МІЖРЕГІОНАЛЬНА АКАДЕМІЯ УПРАВЛІННЯ ПЕРСОНАЛОМ

МАУП

**ISSN 3083-6557 print**

# НАУКОВІ ПРАЦІ МАУП

## Проблеми модернізації України

**Випуск 1 (48), 2025**

Київ
2025

УДК 330-339; 321.7; 159.9
М58

*Схвалено Вченою радою Міжрегіональної Академії управління персоналом (протокол № 4 від 28.05.2025)*

**Редакційна колегія:**
*С. В. Храпатий* (голова), д-р фіз.-мат. наук, проф.
*І. А. Семенець-Орлова,* д-р наук з держ. упр., проф.
*Я. М. Раєвська,* д-р психол. наук, проф.
*С. О. Лисенко*, д-р юрид. наук, проф.
*А. І. Федосов,* д-р мед. наук, проф.
*М. І. Зубрицький,* д-р. юрид. наук
*О. М. Гордієнко,* канд. техн. наук
*В. І. Меджебель* (*Чуєнко*), канд. юрид. наук
*Л. М. Крива*, канд. істор. наук
*І. М. Капеліста* (виконавчий редактор), канд. наук з держ. упр.
*Є. Я. Черняк*

*Матеріали подано в авторській редакції.*
*Відповідальність за зміст та орфографію матеріалів несуть автори.*

**Міжрегіональна Академія управління персоналом.**
М58 Наукові праці МАУП. Проблеми модернізації України / редкол.: С. В. Храпатий (голова) [та ін.]. Вип. 1 (48). Київ: Міжрегіональна Академія управління персоналом, 2025. 686 с. Бібліогр. в кінці ст.

У збірнику висвітлено матеріали X Міжнародної науково-практичної конференції "Розбудова інноваційних економіки, менеджменту та освіти в умовах нової соціальної реальності" (Київ, Міжрегіональна Академія управління персоналом, 20–22 травня 2025 р.).

Наведено тези доповідей учасників науково-практичної конференції МАУП з проблематики широкого кола аспектів процесу системної модернізації України.

Для науковців, громадсько-політичних діячів, студентів, а також усіх, хто цікавиться розвитком Української держави і світовим досвідом проведення модернізаційних процесів.

*Видається з 2001 року.*
*Періодичність: 1 раз на квартал.*
*Засновник*: *ПрАТ "ВНЗ "Міжрегіональна Академія управління персоналом".*
**УДК 330-339; 321.7; 159.9**

© Міжрегіональна Академія управління персоналом (МАУП), 2025

***О. В. Шуліма***
*Дистрибутивно-лагове моделювання взаємозв'язку між ВНП та валовим прибутком змішаного доходу* ..... 215

***В. В. Мельник***
*Спортивні заклади як простір фізичної та психологічної реабілітації ветеранів в умовах війни* ..... 217

***А. О. Артеменко***
*Публічно-приватне партнерство як відповідь на виклики соціальної нестабільності* ..... 220

***Д. С. Сахно***
*Концептуальні підходи до розробки інвестиційно-інноваційних стратегій розвитку залізничного транспорту України в умовах соціальних змін* ..... 223

***С. О. Щуренко, Ю. О. Фірсова***
*Організаційно-економічні засади розвитку систем електронного бізнесу в роздрібній торгівлі* ..... 226

***Л. Я. Шурак***
*Впровадження інновацій на підприємстві в умовах нестабільного ринкового середовища* ..... 229

***І. В. Ляшенко, Г. О. Кришталь***
*Управління результатами фінансової діяльності комерційного банку* ..... 231

***В. Ю. Колєчкін***
*Державне управління в інформаційній сфері для забезпечення сталого розвитку цифрового суспільства* ..... 233

***С. В. Мікулов***
*Вплив штучного інтелекту на прийняття інвестиційних рішень в умовах невизначеності* ..... 235

***Т. М. Іванова***
*Методологічні засади дослідження інтелектуально-інноваційного розвитку будівельних підприємств* ..... 237

***В. П. Кириченко***
*Захист інформаційної інфраструктури як складова стратегії інформаційної безпеки* ..... 238

***Т. В. Панова, Г. О. Кузьменко***
*Розвиток системи кібербезпеки в Україні в умовах зростаючих зовнішніх загрози* ..... 240

***Р. В. Довгалюк, Г. О. Кузьменко***
*Принципи управління інформаційною безпекою* ..... 241

***І. В. Малько, Г. О. Кузьменко***
*Історія формування поняття інформаційної безпеки* ..... 243

***А. В. Величко***
*Змішані моделі інвестування у реконструкцію зруйнованих війною споруд* ..... 244

ганням витоку конфіденційних даних і протидією кіберзагрозам. Досвід провідних країн свідчить, що ефективна система кібербезпеки має спиратися на комплексний підхід: поєднання правового регулювання, сучасних технічних засобів, підвищення інформаційної грамотності населення та активну міжнародну співпрацю.

