

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

УДК 004.056

Відповідальний 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».

Редакційна колегія:

ГОРБАЧЕНКО Станіслав, д.е.н., професор

СОКОЛОВ Артем, д.т.н., професор

АХМАМЕТЬЄВА Ганна, к.т.н., доцент

РАЗІНКІН Нікіта, асистент кафедри

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 Acad-
emy».

Editorial Board:

GORBACHENKO Stanislav, Doctor of Economics, Professor

SOKOLOV Artem, Doctor of Engineering, Professor

AKHMAMETYEVA Anna, Candidate of Engineering, Associate Professor

RAZINKIN Nikita, Assistant

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

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)

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

автомобіля або розробника програмного забезпечення, якщо причина аварії пов'язана з помилкою алгоритмів, несправністю сенсорів, некоректною інтеграцією оновлень або іншими технічними дефектами системи самокерування. Такий підхід змінює традиційну модель дорожньої відповідальності, оскільки юридична увага переноситься з поведінки людини-водія на технічний стан цифрової системи та алгоритмічну надійність транспортного засобу. Він також стимулює виробників приділяти більше уваги якості програмного забезпечення, тестуванню автономних функцій і забезпеченню кіберстійкості, адже саме ці чинники прямо впливають на потенційні юридичні ризики та фінансові наслідки для компаній.

AEVA також регулює оновлення програмного забезпечення, що є критично важливим для безпеки автоматизованих транспортних засобів. Закон передбачає обов'язок користувача встановлювати оновлення, а невиконання цього може стати підставою для відмови у страхових виплатах [3].

Другий великий блок AEVA стосується розвитку інфраструктури електричного транспорту, що є необхідною умовою для масштабного впровадження електромобілів. Закон деталізує вимоги до створення розгалуженої мережі зарядних станцій, зокрема обов'язковість встановлення пунктів заряджання на автозаправних комплексах, уздовж основних автомагістралей та у ключових транспортних вузлах.

AEVA також передбачає стандартизацію платіжних інтерфейсів: користувачі повинні мати можливість заряджати автомобіль без укладання довгострокових контрактів із конкретними операторами, використовуючи універсальні способи оплати. Це спрямовано на усунення бар'єрів для водіїв та створення рівних умов доступу до інфраструктури.

Окрему увагу приділено впровадженню «розумних» (smart) зарядних пристроїв, які здатні автоматично регулювати інтенсивність заряджання залежно від стану електромережі, тарифів, часу доби або рівня навантаження.

Такі пристрої інтегруються у цифрові енергетичні системи та можуть працювати у режимах оптимізації споживання — наприклад, заряджати автомобіль у години найнижчого навантаження або реагувати на сигнали системи управління енергорозподілом. Це дозволяє зменшити пікове навантаження на мережу, підвищити ефективність використання енергії та створити передумови для розвитку концепції «розумних» електромереж, тісно пов'язаних з інформаційними технологіями та цифровими платформами управління. [4].

У контексті штучного інтелекту AEVA стимулює розвиток інтелектуальних транспортних систем, які працюють на основі машинного навчання, аналізу великих даних та високоточних навігаційних алгоритмів.

Закон формує юридичні умови для взаємодії між державою, виробниками, страховими компаніями та ІТ-індустрією.

AEVA також закладає принципи кібербезпеки транспортних систем, оскільки автономні авто стають потенційними об'єктами кібератак. Закон визначає обов'язковість захисту даних, стійкості до втручань та оновлення безпекових модулів у програмному забезпеченні.

Крім того, AEVA має стратегічне значення для розвитку концепції «розумних міст». Автономні та електричні транспортні засоби вимагають інтеграції у цифрову дорожню інфраструктуру, що включає системи моніторингу, аналізу та прогнозування дорожніх ситуацій.

Отже, Automated and Electric Vehicles Act 2018 є стратегічно важливим нормативним актом, що формує правову основу для розвитку транспортних технологій нового покоління. Закон поєднує регулювання автономного транспорту, інфраструктури заряджання електротранспорту, цифрової безпеки та інтелектуальної інфраструктури, створюючи передумови для безпечної й ефективної інтеграції систем штучного інтелекту в транспортну сферу та забезпечуючи стабільність, надійність і безпеку функціонування транспортних систем у цифрову еру.

