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)

2. Top Cybersecurity Statistics for 2025 [Електронний ресурс]. URL: https://www.cobalt.io/blog/top-cybersecurity-statistics-2025 (дата звернення: 09.11.2025).
3. Cyber Security Breaches Survey 2025 [Електронний ресурс]. URL: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2025/cyber-security-breaches-survey-2025 (дата звернення: 09.11.2025).
4. Global Cybersecurity Outlook 2025 [Електронний ресурс]. URL: https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf (дата звернення: 09.11.2025).

Ключові слова: кібербезпека; цифрова трансформація; захист даних; технічні засоби захисту; алгоритмічні методи; людський фактор; бізнес-управління безпекою.
Keywords: cybersecurity; digital transformation; data protection; technical security measures; algorithmic methods; human factor; security management.

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

ШТУЧНИЙ ІНТЕЛЕКТ І ФІНАНСОВА СТАБІЛЬНІСТЬ: КЛЮЧОВІ ВИСНОВКИ КОМІТЕТУ З ФІНАНСОВОЇ ПОЛІТИКИ ВЕЛИКОЇ БРИТАНІЇ

Мовчан Анастасія
студентка 1 курсу факультету цивільної та господарської юстиції Національного університету «Одеська юридична академія»

Штучний інтелект (ШІ) стає одним із головних факторів, що змінюють фінансовий сектор. Він впливає на те, як працюють банки, страховики та інші фінансові установи, а також на те, які ризики виникають у всій фінансовій системі. У квітні 2025 року Комітет з фінансової політики Банку Англії опублікував спеціальну доповідь серії Financial Stability in Focus, у якій проаналізував, як саме ШІ може впливати на фінанси Великої Британії [1].

У документі зазначено, що ШІ — це не лише інструмент для підвищення ефективності. Він також може створювати нові ризики, тому за його впровадженням потрібно уважно стежити та вчасно реагувати на можливі загрози. Комітет підкреслює, що ШІ має властивості «технології широкого застосування», тобто може використовуватися майже скрізь — від обслуговування клієнтів до аналізу складних фінансових даних. Це здатне суттєво підвищити продуктивність завдяки автоматизації рутинних завдань, швидшому аналізу інформації та створенню персоналізованих фінансових сервісів.

Щоб оцінити реальний стан впровадження ШІ, Комітет проаналізував результати спільного опитування Банку Англії та Управління з фінансової поведінки, проведеного у 2024 році. Опитування показало, що 75 % фінансових установ уже використовують ШІ, а ще 10% планують

впровадження протягом трьох років. Найпоширеніші сфери застосування — оптимізація внутрішніх процесів, боротьба з фінансовим шахрайством і кіберзахист [2].

У доповіді ШІ розглядають з точки зору впливу на стійкість усієї фінансової системи. Простими словами, Комітет оцінює, чи допоможе ШІ фінансовому сектору краще витримувати економічні потрясіння, чи навпаки — зробить його вразливішим. Для цього визначено чотири основні напрями: використання ШІ у фінансових рішеннях банків і страховиків, його вплив на фінансові ринки, залежність від зовнішніх технологічних компаній та зміни у сфері кібербезпеки [3].

Перший напрям стосується того, як ШІ застосовують у таких ключових процесах, як кредитування, оцінка ризиків, визначення вартості фінансових продуктів. ШІ дозволяє банкам працювати з великими обсягами даних, точніше оцінювати позичальників і робити послуги доступнішими. Однак це створює і нові ризики. Наприклад, складні моделі можуть давати результати, які важко пояснити. Якщо багато установ використовують схожі моделі, помилка в одній з них може повторитися всюди, що здатне викликати широкі проблеми — так звані «системні дисбаланси», тобто збій у рівновазі всієї фінансової системи [4].

Другий напрям — вплив ШІ на фінансові ринки. Зокрема, це стосується алгоритмічної торгівлі, де рішення приймають комп’ютерні програми. Такі системи можуть робити ринок ефективнішим, швидше реагувати на інформацію. Але є й ризики. Якщо багато алгоритмів реагують однаково, це може призвести до «проциклічної поведінки» — коли учасники ринку масово діють в один бік. У періоди нестабільності це здатне збільшити «волатильність», тобто різкі коливання цін, що ускладнює торгівлю та може створити проблеми з ліквідністю. Також ШІ може виявляти нестандартні можливості для заробітку, які інколи можуть бути схожими на маніпуляції, тому регуляторам доведеться змінювати підхід до нагляду [5].

Третій напрям пов'язаний із тим, що багато фінансових установ використовують сторонні ШІ-сервіси, хмарні платформи та моделі. За опитуванням 2024 року, третина випадків використання ШІ залежить від таких постачальників. Проблема в тому, що кілька великих компаній контролюють більшу частину ринку. Це означає: якщо одна з них зіткнеться зі збоєм, значна частина фінансових установ може одночасно втратити доступ до важливих систем. Таку ситуацію вважають «системним операційним ризиком». Саме тому у Великій Британії вже розглядають ідею спеціального регулювання найбільших постачальників технологій.

Четвертий напрям — кібербезпека. Тут ефект двоякий. З одного боку, ШІ допомагає фінансовим установам краще виявляти загрози, швидше реагувати на них і виявляти шахрайство. З іншого боку, зловмисники також

використовують ШІ: автоматизують атаки, створюють реалістичні фішингові повідомлення, складні підробки аудіо й відео, шукають вразливості у системах [6]. Крім того, ШІ-системи самих фінансових компаній можуть стати слабким місцем, якщо не інтегровані у загальну систему кіберзахисту.

