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)

Інтеграція технічних засобів контролю у процедури ліцензування перетворює ліцензію на керований життєвий цикл цифрового активу: реєстрація та ідентифікація (хеш/фінгерпринт, водяний знак) → договір → нотаризація подій → аудит. Це підвищує юридичну визначеність і скорочує час реагування на порушення. Для інформаційної системи критичні: машиночитні й версіоновані умови ліцензії, доказова цілісність журналів подій і прив'язка операцій до конкретної версії контенту, мінімізація даних і розмежування доступу (публічні хеші/таймстемпи та приватні деталі ліцензії). Технічні контролі підсилюють правові механізми, забезпечуючи їх виконуваність і відтворюваність у кіберпросторі.

Список використаної літератури:

1. Wang X. MPEG-21 Rights Expression Language: enabling interoperable DRM. IEEE MultiMedia. 2004. DOI: 10.1109/MMUL.2004.31.
2. Diehl E. A four-layer model for security of DRM (DRM '08). 2008. DOI: 10.1145/1456520.1456527.
3. Huang H., Fang W. Metadata-based image watermarking for copyright protection. Simulation Modelling Practice and Theory. 2010. DOI: 10.1016/j.simpat.2009.09.004.
4. Ferro E., Saltarella M., Rotondi D., et al. Digital assets rights management through smart legal contracts. Blockchain: Research and Applications. 2023. DOI: 10.1016/j.bcra.2023.100142.
5. Frattolillo A., Petitt J., Kalsi A., et al. Blockchain and smart contract for copyright management. Future Internet. 2024. DOI: 10.3390/fi16050169.
6. Feng X., Pan Y., Xiao N. Digital rights management: a review. Neurocomputing. 2025. DOI: 10.1016/j.neucom.2025.131672.

Ключові слова: ліцензування, цифрові права, DRM, цифровий водяний знак, смарт-контракти, доказовість, журнал подій, кібербезпека, захист інформації.
Keywords: licensing, digital rights, DRM, digital watermarking, smart contracts, evidentiary integrity, audit log, cybersecurity, information protection.

Науковий керівник: к.т.н., доцент Ахмаметьєва Г.В.

СТРАТЕГІЧНІ ТА ТЕХНІЧНІ ЗАСАДИ КІБЕРБЕЗПЕКИ ПІДПРИЄМСТВА

Костіна Олександра

студентка 1 курсу факультету прокуратури та слідства (кримінальної юстиції) Національного університету «Одеська юридична академія»

Кібербезпека набуває виняткового значення для будь-якої організації, незалежно від її сфери діяльності. Зі збільшенням кількості користувачів, розширенням мережевої інфраструктури, підключенням нових пристроїв та програмних рішень, а також зростанням обсягів інформації, що обробляються,

питання захисту даних стає одним із провідних аспектів забезпечення стабільної та безпечної роботи [1].

Особливо актуальним є захист конфіденційної інформації: персональних даних працівників, клієнтів, фінансової документації, комерційних таємниць і стратегічних рішень.

Сучасні кіберзагрози стають дедалі витонченішими. Зловмисники застосовують фішинг, соціальну інженерію, шкідливе програмне забезпечення та програми-вимагачі, атакують мережеву інфраструктуру й бази даних [2].

У результаті будь-яка організація, незалежно від розміру чи напрямку діяльності, може стати об'єктом кібератаки, що призводить до значних фінансових втрат, репутаційних ризиків або навіть до зупинки діяльності.

Тому питання кібербезпеки виходить за межі технічного виміру — воно стає стратегічним напрямом управління організацією. Важливо не лише впроваджувати сучасні технічні засоби захисту, а й формувати культуру інформаційної безпеки серед працівників, забезпечувати постійне навчання персоналу, моніторинг потенційних загроз і оперативне реагування на інциденти. Лише комплексний підхід до побудови системи кіберзахисту дозволить ефективно протистояти новим викликам цифрової ери та гарантувати стабільність функціонування організації в умовах зростаючих кіберризиків.

