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

Т. В. ПАНОВА
здобувачка другого (магістерського) 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

РОЗВИТОК СИСТЕМИ КІБЕРБЕЗПЕКИ В УКРАЇНІ В УМОВАХ ЗРОСТАЮЧИХ ЗОВНІШНІХ ЗАГРОЗ

У відповідь на зростання зовнішніх загроз у кіберпросторі, Україна інтенсивно розвиває власну систему кібербезпеки. Захист цифрового середовища країни забезпечують кілька ключових державних інституцій, серед яких Служба безпеки України, Державна служба спеціального зв'язку та Міністерство внутрішніх справ. Одним із важливих рішень стало створення при РНБО Національного координаційного центру з кібербезпеки. Центр відповідає за спостереження за ситуацією в інформаційному полі, виявлення кіберзагроз та координацію дій щодо їхньої нейтралізації.

Законодавча база, яка регламентує сферу інформаційної безпеки в Україні, визначає основні засади державної політики у цій галузі. Зокрема, у 2016 році була прийнята Доктрина інформаційної безпеки, що встановлює принципи захисту державної інформації, механізми реагування на інформаційні загрози та пріоритети у захисті національних інтересів у кіберсфері.

Кіберзагрози, зокрема атаки на критичну інфраструктуру, дедалі частіше використовуються як інструмент у сучасній гібридній війні. Україна, як і інші держави, стикається з такими викликами, як кібершпигунство, поширення шкідливого програмного забезпечення та крадіжка конфіденційної інформації. У цьому контексті побудова ефективної національної системи кіберзахисту є одним з пріоритетних напрямків. Надійний захист інформаційних систем критично важливий для безперебійного функціонування державного управління, банківської системи та інших ключових секторів.

Україна активно запозичує міжнародний досвід у сфері кібербезпеки. Наприклад, у Канаді стратегія кіберзахисту акцентує увагу на загрозах у вигляді кібершпигунства, терористичних атак у цифровому середовищі та посягань на інфраструктуру. У країні діє централізована система кібербезпеки, яка координує зусилля як державних, так і приватних структур [1].

В Австрії реалізацію заходів у сфері кібербезпеки забезпечує Центр боротьби з кіберзлочинністю при Міністерстві внутрішніх справ. Цей орган відповідає за оперативне реагування на загрози та розробку інструментів для боротьби з кіберзлочинами. Подібна структура функціонує й у Польщі, де Агентство внутрішньої безпеки відіграє провідну роль у сфері кіберзахисту. Крім того, у Польщі функціонує Центр криптології при Міністерстві оборони, відповідальний за захист державної інформації та проведення наступальних кібероперацій.

У багатьох країнах світу функціонують спеціалізовані кіберцентри та підрозділи контррозвідки, які займаються захистом інформаційної інфраструктури, запобі-

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