



Міністерство освіти і науки України
Мукачівський державний університет
Державний університет інтелектуальних технологій і зв'язку
Черкаський національний університет імені Богдана Хмельницького
Люблінська школа бізнесу (Словенія)
Краківський економічний університет (Польща)

VII Міжнародна науково-практична конференція

**“УПРАВЛІННЯ СОЦІАЛЬНО-ЕКОНОМІЧНИМИ
ТРАНСФОРМАЦІЯМИ ГОСПОДАРСЬКИХ ПРОЦЕСІВ:
РЕАЛІЇ І ВИКЛИКИ”**



11 квітня 2025 р.

Міністерство освіти і науки України
Мукачівський державний університет
Державний університет інтелектуальних технологій і зв'язку (м. Одеса)
Черкаський національний університет імені Богдана Хмельницького
Люблінська школа бізнесу (Словенія)
Краківський економічний університет (Польща)

**УПРАВЛІННЯ СОЦІАЛЬНО-ЕКОНОМІЧНИМИ
ТРАНСФОРМАЦІЯМИ ГОСПОДАРСЬКИХ ПРОЦЕСІВ:
РЕАЛІЇ І ВИКЛИКИ**

**MANAGEMENT OF SOCIO-ECONOMIC
TRANSFORMATIONS OF BUSINESS PROCESSES:
REALITIES AND CHALLENGES**

Тези доповідей
VII Міжнародної науково-практичної конференції

11 квітня 2025 р.

Мукачево
2025

невизначеності та воєнного стану	
РОСОЛА У., ЯКУБИШИН Є. Оптимізація ресурсного забезпечення технологічних процесів у виробничому секторі України	81
СИНЕВИЧ І., ГОЛОВАЧКО В. Управління кібербезпекою критичної інфраструктури держави	83
СИРОВЕЦЬ С. Модернізація господарського комплексу України на засадах інноваційного розвитку	85
СТАНІСЛАВИК О. Електронна комерція як інструмент зміцнення міжнародної співпраці	88
СТЕГНЕЙ М., МИХАЛЬЧИНЕЦЬ Г., ГАВРИЛЮК Р. Сучасні тенденції просторової організації економічних систем	91
ТОВКАНЕЦЬ Г. Перспективи розвитку європейської вищої освіти в контексті сталого розвитку	93
ТОВКАНЕЦЬ О. Особливості розвитку світової освітньої системи	95
ФЕНЦИК О., МОЛНАР-ЧАТЛОШ А. Вплив моніторингу як інструмента забезпечення якості професійної підготовки майбутніх учителів початкових класів	97