У законодавчому полі України, зокрема в Законі України «Про основні засади забезпечення кібербезпеки України», кібербезпека визначається як комплексна система захисту життєво важливих інтересів людини, суспільства та держави під час використання кіберпростору [3].

Це поняття охоплює не лише технічну безпеку інформаційних систем, а й забезпечення сталого розвитку інформаційного суспільства, створення безпечного цифрового середовища. Кібербезпека передбачає своєчасне виявлення, попередження і нейтралізацію як реальних, так і потенційних загроз, які можуть завдати шкоди національним інтересам України.

Основна мета забезпечення кібербезпеки — збереження цілісності, конфіденційності та доступності інформації, запобігання кібератакам, кіберзлочинам, несанкціонованому втручанню в роботу державних і приватних інформаційних систем. У межах державної політики кібербезпека стає складовою національної безпеки, оскільки розвиток цифрових технологій породжує нові ризики та виклики. Забезпечення належного рівня кіберзахисту сприяє підвищенню довіри громадян до державних інституцій, розвитку електронного урядування, зміцненню обороноздатності країни та захисту інформаційного суверенітету.

Алгоритмічні та технічні аспекти кібербезпеки охоплюють розробку, впровадження і вдосконалення технологічних засобів захисту інформації у цифровому середовищі. Зростаючі обсяги даних і кількість мережевих

взаємодій вимагають вдосконалених алгоритмічних підходів та технічних рішень, що формують основу ефективної системи кіберзахисту.

Алгоритмічні аспекти включають використання математичних методів, логічних структур і обчислювальних процесів для забезпечення цілісності, конфіденційності й доступності інформації. Це алгоритми шифрування (симетричного й асиметричного типу), цифровий підпис, хешування, автентифікація користувачів, а також методи виявлення вторгнень та аномалій у мережевому трафіку. Наприклад, алгоритми RSA, AES, SHA-256 або новітні квантово-стійкі методи криптографії є ключовими у захисті обміну інформацією. Завдяки розвитку штучного інтелекту й машинного навчання алгоритмічний компонент кібербезпеки постійно вдосконалюється, що дає змогу прогнозувати та запобігати загрозам ще до їх реалізації.

Технічні аспекти стосуються практичної реалізації алгоритмів і інструментів захисту в комп'ютерних системах і мережах. Сюди належать апаратне й програмне забезпечення, системи виявлення вторгнень (IDS/IPS), брандмауери, антивірусні програми, засоби шифрування трафіку, системи контролю доступу, резервного копіювання та відновлення даних. Також важливі технології багатофакторної автентифікації, VPN, хмарні системи захисту та централізовані системи управління безпекою (SIEM).

Взаємозв'язок алгоритмічних і технічних аспектів визначає ефективність кіберзахисту: навіть найпотужніший алгоритм шифрування не забезпечить належного рівня безпеки без правильної технічної реалізації та налаштування системи. Тому ключовим завданням фахівців є інтеграція теоретичних моделей захисту з практичними рішеннями, здатними оперативно реагувати на загрози.

У найближчі роки важливою тенденцією стане інтеграція кібербезпеки з технологіями штучного інтелекту, автоматизації захисту та аналітики кіберзагроз на базі великих даних. Організації, які впроваджуватимуть автоматизовані системи реагування на інциденти, симуляції атак і проактивний захист — отримають стратегічну перевагу [4].

Крім того, соціальний аспект кібербезпеки набуває зростаючого значення: формування цифрової культури безпеки серед працівників, регулярне навчання й підвищення кіберграмотності стають критичними елементами будь-якої програми захисту. Людський фактор залишається одним із найслабших місць у системі — у багатьох випадках 68 % інцидентів пов'язані з людською помилкою.

Список використаних джерел

1. 40+ Data Breach Statistics 2025: Trends & Key Threats [Електронний ресурс]. URL: https://deepstrike.io/blog/data-breach-statistics-2025 (дата звернення: 09.11.2025).

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