

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)

Секція 3. УПРАВЛІНСЬКІ, СОЦІАЛЬНІ ТА ПСИХОЛОГІЧНІ АСПЕКТИ КІБЕРБЕЗПЕКИ

ПЕРСПЕКТИВИ СТВОРЕННЯ КЛАСТЕРУ КІБЕРБЕЗПЕКИ В УКРАЇНІ

Горбаченко Станіслав

*завідувач кафедри кібербезпеки Національного університету
«Одеська юридична академія», доктор економічних наук, професор*

Саврацький Олександр

*аспірант кафедри кібербезпеки Національного університету
«Одеська юридична академія»*

Кібербезпека залишається одним із ключових пріоритетів національної безпеки України в умовах триваючої гібридної агресії російської федерації, яка супроводжується масованими кібератаками на критичну інфраструктуру, державні органи та приватний сектор. Згідно зі Стратегією кібербезпеки України, затвердженою Указом Президента № 447/2021 від 26 серпня 2021 року, розвиток безпечного кіберпростору передбачає посилення координації між державою, бізнесом, академічною спільнотою та міжнародними партнерами на принципах стримування, стійкості та взаємодії [1].

Національний кластер кібербезпеки (National Cybersecurity Cluster) був створений у 2021 році Національним координаційним центром кібербезпеки при РНБО України за підтримки Фонду цивільних досліджень та розвитку США (CRDF Global) та Державного департаменту США. Ця платформа об'єднує державні органи, приватні компанії, міжнародних партнерів (НАТО, ЄС, США) та експертну спільноту [2]. Станом на 2025 рік проведено понад 35 сесій кластера, включно з регіональними (Чернівці, Вінниця, Львів) та міжнародними заходами за участю Tallinn Mechanism.

Ринок кібербезпеки України демонструє стійке зростання: за оцінками DataDriven Research&Consulting, у 2024 році його обсяг сягнув 138 млн дол. США (у 4 рази більше, ніж у 2016-му), а прогноз на 2025–2029 роки — середньорічне зростання 8,54 % до приблизно 209 млн дол. США у 2029 році [3]. Війна стала потужним каталізатором розвитку вітчизняних продуктів та залучення грантів від USAID, ЄС і НАТО.

Розвиток кластерної моделі відкриває низку стратегічних перспектив. Інституційне посилення передбачає створення регіональних хабів та глибшу інтеграцію з центрами компетенцій НАТО (зокрема, Cooperative Cyber Defence Centre of Excellence у Таллінні). У 2025–2026 роках планується розширення співпраці з Румунією, Молдовою та країнами Західних Балкан [2].

Значну роль відіграватиме кадровий напрям: реформа підготовки фахівців, програми перепідготовки ветеранів (за підтримки США та Австралії), розвиток сертифікаційних центрів при Держспецзв'язку [4] та співпраця з Neoversity. Це дозволить частково закрити дефіцит спеціалістів, який на кінець 2025 року оцінюється у 25-30 тис. осіб.

Інноваційний та економічний потенціал кластера полягає у прискореній комерціалізації рішень на базі ШІ, захисту мереж, blockchain та постквантової криптографії. Завдяки координації через кластер Україна вже експортує окремі продукти до країн Азії та Європи, а до 2030 року сектор може стати одним із драйверів економічного відновлення [5].

Міжнародна інтеграція відкриває доступ до фінансування (програми USAID «Кібербезпека критичної інфраструктури України», гармонізація з директивою NIS2 ЄС) та обмін досвідом. Україна демонструє унікальну стійкість та попри зростання атак на 70% у 2024, ринок також розширюється. Дослідження DataDriven, ініційоване ЕВА та Асоціацією ІТ України, показує, що ринок кібербезпеки України досяг 138 мільйонів доларів, що в чотири рази більше, ніж у 2016 році. Прогнозується, що до 2029 року він зросте ще на 50% і перевищить 200 мільйонів доларів [6].