СЕКЦІЯ 3. ЦИФРОВА ЕКОНОМІКА У ВИМІРАХ ГЛОБАЛІЗАЦІЇ ТА МІЖНАРОДНОГО СПІВРОБІТНИЦТВА

ГАЛАН Л., БОРИСЕВИЧ Є. Роль інформаційного менеджменту в умовах цифрової економіки	100
ЖУКОВ І. Короткочасний контент як новий підхід в управлінні підприємницькою діяльністю в умовах цифровізації економіки	103
ІРТИЩЕВА І., ОКСИМЧУК С., РОМАНЮК С. Особливості життєзабезпечення в умовах розвитку цифрової економіки	105
КОЗИК І., КОЗИК В. Основні аспекти трансформаційних перетворень розвитку цифрової економіки	106
КОЧУМА І. Використання AR/VR-технологій як фактор збереження та популяризації культурної спадщини туристичних територій	108
КОШЕЛЯ Д. Моделі змінності ІТ-бізнесу у статусі фізичних осіб-підприємців	110
ЛУЖАНСЬКА Т., ЛЕТА В., НАКОНЕЧНИЙ Ю. Цифрова трансформація економіки України	112
МАКСИМЕНКО Д., ТОКАР І. Цифровізація як фактор підвищення стійкості та конкурентоспроможності агросектору України	115
МАСАЛОВИЧ С., ГОЛОВАЧКО В. Міжнародні стандарти та протоколи в цифровій економіці: питання гармонізації	118
ПАПП В.В., БОШОТА Н., ХИМИЧ В. Роль цифрових технологій у розвитку туризму та рекреації в Україні	120
ПОПОВИЧ О., СВИТЛИК С. Цифрові платформи як каталізатори змін у сфері фінансування проєктів	122
РУСИН Я., ГОЛОВАЧКО В. Оподаткування цифрових послуг в умовах міжнародної економічної інтеграції	123
СТЕГНЕЙ М., ГРИНЧАК І., МЕЙСАР Б., БАТИН М. Особливості розвитку транспортно-логістичної сфери в умовах цифровізації	126
СТЕГНЕЙ М., НОДЬ О., БЕРГХАУЕР О. Особливості розвитку сфери готельно-ресторанного обслуговування в умовах цифровізації та євроінтеграції	128
СТЕГНЕЙ М., РИЖКОВ К. Особливості територіального розвитку в умовах цифровізації	131
ТАРДАСКІНА Т., ЧУКУРНА О. Бізнес-модель для ІТ-продукту у сфері ментального здоров'я	133
ХАДЖИРАДЄВА С., ЧУКУРНА О. Дослідження поведінових реакцій та мотивів виникнення кіберхейту	136
ЧИЗМАР І. Вплив цифрових технологій на зміну традиційних бізнес-моделей	138

СЕКЦІЯ 4. ІННОВАЦІЇ ТА ІНВЕСТИЦІЇ В УПРАВЛІННІ ПРОЦЕСАМИ ЗБЕРЕЖЕННЯ СТІЙКОСТІ ТЕРИТОРІЙ ТА ГРОМАД

ГОБЛИК-МАРКОВИЧ Н., ХИМИНЕЦЬ Д. Інноваційне управління в умовах мінливості	141
--	-----

УДК: 004.056:351.824

ІВАН СИНЕВИЧ

здобувач вищої освіти ОС «Бакалавр»,
спеціальність «Професійна освіта. Економіка»,
Мукачівський державний університет, м. Мукачево, Україна

ВАСИЛЬ ГОЛОВАЧКО

кандидат економічних наук,
доцент кафедри обліку і оподаткування та маркетингу,
Мукачівський державний університет, м. Мукачево, Україна

УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ДЕРЖАВИ

Динамічна цифровізація суспільства, зростання ролі інформаційних технологій у всіх сферах державного управління та економіки зумовлюють нові виклики для національної безпеки. Особливої уваги набуває питання забезпечення кібербезпеки критичної інфраструктури держави, оскільки сучасні технологічні рішення, з одного боку, підвищують ефективність функціонування ключових галузей, а з іншого – створюють нові вразливості для кіберзагроз. Атаки на енергетику, транспорт, фінансову систему, медицину чи зв'язок можуть мати катастрофічні наслідки для суспільства, економіки й навіть політичної стабільності. Саме тому управління кібербезпекою критичної інфраструктури є однією з пріоритетних задач сучасної державної політики, що знаходить відображення у численних наукових дослідженнях українських фахівців.

Критична інфраструктура (КІ) – це сукупність об'єктів, мереж, систем і сервісів, безперервна робота яких є необхідною для функціонування держави, економічної стабільності, безпеки громадян та підтримки базових суспільних процесів. До таких об'єктів в Україні належать енергетика, водопостачання, транспорт, сфера зв'язку, фінансові системи, медицина, інформаційні ресурси органів влади тощо. Від їх захищеності залежить життєздатність держави у кризових ситуаціях, а також здатність протистояти зовнішнім і внутрішнім загрозам.

Як зазначає О.В. Гусев [1], особливість кібербезпеки КІ полягає в тому, що більшість сучасних об'єктів інтегровані у єдині цифрові мережі та активно використовують автоматизовані системи управління, від яких залежить не лише ефективність, а й безпечність їх роботи.