У доповіді також окреслено, як саме регулятори планують стежити за впровадженням ШІ. Вони використовуватимуть опитування, роботу спеціальних аналітичних груп, результати перевірок та інші джерела даних. У Великій Британії вже розробляють додаткові нормативні документи, що мають допомогти краще керувати ризиками ШІ. А на міжнародному рівні враховуються рекомендації Ради з фінансової стабільності, яка ще у 2017 році попереджала про можливі наслідки використання ШІ у фінансах.

Також у доповіді зазначено, що фінансова політика має бути гнучкою. Якщо роль ШІ і надалі зростатиме, можуть знадобитися нові інструменти: наприклад, додаткові перевірки моделей на стійкість до стресових ситуацій, контроль за залежністю від великих технологічних компаній, підсилення вимог до операційної стійкості та кіберзахисту.

Загалом FPC підкреслює, що ШІ приносить фінансовому сектору значні переваги: підвищення продуктивності, створення нових послуг, кращі можливості боротьби з шахрайством. Але одночасно наголошує, що ШІ може створити нові загрози, і тому потрібен продуманий підхід до регулювання. Це дозволить розвивати сучасні технології без ризику для стабільності всієї фінансової системи.

Список використаних джерел

1. Bank of England. Financial Stability in Focus: Artificial intelligence in the financial system. 09.04.2025. URL: https://www.bankofengland.co.uk/financial-stability-in-focus/2025/april-2025 (дата звернення: 06.11.2025).
2. Bank of England; Financial Conduct Authority. Artificial intelligence in UK financial services – 2024. 21.11.2024. URL: https://www.bankofengland.co.uk/report/2024/artificial-intelligence-in-uk-financial-services-2024 (дата звернення: 06.11.2025).
3. UK Financial Stability in Focus report: AI in the financial system. A&O Shearman FinReg Blog, 09.04.2025. URL: https://finreg.aoshearman.com/UK-Financial-Stability-in-Focus-report-AI-in-the-?utm_source (дата звернення: 06.11.2025).
4. Bank of England; Prudential Regulation Authority; Financial Conduct Authority. DP5/22 – Artificial Intelligence and Machine Learning. Discussion Paper 5/22, 11.10.2022. URL: https://www.bankofengland.co.uk/prudential-regulation/publication/2022/october/artificial-intelligence (дата звернення: 06.11.2025).
5. Financial Stability Board. Artificial intelligence and machine learning in financial services: Market developments and financial stability implications. 01.11.2017. URL: https://www.fsb.org/uploads/P011117.pdf (дата звернення: 06.11.2025).
6. Treacy S., Qemali E. Bank of England considers financial stability implications of AI. Linklaters Financial Regulation Blog, 29.04.2025. URL: https://financialregulation.linklaters.com/post/102k9ri/bank-of-england-considers-financial-stability-implications-of-ai (дата звернення: 06.11.2025).

Ключові слова: штучний інтелект; фінансова стабільність; Комітет з фінансової політики; системні ризики; регулювання фінансового сектору.
Keywords: artificial intelligence; financial stability; Financial Policy Committee; systemic risks; financial sector regulation.

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

AEVA 2018: РЕГУЛЯТОРНІ ЗАСАДИ ІНТЕГРАЦІЇ ШТУЧНОГО ІНТЕЛЕКТУ В ТРАНСПОРТНУ ІНФРАСТРУКТУРУ ВЕЛИКОЇ БРИТАНІЇ

Лозовій Вероніка
студентка 1 курсу факультету судового та міжнародного права Національного університету «Одеська юридична академія»

Automated and Electric Vehicles Act 2018 (AEVA) є ключовим нормативним актом Великої Британії, який створює правову рамку для функціонування автоматизованих транспортних засобів та розвитку інфраструктури електричного транспорту. Закон визначає механізми відповідальності, стандарти безпеки, вимоги до оновлення програмного забезпечення та принципи інтеграції електричних і автоматизованих транспортних засобів у національну транспортну систему, що робить AEVA одним із перших нормативних документів, який враховує зв'язок правового регулювання та сучасних інформаційних технологій [1].

Центральною частиною AEVA є врегулювання питань, пов'язаних із використанням автоматизованих транспортних засобів. Автономні автомобілі використовують комплекс цифрових технологій, включно з алгоритмами штучного інтелекту, сенсорними системами та телеметричними даними. Саме тому AEVA закладає правові механізми визначення відповідальності у разі ДТП або технічного збою систем самокерування [2].

Важливо, що закон вводить офіційний перелік автоматизованих транспортних засобів, які допускаються до руху у режимі самокерування. Це означає, що алгоритмічні системи штучного інтелекту проходять окрему верифікацію щодо відповідності вимогам безпеки.

Одним із найбільш прогресивних положень AEVA є спеціальна модель страхової відповідальності для автоматизованих транспортних засобів. Закон встановлює, що якщо автомобіль працював у режимі самокерування, то у разі дорожньо-транспортної пригоди відповідальність за відшкодування шкоди покладається не на водія, а на страхову компанію. Це означає, що потерпілі отримують компенсацію швидше і без необхідності доводити провину конкретної особи. Після виплати страховик отримує право регресу — тобто може звернутися з вимогою відшкодувати понесені витрати до виробника