

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)

ПРАВОВІ ІНСТРУМЕНТИ ЄС У ЗАБЕЗПЕЧЕННІ БЕЗПЕКИ РИНКУ МОБІЛЬНИХ ДОДАТКІВ

Волонтирець Анастасія

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

Швидке розширення цифрової економіки та стрімке зростання кількості мобільних користувачів у світі призвели до істотного збільшення випадків появи шахрайських мобільних додатків, що маскуються під легітимні продукти в App Store та Google Play. Такі програми використовуються для викрадення персональних даних, несанкціонованих списань коштів, фішингу або прихованого нав'язування платних послуг. З огляду на ці загрози Європейський Союз формує комплексну політику цифрового регулювання, спрямовану на підвищення прозорості та відповідальності цифрових платформ, зокрема в межах Digital Services Act (DSA) та Digital Markets Act (DMA) [1].

ЄС створює уніфіковану нормативну базу, яка покладає на великі онлайн-платформи, включно з магазинами мобільних додатків, чітко визначені обов'язки щодо оцінювання та мінімізації ризиків поширення незаконного або шкідливого контенту. DSA встановлює вимогу впроваджувати системи виявлення та протидії потенційно небезпечним додаткам ще на етапі попередньої перевірки, що вимагає від App Store і Google Play розроблення ефективніших алгоритмів модерації [2].

Важливим напрямом є підвищення прозорості діяльності платформ. Згідно з нормами DSA, оператори магазинів мобільних додатків повинні регулярно публікувати звіти щодо видалення або блокування програм, а також надавати доступ до базових технічних даних для незалежних дослідників і наглядових установ [3]. Це дозволяє оцінювати реальні результати боротьби з шахрайськими продуктами та створює підзвітність для технологічних компаній.

Протягом 2024–2025 років Європейська комісія активно застосовує наглядові механізми, надсилаючи запити Apple та Google з вимогою надати інформацію про політики модерації, статистику скарг і процедури реагування на порушення [4]. Такий підхід переходить від декларування відповідальності платформ до реального контролю за виконанням вимог законодавства.

DMA запроваджує додаткові правила для так званих «гейткіперів» — великих технологічних компаній, які контролюють критично важливі цифрові екосистеми. Для Apple та Google це означає обмеження можливості зловживання ринковою владою, забезпечення рівного доступу сторонніх розробників і формування прозорих умов перевірки додатків. DMA передбачає відкритість екосистем, можливість встановлення додатків із зовнішніх

джерел, а також зобов'язує компанії гарантувати захист прав користувачів у випадках виявлення шахрайства [2].

Окремим пріоритетом ЄС є створення превентивних механізмів, спрямованих на зменшення ризику поширення шкідливих додатків. До них належать удосконалені системи верифікації розробників, перевірки автентичності програм, аналіз платіжних інтеграцій і посилений контроль за використанням API та персональних даних. У межах DSA також передбачено механізм «trusted flaggers» — авторизованих організацій, які мають право оперативно повідомляти платформи про небезпечні програми, забезпечуючи швидший процес реагування.

Додаткові вимоги ЄС також стосуються прозорості алгоритмів, що застосовуються платформами для ранжування, модерації й рекомендацій додатків. Оскільки значна частина завантажень у магазинах мобільних застосунків формуються через рекомендаційні системи, Європейський Союз наголошує на важливості відкритості їх базових принципів. DSA передбачає обов'язок пояснювати користувачам логіку роботи таких алгоритмів та надавати можливість відмови від персоналізованого ранжування. Це спрямовано на запобігання маніпуляціям, завдяки яким шахрайські програми можуть підвищувати видимість за рахунок викривлення метаданих чи рекламних механізмів.

Крім того, вагомим елементом європейської стратегії є підвищення відповідальності розробників додатків. Нормативні вимоги ЄС передбачають не лише контроль за платформами, а й зобов'язання незалежних розробників підтверджувати свою ідентичність, дотримуватися стандартів безпеки та оперативно реагувати на повідомлення про зловживання. Такий комплексний підхід, що поєднує регулювання платформ та відповідальність розробників, формує більш стійку модель захисту цифрового ринку та сприяє зниженню кількості шкідливих додатків у європейському цифровому середовищі.

Законодавство встановлює і вагомі санкції. У разі серйозних або систематичних порушень DSA передбачає штрафи до 6 % від глобального річного обороту компанії [5]. Це створює реальний фінансовий стимул для дотримання вимог та підтримки безпечного цифрового середовища.

Проблематика шахрайських додатків має не лише юридичну, а й технічну складову. Сучасні шахраї застосовують штучний інтелект для обходу традиційних систем виявлення, що ускладнює модерацію та потребує постійного вдосконалення алгоритмічних інструментів. Тому ЄС підкреслює важливість координації між платформами, фінансовими установами, телекомунікаційними компаніями та правоохоронними органами з метою створення єдиної системи кіберзахисту.

Перспективи розвитку європейського регулювання передбачають поєднання наглядових заходів із формуванням культури етичного

саморегулювання платформ. ЄС прагне підтримувати баланс між безпекою користувачів і свободою підприємницької діяльності, одночасно забезпечуючи конкурентність цифрового ринку та високий рівень довіри до мобільних екосистем.

Отже, протидія шахрайським додаткам у магазинах App Store і Google Play є важливою складовою ширшої стратегії цифрової безпеки ЄС. Інтеграція вимог Digital Services Act і Digital Markets Act формує системний підхід до регулювання платформ, створює чіткі правила відповідальності, забезпечує прозорість і сприяє зміцненню Єдиного цифрового ринку.

Список використаних джерел

1. Digital Services Act: Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services. Official Journal of the European Union. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065> (дата звернення: 13.11.2025).
2. Digital Markets Act: Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector. Official Journal of the European Union. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R1925> (дата звернення: 13.11.2025).
3. European Commission. The Digital Services Act and Digital Markets Act: New Rules for Online Platforms. Brussels, 2023. URL: <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package> (дата звернення: 13.11.2025).
4. European Commission. Questions to Apple and Google on Fraudulent Apps. Press release, 2025. URL: https://ec.europa.eu/commission/presscorner/detail/en/ip_25_541 (дата звернення: 13.11.2025).
5. European Parliament. Fact Sheet: Enforcement and Penalties under the DSA. Brussels, 2023. URL: <https://www.europarl.europa.eu/factsheets/en/sheet/214/digital-services-act> (дата звернення: 13.11.2025).

Ключові слова: цифрове регулювання; Digital Services Act; Digital Markets Act; шахрайські додатки; мобільні платформи; кібербезпека; модерація контенту; європейське законодавство.

Keywords: digital regulation; Digital Services Act; Digital Markets Act; fraudulent apps; mobile platforms; cybersecurity; content moderation; EU legislation.

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