Попри виклики (недостатнє бюджетне фінансування — близько 0,15 % від видатків держбюджету проти 1-4 % у розвинених країнах, залежність від імпортного обладнання), кластерна модель вже довела свою ефективність і продовжує еволюціонувати в повноцінну національну екосистему кібербезпеки. Подальше розширення до спеціалізованих підкластерів (фінансовий сектор, енергетика, біокібербезпека) та посилення державно-приватного партнерства дозволить Україні не лише надійно захищатися, а й стати регіональним експортером кібертехнологій у Європі.

Список використаних джерел:

1. Указ Президента України № 447/2021 «Про рішення Ради національної безпеки і оборони України від 27 серпня 2021 року «Про Стратегію кібербезпеки України»». Офіційне інтернет-представництво президента України. URL: <https://www.president.gov.ua/documents/4472021-40013> (дата звернення: 18.11.2025).
2. Національний кластер кібербезпеки. Офіційний сайт. URL: <https://cybersecuritycluster.org.ua> (дата звернення: 18.11.2025).
3. Феценко Ю. Український ринок кібербезпеки оцінили в \$138 млн. Як він змінився та чого від нього чекати. MC.today. URL: <https://mc.today/uk/ukrayinskij-rinok-kiberbezpeki-otsinili-v-138-mln-yak-vin-zminivsia-ta-chogo-vid-nogo-chekati/> (дата звернення: 18.11.2025).
4. Держспецзв'язку та eGA запускають проєкт з підвищення кіберстійкості критичної інфраструктури. Державна служба спеціального зв'язку та захисту інформації України. URL: <https://cip.gov.ua/ua/news/ssscip-and-ega-to-enhance-cyber-resilience-of-ukrainian-critical-infrastructure> (дата звернення: 19.11.2025).

5. Ukraine's tech market: 2025 report. N-ix. URL: <https://src.n-ix.com/uploads/2025/02/25/d3f17988-8246-40ae-9703-3cd14f6163ad.pdf> (дата звернення: 19.11.2025).
6. Ukraine's Cybersecurity Market to Hit \$200M as Attacks Grow in Sophistication. IT Ukraine Association. URL: <https://itukraine.org.ua/en/ukraine-s-cybersecurity-market-to-hit-200m-as-attacks-grow-in-sophistication/> (дата звернення: 19.11.2025).

Ключові слова: кібербезпека, кластер кібербезпеки, кіберстійкість, кібератаки, критична інфраструктура.

Keywords: cybersecurity, cybersecurity cluster, cyber resilience, cyberattacks, critical infrastructure.

АНАЛІЗ МЕТОДІВ ВИЯВЛЕННЯ ТОКСИЧНОГО КОНТЕНТУ ПРИ СПІЛКУВАННІ УКРАЇНСЬКОЮ МОВОЮ

Гура Володимир

*доцент кафедри інформаційних технологій Національного університету
«Одеська юридична академія», кандидат технічних наук, доцент*

Касян Павло

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

Сучасний етап розвитку цифрових платформ висуває нові вимоги до модерації контенту в українських онлайн-спільнотах. За даними дослідження, опублікованого у 2025 році, 68% користувачів стикаються з токсичними повідомленнями щотижня, а 42% припиняють активність у спільнотах через психологічний тиск [1]. Найбільш гостро ця проблема проявляється у групових чатах месенджерів і соціальних мереж, де відсутність професійних модераторів поєднується з постійним збільшенням токсичного контенту. Саме ці фактори стали основним стимулом для розробки автоматизованої системи аналізу та виявлення прямих образ, сарказму, мікроагресії та групового тиску в реальному часі.

