



МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ  
МАРИУПОЛЬСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

# **АКТУАЛЬНІ ПРОБЛЕМИ НАУКИ ТА ОСВІТИ**

**Збірник матеріалів**

**XXVI підсумкової науково-практичної  
конференції викладачів**

22 лютого 2024

Київ 2024

УДК 061.3(063)

АКТУАЛЬНІ ПРОБЛЕМИ НАУКИ ТА ОСВІТИ: Збірник матеріалів XXVI підсумкової науково-практичної конференції викладачів МДУ / За заг. ред. М.В. Трофименка. Київ: МДУ, 2024. 406 с.

Рекомендовано до друку та поширення через мережу Інтернет вченою радою Маріупольського державного університету (протокол № 11 від 22.04.2024)

**Редакційна колегія:**

*Голова* Трофименко М.В., ректор МДУ, кандидат політичних наук, професор;

*Члени редколегії* Балабаниць А.В., доктор економічних наук, професор;  
Безчотнікова С.В., доктор філологічних наук, професор;  
Булатова О.В., доктор економічних наук, професор;  
Задорожня-Княгницька Л.В., доктор педагогічних наук, професор;  
Іванець Т. М., голова Ради молодих вчених МДУ, кандидат політичних наук;  
Константинова Ю. В., кандидат історичних наук, доцент;  
Омельченко В.Я., доктор економічних наук, професор;  
Павленко О.Г., доктор філологічних наук, професор;  
Романцов В.М., доктор історичних наук, професор;  
Сабадаш Ю. С., доктор культурології, професор;  
Тарасенко Д. Л., доктор економічних наук, професор;  
Толпежніков Р.О., доктор економічних наук, професор.

Збірник містить матеріали XXVI підсумкової науково-практичної конференції викладачів МДУ, яка відбулася 22 лютого 2024 року в Маріупольському державному університеті.

У матеріалах висвітлені актуальні проблеми розвитку міжнародних відносин та зовнішньої політики, філософії та соціології, історії, економіки та менеджменту, права, екології, кібербезпеки, документознавства, культурології, журналістики, філології, літературознавства, методики викладання, педагогіки та психології.

Видання адресоване науковцям, викладачам, аспірантам та здобувачам вищої освіти, а також усім, хто цікавиться сучасними проблемами науки та освіти.

*Редакція не несе відповідальності за авторський стиль тез, опублікованих у збірнику.*

Омельченко Володимир,  
доктор економічних наук, професор кафедри менеджменту та фінансів  
Маріупольський державний університет

Омельченко Ганна,  
кандидат економічних наук, доцент,  
доцент кафедри економіки та міжнародних економічних відносин  
Маріупольський державний університет

## **РОЗВИТОК ІНФОРМАЦІЙНОЇ СКЛАДОВОЇ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВ В КОНТЕКСТІ ГІБРИДНОЇ ВІЙНИ**

У 2024 році виповнюється десять років з моменту різкого поглиблення конфронтації між Російською федерацією та Україною в соціально-політичній, економічній та військовій сферах, яка у 2022 році переросла в широкомасштабну агресію РФ проти нашої держави. В рамках воєнних дій, а також в соціально-політичному та інформаційному контексті широко застосовується інструментарій гібридної війни. При цьому гібридну війну треба розглядати як процес, спрямований на втілення зовнішнього контролю над об'єктом управління за допомогою інформаційних засобів в якості одного з пріоритетних механізмів. В контексті війни гібридні загрози застосовуються супротивниками як звичайне озброєння, терористичні засоби, злочинна поведінка в зоні бойових дій та інформаційному просторі для досягнення своїх політичних інтересів. Таким чином гібридність загроз може відноситися до воєнної ситуації, до стратегії та тактики противника, а також до типу сил і засобів, створених та розвинутих державою [2, с.330].

В сучасній війні гібридні дії противника характеризуються перш за все неоднозначністю типів та засобів застосування. Суб'єкти гібридних загроз не чітко підпорядковуються звичним форматам міжнародної політики, вони розвиваються у інформаційному просторі та виконують дії як з зовнішніми так і з внутрішніми державними і недержавними структурами, використовують законні і злочинні засоби досягнення результатів[3, с.22].