З-поміж найпоширеніших кіберзагроз для КІ можна виділити:

1. Несанкціонований доступ до інформаційних систем – здобуття контролю над АСУ ТП, зміна налаштувань, викрадення чи модифікація даних.
2. DDoS-атаки – масові атаки на сервери, які виводять з ладу критичні сервіси.
3. Вірусні та шкідливі програми – спеціалізоване ПЗ, що проникає у внутрішні мережі та руйнує, блокує або викрадає інформацію.
4. Кібершпигунство – цілеспрямоване проникнення з метою збору розвідувальних даних про критичні об'єкти.
5. Гібридні атаки – поєднання кібер- і фізичних загроз для комплексного виведення з ладу важливих систем.

В.М. Шеховцов [4] підкреслює, що зростає ризик використання кіберзброї державами-агресорами чи організованими злочинними групами. Приклади таких атак на критичну інфраструктуру України стали особливо помітними після 2014 року, коли кіберзлочинці здійснили атаки на енергетичні компанії, банки, урядові органи та об'єкти транспорту.

В Україні питання забезпечення кібербезпеки критичної інфраструктури регламентуються Законом «Про основні засади забезпечення кібербезпеки України»,

іншими нормативно-правовими актами, а також Стратегією кібербезпеки України. Центральними органами у цій сфері є:

- Національний координаційний центр кібербезпеки при РНБО України, який виконує стратегічну координацію дій.
- Державна служба спеціального зв'язку та захисту інформації (Держспецзв'язку) – організація технічних заходів, аудиту та моніторингу безпеки.
- Служба безпеки України – протидія кібершпигунству та кібертероризму.
- Міністерство цифрової трансформації України – розробка політик, просування цифрової грамотності, стандартизація.

Згідно з Н.М. Пархоменко, одним із важливих напрямів є ідентифікація об'єктів КІ, категоризація їх за ступенем критичності, проведення регулярної оцінки ризиків, а також впровадження стандартів захисту (наприклад, ISO/IEC 27001, NIST).

Ефективне управління кібербезпекою передбачає реалізацію таких практичних заходів:

1. Моніторинг і виявлення кіберінцидентів – застосування засобів SIEM, IDS/IPS, регулярний аудит журналів подій.
2. Розробка і впровадження політик інформаційної безпеки – стандартизація процедур доступу, резервного копіювання, оновлення ПЗ.
3. Підготовка і навчання персоналу – постійне підвищення кваліфікації, проведення симуляційних навчань з реагування на інциденти.
4. Планування реагування на надзвичайні ситуації – створення чітких планів відновлення роботи систем, тестування процедур резервування.
5. Розвиток державно-приватного партнерства – залучення приватних компаній до створення інноваційних рішень, обмін досвідом та інформацією про загрози.

Як зазначають І.В. Куліш та О.Є. Марущак [2], у сучасних умовах особливої ваги набуває впровадження систем управління інформаційною безпекою (ISMS), орієнтованих на постійну адаптацію до нових технологічних і організаційних ризиків.

Глобальний характер кіберзагроз зумовлює необхідність міжнародної координації зусиль. Україна є членом Глобального форуму з кібербезпеки, співпрацює з НАТО, ЄС, США та іншими країнами щодо обміну інформацією про інциденти, впровадження стандартів і процедури реагування. За даними Пархоменко Н.М. [3], рівень міжнародної інтеграції є критично важливим для отримання сучасних технологій захисту, підвищення стійкості до нових типів атак, участі у спільних навчаннях та розробці законодавчих ініціатив.

Попри наявність значних досягнень, залишаються актуальними такі проблеми:

1. Недостатнє фінансування кібербезпеки, особливо для державних і комунальних підприємств.
2. Дефіцит кваліфікованих кадрів та відтік фахівців у приватний сектор або за кордон.
3. Фрагментарність нормативної бази, відсутність єдиних стандартів для різних галузей КІ.
4. Недостатній рівень обізнаності персоналу щодо сучасних кіберзагроз.

