими технологіями: Wi-Fi, Bluetooth Low Energy, Narrowband IoT, LTE-M і 5G. Поява 5G особливо важлива, оскільки вона дає високу пропускну здатність, мінімальні затримки та можливість одночасного підключення великої кількості пристроїв. Це робить IoT придатним для складних корпоративних інфраструктур та промислових середовищ [4].

IoT значно підсилює ефективність операційних процесів. Сенсорні системи контролюють виробниче обладнання, аналізують технічний стан, прогнозують поломки та дозволяють автоматизувати технічне обслуговування. Такий підхід мінімізує простої, скорочує витрати та збільшує продуктивність. IoT переводить управління у стан, де рішення приймаються на основі фактичних даних, а не припущень, що суттєво підвищує точність управління [5].

Концепція прозорої логістичної інфраструктури також формується за допомогою IoT. Використання RFID-міток, GPS-трекерів, датчиків температури та систем моніторингу забезпечує доступ до даних про рух товару в реальному часі. Це дозволяє оптимізувати маршрути транспортування, уникати псування продукції, прогнозувати затримки та раціонально розподіляти складські ресурси. Управління ланцюгами постачання стає точним, що позитивно впливає на прибутковість бізнесу [6].

Аналітика є ключовим елементом IoT у бізнесі. Технологія створює великий потік даних, які обробляються за допомогою машинного навчання, статистичних моделей та штучного інтелекту. Компанії можуть прогнозувати попит, моделювати поведінку споживачів, виявляти відхилення у роботі систем і точніше планувати діяльність. IoT фактично формує нову культуру менеджменту, засновану на даних, а не на інтуїції.

Активне застосування IoT також стосується взаємодії зі споживачами. Розумні пристрої збирають дані про поведінку клієнтів, відстежують їхні

переваги й дозволяють створювати персоналізовані пропозиції. Це формує модель випереджальної клієнтської підтримки, у якій компанія передбачає потребу до того, як клієнт її висловить. Таким чином, IoT виступає основу для побудови лояльності й індивідуалізованого сервісу.

Незважаючи на значні переваги, IoT супроводжується суттєвими викликами. Одним із центральних є інформаційна безпека: велика кількість підключених пристроїв створює значну поверхню атаки, ускладнює сегментацію мережі, оновлення прошивок і управління правами доступу [7].

Додатково існують питання конфіденційності персональних даних, сумісності обладнання, високої вартості впровадження та інтеграції із застарілими системами. Бізнес має розробляти комплексні стратегії захисту та впроваджувати кібербезпекові стандарти для мінімізації ризиків.

Очікується масштабне зростання IoT-рішень у корпоративному секторі протягом найближчих років. Технологія стає доступнішою, швидшою та інтелектуальнішою. Поширення 5G, розвиток хмарних платформ та поява нових сенсорів сприятимуть розширенню IoT у виробництві, транспорті, фінансах, медицині та сфері обслуговування. IoT стає не просто інструментом, а базовою інфраструктурою бізнесу.

Новий аспект полягає у впровадженні IoT у межах інтегрованого управління процесами підприємства (Business Process Management). Об'єднання IoT і BPM дозволяє створити адаптивні ланцюги процесів, які автоматично реагують на зміни контексту та внутрішнього стану системи. Це відкриває шлях до автономізації управлінських рішень і структурної оптимізації бізнес-операцій [8].

Другим важливим напрямом розвитку є екологічний і соціальний вплив IoT. Підприємства впроваджують рішення для моніторингу енерговитрат, викидів, якості довкілля і стану інфраструктури; це дозволяє керівництву підвищувати екологічну відповідальність та звітування відповідно до міжнародних стандартів сталого розвитку. Таким чином, IoT стає інструментом не лише управлінського, але й стратегічного характеру.

Назагал, Інтернет речей є одним із найважливіших інструментів менеджменту в сучасному бізнесі. Його застосування охоплює оптимізацію виробництва, покращення логістики, цифрову аналітику, формування клієнтоорієнтованих стратегій та створення інтелектуальних бізнес-моделей. Компанії, які впроваджують IoT-технології, отримують конкурентні переваги, знижують витрати та підвищують якість управління. Незважаючи на супутні ризики, IoT стає ключовою технологією економіки даних.

Список використаних джерел

1. Sevak K.Y. "The evolution of Internet of Things (IoT) research in business and management." Journal of Information Technology & Digital Economy. 2024. URL:

https://www.emerald.com/jide/article/4/3/242/1212329/The-evolution-of-Internet-of-Things-IoT-research [дата звернення: 06.11.2025]
2. IoT in Business Management: Opportunities, Challenges and Future Implications. ResearchGate. 2023. URL: https://www.researchgate.net/publication/370952972_IoT_in_Business_Management_Opportunities_Challenges_and_Future_Implications [дата звернення: 06.11.2025]
3. The Role of the Internet of Things (IoT) in Business and ... Atlantis Press. 2021. URL: https://www.atlantis-press.com/article/125960576.pdf [дата звернення: 06.11.2025]
4. Applications for the Internet of Things (IoT) in business. Nexford Insights. 2025. URL: https://www.nexford.edu/insights/applications-for-the-internet-of-things-iot-in-business [дата звернення: 06.11.2025]
5. Internet of Things: Impact on business. InovaDigital. 2022. URL: https://www.inovadigital.eu/en/internet-of-things-impact-on-business/ [дата звернення: 06.11.2025]
6. How IoT has Impacted Business Operations. PXP Blog. URL: https://pxp.io/blog/iot-in-business-operations [дата звернення: 06.11.2025]
7. Nearly half of network connections come from high-risk IoT and IT devices – TechRadar. (2025) URL: https://www.techradar.com/pro/security/nearly-half-of-network-connections-come-from-high-risk-iot-and-it-devices-so-make-sure-youre-protected [дата звернення: 06.11.2025]
8. On the Interplay Between Business Process Management and IoT. Business & Information Systems Engineering. 2024. URL: https://link.springer.com/article/10.1007/s12599-024-00859-6 [дата звернення: 06.11.2025]

Ключові слова: Інтернет речей; цифрова трансформація; аналітика бізнес-даних; логістика й виробництво; кібербезпека пристроїв.
Keywords: Internet of Things; digital transformation; business data analytics; logistics and manufacturing; IoT cybersecurity.

Науковий керівник: к.ю.н. доцент Чанишев Р.І.

МЕТОДИ МАШИННОГО НАВЧАННЯ ДЛЯ ВИЗНАЧЕННЯ СТИЛІВ НАВЧАННЯ

Дашдаміров Гліб

студент 2 курсу магістратури факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Моделі машинного навчання (МН) відкривають нові можливості для виявлення прихованих закономірностей у поведінці здобувачів освіти, їхніх взаємодіях з навчальним контентом, темпах засвоєння матеріалу та когнітивних патернах. Використання таких моделей дозволяє не лише класифікувати стилі навчання (візуальний, аудіальний тощо), а й прогнозувати ефективність освітніх стратегій, адаптувати контент у реальному часі та підвищувати мотивацію здобувачів.

ЗМІСТ