Сучасний стан системи безпеки бізнесу в Україні знаходиться під постійним впливом існування різних форм гібридних загроз. В умовах активної фази гібридної війни противник застосовує соціально-економічні, психологічні та інформаційно-диверсійні методи злочинної діяльності в середині країни, що не може не впливати на стан фінансово-економічної безпеки підприємств та галузей економіки, а також появу нових загроз (як характерний приклад:

хакерська атака РФ на інфраструктуру мережі «Київстар», що призвело до збоїв роботи системи провайдера мобільного зв'язку). Таким чином гібридні загрози реалізуються завдяки активному використанню передових технологій та розвинутої тактики їх застосування. При цьому, гібридні загрози мають перевагу над класичними у тому, що змінюють традиційні уявлення щодо практики війни, виграючи у системності та прихованості нанесеної шкоди.

В Україні під впливом гібридної війни опинились фактично усі сфери життєдіяльності, такі як, економіка, політика, культура, інформаційне забезпечення та споживання. Сильна прив'язаність до російського ринку деяких секторів промислового виробництва, відсутність альтернативних джерел постачання ресурсів для значної кількості галузей господарства підкреслює актуальність вирішення проблем національної безпеки.

Очевидно, що в таких умовах необхідно переосмислення підходів до створення та розвитку інформаційних систем та технологій, а питання безпеки повинні визначатися як складові елементи при формуванні інформаційних систем, починаючи з моменту їх проектування, виробництва і підтримки. Для досягнення позитивного результату роботи системи інформаційної безпеки дуже важливим є вирішення наступних фундаментальних завдань: забезпечити обмін інформацією в режимі реального часу, широке співробітництво в області кібербезпеки, використання інтегрованих технологічних платформ.

Темпи розвитку діджиталізації світового простору невпинно продовжують зростати, тому потрібно швидко реагувати на нові гібридні загрози та виявляти слабкі місця в системі інформаційної безпеки. Тому розробники інформаційних систем мають орієнтуватись на проектування та створення інтегрованих технологічних платформ, впровадження нових підходів до їх розроблення, що сформує безпечне функціонування інформаційних систем [1, с. 63].

При цьому важливим є визначення факторів, які формують розвиток потенціалу інформаційної безпеки підприємства під впливом гібридних загроз. Інформаційна безпека підприємства повинна являти собою гнучку систему з чітко визначеними елементами, яка обов'язково має змінюватися і адаптуватися до зовнішніх та внутрішніх умов і загроз ефективному функціонуванню підприємства.

Виходячи з цього, необхідно зробити висновок, що в умовах гібридної війни першочерговою значущістю набувають процеси вирішення проблеми насильницького розв'язання конфліктів, які характеризується інтенсивністю і широким застосуванням різноманітних методів прямої та непрямой агресії, можливістю використовувати велику кількість людей для їх реалізації, що негативно впливає на систему бізнес-процесів, державної стабільності та інформаційної безпеки країни.

## Література

1. Борсуковський Ю.В. Визначення вимог щодо побудови концепції інформаційної безпеки в умовах гібридних загроз. *Кібербезпека: освіта, наука, техніка*. 2019. № 1. С. 61-72. URL: [http://nbuv.gov.ua/UJRN/cest\\_2019\\_1\\_8](http://nbuv.gov.ua/UJRN/cest_2019_1_8)
2. Гришко С., Кодрул Р. Зміна безпекового ландшафту як передумова розвитку гібридних загроз: матеріали *Міжнародної науково практичної конференції «Управління та адміністрування в умовах протидії гібридним загрозам національній безпеці»*, м.Київ, 22 листоп. 2022 р. С.324-334.
3. The landscape of Hybrid Threats: A Conceptual Model (PublicVersion). Giannopoulos, G., Smith, H. and Theocharidou, M. (ed.). EUR 30585 EN, Publications Office of the European Union, Luxembourg, 2021. 58 p.