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)

Список використаних джерел:

1. AI bias in law enforcement. *Europol*. 27.07.2025. URL: https://www.europol.europa.eu/publications-events/publications/ai-bias-in-law-enforcement
2. Vaswani A., Shazeer N., Parmar N., Uszkoreit J., Jones L., Gomez A. N., Kaiser Ł., Polosukhin I. Attention is all you need. *Advances in Neural Information Processing Systems*. 2017. Vol. 30. P. 5998–6008. URL: https://proceedings.neurips.cc/paper/2017/hash/3f5ee243547dee91fbd053c1c4a845aa-Abstract.html
3. ESET discovers PromptLock, the first AI-powered ransomware. *ESET Research.* 27.08.2025. URL: https://www.eset.com/us/about/newsroom/research/eset-discovers-promptlock-the-first-ai-powered-ransomware .
4. GTIG AI Threat Tracker: Advances in Threat Actor Usage of AI Tools. *Google Threat Intelligence Group.* 6.11.2025. URL: https://cloud.google.com/blog/topics/threat-intelligence/threat-actor-usage-of-ai-tools/

Ключові слова: самовдосконалювані віруси, штучний інтелект, ШІ, трансформерні архітектури.
Keywords: self-improving viruses, artificial intelligence, AI, transformative architectures.

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

МАШИННЕ НАВЧАННЯ У ПЕРЕВІРЦІ ПРОГРАМНИХ КОДІВ: ЕФЕКТИВНІСТЬ АЛГОРИТМУ RANDOM FOREST

Григор'єв Олександр

студент 2 курсу магістратури факультету кібербезпеки та інформаційних технологій Національний університет «Одеська юридична академія»

Перевірка лабораторних робіт з програмування є складним завданням для викладачів, оскільки вимагає великих зусиль як у плані часу, так і когнітивних витрат. Використання методів машинного навчання (МН) дозволяє створити інтелектуальну систему, яка може автоматизувати аналіз програмного коду, виявляти помилки та оцінювати стиль програмування. Для цього рекомендується використовувати алгоритм Random Forest, який поєднує високу точність класифікації з прийнятною швидкістю роботи, забезпечує можливість інтерпретації результатів та виявляє високу стійкість до шумових даних.

Алгоритм Random Forest – це метод машинного навчання, який використовує незалежні дерева рішень, побудовані на основі навчальної вибірки з відомими класами. Кожне дерево навчається на випадковій підмножині даних, враховуючи лише деякі ознаки при формуванні вузлів. Узагальнене рішення моделі визначається шляхом голосування дерев для класифікації або усереднення їхніх прогнозів для регресії [1].

Вибір алгоритму Random Forest для задачі автоматизованої перевірки програмного коду обумовлений низкою переваг. В процесі аналізу програмного коду, використовуються чотири категорії ознак: лексичні, синтаксичні, семантичні та поведінкові. Даний алгоритм ефективно обробляє такі неоднорідні дані без необхідності їх нормалізації або стандартизації, на відміну від багатьох інших алгоритмів машинного навчання. Алгоритм Random Forest дозволяє визначити важливість кожної ознаки, що надає можливість аналізу того, які характеристики коду найбільше впливають на кінцевий результат оцінювання. Це особливо важливо у контексті навчального процесу, де пояснюваність моделі сприяє об'єктивності оцінки та дозволяє викладачам зрозуміти логіку прийняття рішень системою.

Лабораторні роботи здобувачів можуть містити як незначні синтаксичні помилки, так і логічні неточності. Завдяки ансамблевій природі Random Forest є менш чутливим до таких відхилень, ніж окремі класифікатори (наприклад, окреме дерево рішень або логістична регресія).

Модель може бути легко розпаралелена, що забезпечує швидку обробку великої кількості робіт навіть за умови збільшення обсягу даних. Це дозволяє ефективно використовувати метод у реальних умовах, коли система обробляє роботи групи з 25–30 студентів.