Аналіз методів виявлення токсичного контенту проведено на основі огляду наукових джерел за період 2023 – 2025 років. Аналіз охопив лексичні, семантичні, графові, контекстні та гібридні підходи, з акцентом на підтримку української мови у контексті виявлення прихованої агресії. Як встановлено у дослідженні, лише 12 % інструментів підтримують мови з низьким рівнем ресурсів, до яких належить українська, а 79% систем фокусуються виключно на прямих образах, ігноруючи імпліцитну агресію [2]. Більшість рішень не адаптовано до української мови і потребують значних обчислювальних ресурсів або зовнішніх сервісів. Крім того, приховані форми токсичності, такі як сарказм, невербальні маркери та контекст, залишаються поза увагою.

Секція 3. УПРАВЛІНСЬКІ, СОЦІАЛЬНІ ТА ПСИХОЛОГІЧНІ АСПЕКТИ КІБЕРБЕЗПЕКИ.....	211
ПЕРСПЕКТИВИ СТВОРЕННЯ КЛАСТЕРУ КІБЕРБЕЗПЕКИ В УКРАЇНІ	211
<i>Горбаченко Станіслав</i>	
<i>Саврацький Олександр</i>	
АНАЛІЗ МЕТОДІВ ВІЯВЛЕННЯ ТОКСИЧНОГО КОНТЕНТУ ПРИ СПІЛКУВАННІ УКРАЇНСЬКОЮ МОВОЮ	218
<i>Гура Володимир</i>	
<i>Касян Павло</i>	
ГЕНЕЗИС РОЗВИТКУ 3D-ТЕХНОЛОГІЙ У МОДЕЛЮВАННІ ТА АНІМАЦІЇ	221
<i>Задерейко Олександр</i>	
<i>Тимофєєв Михайло</i>	
ОСОБЛИВОСТІ ЗАХОДІВ КІБЕРБЕЗПЕКИ У РЕСТОРАННІЙ СФЕРІ.....	224
<i>Разінкін Нікіта</i>	
<i>Нгуен Фиок Бао Шон</i>	
СИСТЕМНИЙ АНАЛІЗ ТА ОПТИМІЗАЦІЯ ЕФЕКТИВНОСТІ ВЕБПОРТАЛУ НА ОСНОВІ ПОВЕДІНКИ КОРИСТУВАЧА.....	228
<i>Куклінова Софія</i>	
ANALYSIS AND MODELING OF THE PLAYER'S EMOTIONAL STATES IN ADAPTIVE GAME DESIGN SYSTEMS	230
<i>Chepurna Olena</i>	
<i>Shliakhtytskyi Dmytro</i>	
ДОСЛІДЖЕННЯ МЕТОДІВ АДАПТАЦІЇ ІНТЕРФЕЙСІВ ДЛЯ КОРИСТУВАЧІВ З КОГНІТИВНИМИ ПОРУШЕННЯМИ.....	2360
<i>Гура Володимир</i>	
<i>Вдовін Олександр</i>	
КОМУНІКАЦІЙНІ СТРАТЕГІЇ ПРОТИДІЇ РЕПОСТАМ І «ДЗЕРКАЛАМ» МУЛЬТИМЕДІЙНОГО КОНТЕНТУ: ВЗАЄМОДІЯ З ПЛАТФОРМАМИ ТА СПІЛЬНОТАМИ	239
<i>Овчинников Микола</i>	
ПЛАТФОРМЕНА ЕКОНОМІКА: МОЖЛИВОСТІ ТА ВИКЛИКИ.....	241
<i>Маріна Аліна</i>	
НМІ ЯК ЧИННИК ЦИФРОВОЇ ЕВОЛЮЦІЇ УПРАВЛІНСЬКИХ ПРАКТИК	245
<i>Кочубинська Юлія</i>	
ПОРІВНЯЛЬНИЙ АНАЛІЗ ПРОДУКТИВНОСТІ ДЕКЛАРАТИВНОГО ТА ІМПЕРАТИВНОГО ПІДХОДІВ ДО ПОБУДОВИ КОРИСТУВАЦЬКИХ ІНТЕРФЕЙСІВ МОБІЛЬНИХ ЗАСТОСУНКІВ.....	2475
<i>Земан Артур</i>	