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».

Редакційна колегія:

ГОРБАЧЕНКО Станіслав, д.е.н., професор

СОКОЛОВ Артем, д.т.н., професор

АХМАМЕТЬЄВА Ганна, к.т.н., доцент

РАЗІНКІН Нікіта, асистент кафедри

© НУ «Одеська юридична академія», 2025

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».

Editorial Board:

GORBACHENKO Stanislav, Doctor of Economics, Professor

SOKOLOV Artem, Doctor of Engineering, Professor

AKHMAMETYEVA Anna, Candidate of Engineering, Associate Professor

RAZINKIN Nikita, Assistant

© National University "Odesa Law Academy", 2025

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)

ІНФОРМАЦІЙНА БЕЗПЕКА ДЕРЖАВИ У СОЦІАЛЬНИХ МЕРЕЖАХ: ВИКЛИКИ ТА ЗАГРОЗИ СУЧАСНОГО ЕТАПУ

Дикий Олег

декан факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія», кандидат юридичних наук, доцент

Проблематика забезпечення інформаційної безпеки держави у соціальних інтернет-сервісах у 2025 році набула критичного значення у зв'язку з повномасштабною збройною агресією російської федерації проти України та трансформацією гібридної війни в широкомасштабне вторгнення, де інформаційний простір виступає одним із ключових театрів бойових дій. Соціальні інтернет-сервіси, які ще донедавна розглядалися переважно як інструмент комунікації та соціальної взаємодії, фактично перетворилися на системоутворюючий елемент національного інформаційного середовища, здатний безпосередньо впливати на суспільну свідомість, поведінку громадян і стабільність державних інституцій.

У цьому контексті вважаю, що положення, викладені у статті Р. Грищука та К. Молодецької-Гринчук «Методологія побудови системи забезпечення інформаційної безпеки держави у соціальних інтернет-сервісах», зберігають не лише наукову, а й значну прикладну цінність. Запропонована авторами методологія комплексного моніторингу текстового контенту, виявлення та оцінювання організаційних, змістовних і маніпулятивних ознак загроз, а також аналіз профілів акторів соціальних мереж повністю відповідає сучасному характеру інформаційних операцій, що реалізуються проти України[1].

Після 2022 року соціальні мережі та месенджери стали основним каналом поширення дезінформації, маніпулятивних наративів і психологічного тиску на населення. У матеріалах українських та міжнародних засобів масової інформації неодноразово фіксувалися приклади координованих кампаній у Telegram, Facebook та X (Twitter), спрямованих на дискредитацію Збройних Сил України, підрив довіри до процесів мобілізації, формування панічних настроїв та спотворення інформації про міжнародну підтримку України. Такі кампанії, як правило, характеризуються використанням бот-мереж, псевдоекспертних коментарів, емоційно забарвленого контенту та прихованих семантичних конструкцій, що є механізмами інформаційно-психологічного впливу.

Варто звернути увагу, що соціальні інтернет-сервіси є складними соціотехнічними системами з нелінійною динамікою розвитку. В умовах війни

українське суспільство перебуває у стані підвищеної інформаційної напруги, коли навіть незначні інформаційні імпульси можуть призводити до різких соціальних коливань. Це підтверджує доцільність використання елементів теорії динамічного хаосу, біфуркацій і атракторів для аналізу поведінки віртуальних спільнот, що дозволяє адекватніше описувати процеси переходу від стабільного до нестійкого стану інформаційної безпеки.

Не менш актуальною є концепція синергетичного управління, запропонована у статті[1], яка передбачає використання природних механізмів самоорганізації акторів соціальних мереж для досягнення керованого переходу віртуальних спільнот до заданого стійкого стану інформаційної безпеки. Такий підхід корелює з положеннями, викладеними у працях В. Горбуліна, О. Додонова та Д. Ланде, де інформаційні операції розглядаються як системний інструмент впливу на безпеку суспільства та держави, а протидія їм потребує комплексних міждисциплінарних рішень[2].