Україна також прагне посилити свою систему кіберзахисту. Зокрема, пропонується створити Національний центр кібербезпеки під егідою Служби безпеки України, який стане координаційною ланкою для різних державних структур. Також одним із перспективних напрямів є розвиток національних технологічних рішень, що дозволить знизити залежність від іноземного програмного забезпечення та обладнання.

Формування ефективної системи інформаційної безпеки передбачає налагоджену взаємодію між органами влади, силовими структурами, бізнесом та громадським сектором. Надзвичайно важливим є забезпечення координації між усіма учасниками цієї сфери, що сприятиме швидкому реагуванню на новітні загрози та зменшенню їх впливу.

У нових реаліях інформаційного протистояння Україна повинна адаптуватися до змін, впроваджувати нові стратегії, розвивати IT-інфраструктуру, підтримувати дослідження у сфері інформаційної безпеки та готувати кваліфікованих фахівців. Важливим завданням є створення національної системи кіберзахисту, яка поєднує технічні рішення із законодавчими ініціативами для ефективного захисту даних [2].

Інтеграція у глобальну систему інформаційної безпеки зміцнить позиції України у світі, відкриє доступ до передових технологій та сприятиме підвищенню рівня кіберзахисту. Співробітництво з країнами НАТО та ЄС відіграє в цьому процесі важливу роль, адже міжнародна підтримка дозволить ефективніше протистояти загрозам у цифровому просторі.

**Джерела**


1. *Криволап Є., Юринець Ю.* Взаємозв'язок стратегій безпеки України з інформаційною та кібербезпекою. *Актуальні проблеми сучасної науки*. 2023. № 8(14). URL: https://doi.org/10.52058/2786-6300-2023-8(14)- 477-487
2. *Лазарєв В.* Концептуальні основи державного управління інформаційною безпекою електронних послуг: теорія та проблеми. *Наукові перспективи*. 2023. № 6(36). URL: https://doi.org/10.52058/2708- 7530-2023-6(36)-143-150



***Р. В. ДОВГАЛЮК***

*здобувач першого (бакалаврського) рівня освіти*
*Навчально-наукового інституту управління, економіки та бізнесу МАУП*

***Г. О. КУЗЬМЕНКО***

*PhD, доцент, доцент кафедри публічного адміністрування*
*Навчально-наукового інституту управління, економіки та бізнесу МАУП*


## ПРИНЦИПИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

Аналіз засад, на яких базується інформаційна безпека, свідчить, що українське законодавство вже містить основні теоретичні положення, необхідні для створення

цілісної системи управління у цій сфері. Проте стрімкий розвиток цифрових технологій і поява нових загроз зумовлюють потребу не лише в уточненні вже існуючих принципів, а й у розробці нових підходів, які зможуть ефективно реагувати на виклики сучасного інформаційного середовища.

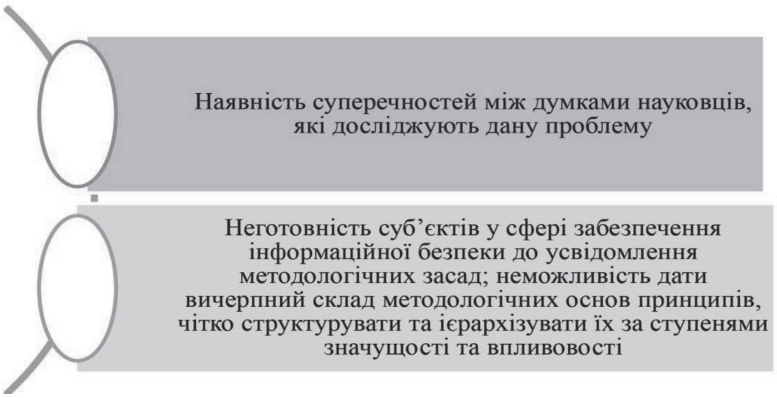
Забезпечення безпеки інформації є складним процесом, що охоплює кілька рівнів і вимагає комплексного підходу. Успішна реалізація цієї мети передбачає інтеграцію правових, технічних, організаційних та економічних механізмів. В умовах глобалізації, посилення кіберзагроз, поширення дезінформації, витоків персональних даних та атак на об'єкти критичної інфраструктури, вдосконалення принципів управління інформаційною безпекою набуває особливої актуальності [1].