Список використаних джерел

1. Automated and Electric Vehicles Act 2018.. URL: <https://www.legislation.gov.uk/ukpga/2018/18> (дата звернення: 06.11.2025).
2. The Automated and Electric Vehicles Act 2018: Briefing Paper CBP-8118. URL: <https://researchbriefings.files.parliament.uk/documents/CBP-8118/CBP-8118.pdf> (дата звернення: 06.11.2025).
3. Autonomous vehicles: legal and regulatory framework – United Kingdom. 2024. URL: <https://uk.practicallaw.thomsonreuters.com/w-013-2663> (дата звернення: 06.11.2025).
4. Automated and Electric Vehicles Act 2018 Regulatory Report: July 2023 – December 2024. 10 березня 2025. URL: <https://www.gov.uk/government/publications/automated-and-electric-vehicles-act-2018-regulatory-report-2024> (дата звернення: 06.11.2025).

Ключові слова: автономні транспортні засоби, електричний транспорт, штучний інтелект, інформаційні технології, правове регулювання.

Keywords: autonomous vehicles, electric transport, artificial intelligence, information technologies, legal regulation.

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

COMPETITION AND MARKETS AUTHORITY (CMA): УПРАВЛІННЯ КОНКУРЕНЦІЄЮ В ЕПОХУ ЦИФРОВИХ РИНКІВ.....	247
---	-----

Власюк Олександра

Секція 4. Нормативно-правові засади кібербезпеки та захисту інформації..... 251

НОРМАТИВНО-ПРАВОВІ ЗАСАДИ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ	251
---	-----

Задерейко Олександр

Іванов Володимир

АНАЛІЗ МЕТОДІВ ВИЛУЧЕННЯ КЛЮЧОВОЇ ІНФОРМАЦІЇ З ЮРИДИЧНИХ ТЕКСТІВ	255
--	-----

Гура Володимир

Курчук Роман

ЄВРОПЕЙСЬКИЙ ЗАГАЛЬНИЙ РЕГЛАМЕНТ ЗАХИСТУ ДАНИХ (GDPR): НАПРЯМИ ДІЇ, ВПЛИВ І ВИКЛИКИ.....	262
--	-----

Шевчук Марія

ЛІЦЕНЗУВАННЯ ТА УПРАВЛІННЯ ПРАВАМИ НА ЦИФРОВИЙ МУЛЬТИМЕДІЙНИЙ КОНТЕНТ: ІНТЕГРАЦІЯ ТЕХНІЧНИХ ЗАСОБІВ КОНТРОЛЮ У ПРАВОВІ ПРОЦЕДУРИ	265
--	-----

Овчинников Микола

СТРАТЕГІЧНІ ТА ТЕХНІЧНІ ЗАСАДИ КІБЕРБЕЗПЕКИ ПІДПРИЄМСТВА	268
--	-----

Костіна Олександра

ШТУЧНИЙ ІНТЕЛЕКТ І ФІНАНСОВА СТАБІЛЬНІСТЬ: КЛЮЧОВІ ВИСНОВКИ КОМІТЕТУ З ФІНАНСОВОЇ ПОЛІТИКИ ВЕЛИКОЇ БРИТАНІЇ.....	271
--	-----

Мовчан Анастасія

AEVA 2018: РЕГУЛЯТОРНІ ЗАСАДИ ІНТЕГРАЦІЇ ШТУЧНОГО ІНТЕЛЕКТУ В ТРАНСПОРТНУ ІНФРАСТРУКТУРУ ВЕЛИКОЇ БРИТАНІЇ	274
---	-----

Лозовій Вероніка

ПРАВОВІ ІНСТРУМЕНТИ ЄС У ЗАБЕЗПЕЧЕННІ БЕЗПЕКИ РИНКУ МОБІЛЬНИХ ДОДАТКІВ	277
--	-----

Волонтирець Анастасія