Пархоменко Н.М. наголошує на необхідності розробки комплексної системи підготовки кадрів, створення центрів реагування на інциденти (CERT), впровадження системи постійного аудиту та моніторингу безпеки, розвитку

Отже, управління кібербезпекою критичної інфраструктури держави є складним і багаторівневим процесом, що вимагає постійної адаптації до нових загроз, удосконалення нормативного поля та впровадження сучасних технологій захисту. Досвід українських науковців свідчить про необхідність комплексного підходу, розвитку кадрового потенціалу, посилення міжнародної співпраці й формування культури кібербезпеки на всіх рівнях. Лише системна та скоординована діяльність державних і приватних структур

дозволить забезпечити надійний захист критичних об'єктів та стійкість держави до кіберзагроз.

Список використаних джерел

1. Гусєв О.В. Кібербезпека критичної інфраструктури: концептуальні засади та державне управління // *Вісник НАДУ*. – 2022. – №3. – С. 33–41.
2. Куліш І.В., Марущак О.Є. Проблеми та перспективи забезпечення кібербезпеки критичної інфраструктури України // *Державне управління: теорія та практика*. – 2023. – №1. – С. 95–102.
3. Пархоменко Н.М. Державна політика забезпечення кібербезпеки України: сучасний стан та перспективи розвитку // *Економіка і держава*. – 2022. – №12. – С. 47–52.
4. Шеховцов В.М. Захист критичної інфраструктури в умовах гібридних загроз // *Інформаційна безпека*. – 2023. – №2. – С. 11–19.

УДК 911.3:30/33 (477.8)

СЕРГІЙ СИРОВЕЦЬ

кандидат географічних наук, доцент
доцент кафедри країнознавства та туризму
Київський національний університет ім. Т.Г. Шевченка, м. Київ, Україна

**МОДЕРНІЗАЦІЯ ГОСПОДАРСЬКОГО КОМПЛЕКСУ УКРАЇНИ НА ЗАСАДАХ
ІННОВАЦІЙНОГО РОЗВИТКУ**

Відсутність системних структурних реформ в Україні, посилення тенденцій структурних дисбалансів в економіці регіонів та практичне вичерпання потенціалу традиційних чинників економічного зростання та стійкості у глобальному та національному масштабах обумовлюють необхідність удосконалення політики територіального розвитку в Україні.

В умовах новітніх глобальних трендів економічного розвитку (у тому числі метрополізації, мережизації, інтелектуалізації та діджиталізації практично усіх суспільно-економічних процесів) актуалізуються питання пошуку виважених рішень щодо використання даного потенціалу, подолання викликів, пов'язаних із стрімкими інноваційними та операційними нововведеннями, а також розуміння того, як працюють нові бізнес-моделі та яким чином слід модифікувати системи управління трансформаційними процесами в економіці міст та регіонів задля отримання найбільшої вигоди для усіх зацікавлених сторін.

Нині при визначеному державному курсі на запровадження інноваційних форм розвитку територій в Україні недостатньо вивченими залишаються питання, пов'язані з безпосереднім їх упровадженням, а також визначенням критеріїв вибору методів і інструментів управління ними.

У структурі економіки міст закладений найважливіший резерв економічного зростання. Економічне зростання країн Західної Європи було зумовлено за рахунок використання потенціалу зростання міст, глибинної трансформації структур їх економік у напрямку впровадження у ключові галузі новітніх розробок та прогресивних технологій науково-технічного процесу, розвитку інформаційно-комунікативного середовища та включення суб'єктів господарювання та ділової інфраструктури у глобальні потоки інформації, капіталів та управлінських рішень. Актуалізуються питання досягнення ефективності економічних структурних трансформацій в контексті секторальних, діяльнісно-видових, технологічних, відтворювальних, соціальних,



МУКАЧІВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

89600, м. Мукачево, вул. Ужгородська, 26

тел./факс +380-3131-21109

Веб-сайт університету: www.msu.edu.ua

E-mail: info@msu.edu.ua, pr@mail.msu.edu.ua

Веб-сайт Інституційного репозитарію Наукової бібліотеки МДУ: <http://dspace.msu.edu.ua:8080>

Веб-сайт Наукової бібліотеки МДУ: <http://msu.edu.ua/library/>