Основні параметри моделі (кількість дерев n_estimators, глибина дерева max_depth, мінімальна кількість зразків у листі min_samples_leaf) дозволяють збалансувати точність і швидкодію системи відповідно до конкретних вимог навчального закладу.

Модель для автоматизованої перевірки лабораторних робіт побудована за принципом послідовного конвеєра (pipeline), що поєднує етапи попередньої обробки коду, його векторизації та класифікації результатів.

На початковому етапі здійснюється очищення програмного коду від коментарів, уніфікація імен змінних і функцій, а також нормалізація форматування. Така обробка дає змогу усунути вплив несуттєвих відмінностей у стилі програмування та зосередитися на структурі й логіці реалізації алгоритму.

Векторизація коду перетворює програмний код у числове представлення за допомогою методу TF-IDF (Term Frequency – Inverse Document Frequency [2]), який визначає вагомість кожного токена в межах усієї вибірки. Це дозволяє моделі виокремлювати найважливіші елементи синтаксичної структури програм і враховувати частотні закономірності, характерні для різних типів рішень.

Отримані вектори ознак передаються до класифікаційної моделі, побудованої на основі визначеного алгоритму, який формує ансамбль дерев рішень, де кожне дерево приймає власне рішення, а підсумковий результат

визначається за принципом більшості голосів. Такий підхід забезпечує стійкість моделі до шумових даних і зменшує ризик перенавчання.

Модель інтегрується у процес перевірки робіт у вигляді конвеєра, реалізованого засобами бібліотеки Scikit-learn мовою програмування Python.

Ефективність роботи моделі Random Forest залежить від правильного налаштування її параметрів:

n_estimators (кількість дерев у лісі) – показує кількість дерев рішень, що входять до складу ансамблю. Збільшення кількості дерев підвищує точність моделі, але збільшує час навчання та обсяг використовуваної пам'яті.

max_depth (максимальна глибина дерева) – обмежує глибину кожного дерева. Значення None дозволяє дереву розгалужуватися до повного поділу даних, що забезпечує максимальну точність за умови достатнього обсягу тренувальних даних.

min_samples_split (мінімальна кількість зразків для поділу вузла) – визначає мінімальну кількість зразків, необхідних для поділу внутрішнього вузла. Більші значення запобігають перенавчанню.

max_features (кількість ознак при поділі) – визначає кількість ознак, що розглядаються при кожному поділі. Зазвичай задається як квадратний корінь із загальної кількості ознак.

random_state – фіксується для забезпечення відтворюваності результатів при повторних запусках моделі.

Оптимальні значення параметрів визначаються за допомогою методів пошук за сіткою або випадковий пошук, що дозволяє знайти найкращий баланс між точністю моделі та її обчислювальною ефективністю.

Пошук за сіткою (Grid Search) працює за допомогою сітки значень гіперпараметрів і для кожної комбінації навчається модель та вона оцінюється на основі даних перевірки. У цьому підходу перевіряється кожна окрема комбінація значень гіперпараметрів, що може бути дуже неефективно.

Випадковий пошук (Randomized Search) – створюється сітка значень гіперпараметрів та обирається випадкові комбінації для навчання моделі та оцінювання. Кількість ітерацій пошуку встановлюється на основі часу/ресурсів [3].

Перевагами використання алгоритму Random Forest для створення та навчання моделі є висока точність класифікації – модель поєднує результати багатьох незалежних дерев рішень, що забезпечує точність на рівні 85-92%. Стійкість до неповних даних – алгоритм ефективно працює навіть у випадку перевірки робіт здобувачів, які можуть містити помилки або відмінності в стилі програмування. Оцінювання важливості ознак – можливість визначити, які характеристики коду найбільше впливають на підсумкову оцінку, що підвищує інтерпретованість результатів. Масштабованість – модель легко розпаралелюється та може працювати в паралельному режимі, що

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].

ЗМІСТ