У зв'язку з цим постає низка наукових питань, що потребують подальшого системного дослідження. Передусім це проблема своєчасного виявлення моментів переходу інформаційного середовища соціальних інтернет-сервісів у критичний або передкризовий стан, коли локальні інформаційні впливи здатні спричиняти масштабні соціальні ефекти. Недостатньо вивченими залишаються закономірності формування та еволюції деструктивних інформаційних наративів, механізми їх адаптації до змін зовнішнього контексту та способи інтеграції таких наративів у природні комунікаційні потоки віртуальних спільнот.

Окремої уваги потребує дослідження ролі автоматизованих та напівавтоматизованих акторів, зокрема бот-мереж і керованих акаунтів, у процесах штучного підсилення інформаційних коливань. Актуальним є також питання ідентифікації прихованих центрів управління інформаційними кампаніями, а також визначення критеріїв відмежування органічної громадської дискусії від скоординованого інформаційно-психологічного впливу. У цьому контексті важливим напрямом подальших досліджень є розроблення показників стійкості віртуальних спільнот до дезінформаційних впливів та методів оцінювання ефективності контрнаративів.

З методологічної точки зору доцільним видається використання міждисциплінарного підходу, що поєднує системний аналіз, методи теорії складних систем, соціальної інформатики та кібернетики. Перспективним є застосування математичного моделювання нелінійних процесів у соціальних інтернет-сервісах у поєднанні з емпіричним аналізом великих масивів даних, отриманих у результаті моніторингу відкритих джерел. Такий підхід дозволяє не лише фіксувати вже реалізовані інформаційні атаки, але й прогнозувати можливі сценарії розвитку інформаційних загроз.

Крім того, подальшого розвитку потребують методи синергетичного управління інформаційною безпекою, спрямовані на використання внутрішніх механізмів самоорганізації віртуальних спільнот. Йдеться про формування умов, за яких деструктивні інформаційні впливи втрачають здатність до масштабування, а система повертається до відносно стійкого стану без застосування надмірних адміністративних або репресивних заходів. У поєднанні з сучасними інструментами аналізу природної мови, мережевої аналітики та елементами штучного інтелекту така методологія може стати основою для побудови ефективних систем забезпечення інформаційної безпеки держави в умовах тривалої війни.

Список використаних джерел

1. Грищук Р., Молодецька-Гринчук К. Методологія побудови системи забезпечення інформаційної безпеки держави у соціальних інтернет-сервісах // Захист інформації. – 2017. – Т. 19, № 4 (жовтень–грудень). – С. 254–262. – DOI: 10.18372/2410-7840.19.12204.
2. Горбулін В. П., Додонов О. Г., Ланде Д. В. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання : монографія. – Київ : Інтертехнологія, 2009. – 164 с.

Ключові слова: інформаційна безпека держави, соціальні інтернет-сервіси, дезінформація, інформаційно-психологічний вплив.
Keywords: state information security, social internet services, disinformation, information and psychological influence.

A REVIEW ON MANY-VALUED LOGIC: A NOVEL PARADIGM FOR INFORMATION SECURITY

Aboobacker P
Govt.Engineering College, Palakkad, India
Department of Mathematics, Ph.D., Assistant Professor

1. Introduction. In the modern world, technology is changing at an astounding rate. We are more inventive, efficient, and connected than ever. Although this digital revolution has opened up a lot of possibilities, it has also increased risk and complexity. This scenario includes two phases: the incredible opportunity the digital world offers us and the significant challenges we must all overcome to realize that potential.

Modern advancement is built upon connectivity. Cybersecurity is not an obstacle to innovation; rather, it is a crucial enabler that permits us to safely seize new opportunities. The Internet has become the fastest-growing daily infrastructure. Many current technological advancements are transforming society. However, these new

ЗМІСТ