Одним з ключових завдань є розробка чіткої методології, яка забезпечуватиме ефективність державної політики у сфері інформаційного захисту. Серед основних напрямків виділяються наступні:

- **Актуалізація законодавства** у відповідності до міжнародних норм та стандартів, зокрема гармонізація українського права з європейськими та світовими вимогами в галузі кібербезпеки.
- **Формування загальнодержавної стратегії управління** інформаційною безпекою, яка охоплюватиме юридичні, організаційні, технічні та соціальні аспекти.
- **Впровадження інноваційних методів** захисту, серед яких — використання сучасних криптографічних засобів, технологій штучного інтелекту для ідентифікації загроз, а також розвиток навичок кібергігієни серед користувачів.
- **Посилення співпраці** між органами державної влади, бізнесом і громадянським суспільством у питаннях захисту інформації.

Сучасні загрози інформаційній безпеці вже не обмежуються виключно кіберзлочинністю. Значну небезпеку становлять також інформаційно-психологічні операції, маніпуляції громадською свідомістю через цифрові канали, а також зовнішній вплив на політичні й економічні процеси, зокрема під час виборів або через інформаційні атаки на фінансові інститути. Це вимагає розширення підходів до побудови системи інформаційної безпеки, включно з удосконаленням механізмів виявлення, запобігання та нейтралізації таких загроз.

Особливої уваги заслуговує підготовка висококваліфікованих кадрів у сфері інформаційної безпеки. Не менш важливими є міждисциплінарні дослідження, які поєднують технічні, правові, соціальні та психологічні аспекти захисту інформаційного середовища.




**Основні причини проблеми визначення методологічних засад управління інформаційною безпекою**

З огляду на вищезазначене, можна зробити висновок, що складність визначення чітких методологічних засад управління інформаційною безпекою вимагає глибокого аналізу та формування сучасної концепції. Така концепція має враховувати не лише існуючі загрози, але й технологічні перспективи, включаючи розвиток цифрових систем та космічних технологій [2].

Встановлення чіткої системи принципів управління інформаційною безпекою сприятиме підвищенню ефективності її інтеграції у соціально-економічний контекст країни. На основі таких принципів можна сформувати цілісну, системну модель інформаційної безпеки, що забезпечить її стійкість і результативність.

**Джерела**


1. *Наконечний В. К.* Стан розвитку управління інформаційною безпекою у світовій практиці та його вплив на економічний розвиток України. *Сучасний захист інформації*. 2015. № 4. С. 10–15.
2. *Терещенко О.* Правові аспекти забезпечення національної безпеки в Україні. *Міжнародна та національна безпека*: *теоретичні та прикладні аспекти*. 2023. URL: https://doi.org/10.31733/17-03-2023-98-99



***І. В. МАЛЬКО***

*здобувач першого (бакалаврського) рівня освіти*
*Навчально-наукового інституту управління, економіки та бізнесу МАУП*

***Г. О. КУЗЬМЕНКО***

*PhD, доцент, доцент кафедри публічного адміністрування*
*Навчально-наукового інституту управління, економіки та бізнесу МАУП*


## ІСТОРІЯ ФОРМУВАННЯ ПОНЯТТЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Інформаційний простір охоплює певний обсяг, що визначається кількістю доступних у конкретний момент часу матеріальних та нематеріальних об'єктів. На відміну від кіберпростору, який обмежується фізичними межами планети, інформаційний простір є практично безмежним завдяки наявності нематеріальних елементів.

Цей простір складається як з матеріальних компонентів — технічного обладнання, засобів комунікації, телекомунікаційної інфраструктури, програмних кодів і алгоритмів, — так і з нематеріальних — самої інформації, а також процесів її сприйняття, зберігання, передачі та аналізу. У даному випадку матеріальність не слід розуміти у філософському сенсі, а радше як усе, що здатне бути сприйняте через органи чуття [1].

Отже, інформаційний простір — це середовище, створене людиною з метою задоволення її інформаційних потреб, без урахування можливих негативних наслідків, які можуть виникати внаслідок його розвитку.

З урахуванням вищевикладеного, можна зробити наступні узагальнення:

- Об'єкти інформаційного простору — це не лише матеріальні чи нематеріальні системи, а й живі організми, організації та спільноти, здатні до сприйняття,