ДОДАТОК А

Копії публікацій

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ

Кафедра економічної кібернетики та управління економічною безпекою

СУЧАСНІ СТРАТЕГІЇ ЕКОНОМІЧНОГО РОЗВИТКУ:
НАУКА, ІННОВАЦІЇ ТА БІЗНЕС-ОСВІТА

матеріали
V Міжнародної науково-практичної конференції

3 грудня 2024 року

Харків 2024

УДК 330.341; 338.24; 005 (06)
С91

Сучасні стратегії економічного розвитку: наука, інновації та бізнес-освіта. Матеріали V Міжнародної науково-практичної конференції (м. Харків, 3 грудня 2024 р.) / За заг. ред. д.е.н., проф. Т.В. Полозової. Харків. ХНУРЕ. 2024. 192 с.

У збірнику містяться матеріали, що були подані на V Міжнародну науково-практичну конференцію «Сучасні стратегії економічного розвитку: наука, інновації та бізнес-освіта» (м. Харків, 3 грудня 2024 року).

Праці науковців охоплюють такі тематичні напрями досліджень: сучасні економічні теорії та історія економічної думки; світове господарство: нові виклики та інноваційні форми міжнародних економічних відносин; єдиний цифровий ринок Європейського союзу; економіка та управління національним господарством; розвиток сучасного підприємництва в умовах впливу та протидії гібридним загрозам; інформаційні технології в бізнесі: електронна комерція та віртуальна торгівля; економіка природокористування та сучасні проблеми охорони навколишнього середовища; демографія, економіка праці, соціальна економіка і політика; бухгалтерський облік, аналіз і аудит: національні особливості та світові тенденції; сучасні математичні методи, моделі та інформаційні системи в економіці; Україна-ЄС: цифрові інновації для змін; фінанси, страхування та банківська справа; економіка підприємства та корпоративне управління: безпека бізнесу та модернізація бізнес-процесів; інновації в бізнес-освіті.

Результати наукових досліджень, що представлені у збірнику, виконані в межах реалізації НДР і Міжнародного гранту кафедри економічної кібернетики та управління економічною безпекою Харківського національного університету радіоелектроніки, а саме: науково-дослідної роботи «Організаційно-економічне забезпечення інноваційного розвитку та економічної безпеки суб'єктів господарювання» (Державний реєстраційний номер 0122U000510); Міжнародного проєкту Еразмус + KA2 «University-communities: strengthening cooperation/UNICOM» (project #101083077 CBHE Strand 3).

Для науковців, викладачів, аспірантів, а також фахівців, що займаються дослідженням питань соціально-економічного розвитку та забезпечення економічної безпеки підприємств, галузей, регіонів та країни.

УДК 330.341; 338.24; 005 (06)

Автори є цілком відповідальними за висловлені ідеї, висновки та пропозиції.
Праці відтворюються безпосередньо з авторських оригіналів.
У разі використання матеріалів збірника посилання на авторів і видання обов'язкове.
Розповсюджувати та тиражувати без офіційного дозволу ХНУРЕ забороняється.

© Кафедра економічної кібернетики та управління економічною безпекою, 2024
© Харківський національний університет радіоелектроніки, 2024
© Колектив авторів, 2024

Міністерство освіти і науки України
Харківський національний університет радіоелектроніки
Українська асоціація з розвитку менеджменту та бізнес-освіти
Науково-дослідний центр індустріальних проблем розвитку НАН України
Київський національний університет технологій та дизайну
Асоціація «Міжнародний науково-освітній траст»
Національний фонд досліджень України
ТОВ «Компанія з управління активами «Реноме-2008»
Університет національної та світової економіки, Болгарія
The European Academy of Sciences Ltd, United Kingdom
Латвійський університет, Латвія
Університет Бабеш-Больої, Клуж-Напока, Румунія

ЧЛЕНИ ОРГАНІЗАЦІЙНОГО КОМІТЕТУ КОНФЕРЕНЦІЇ

Ігор Рубан, в.о. ректора Харківського національного університету радіоелектроніки, д.т.н., професор, Україна.
Юрій Романенков, проректор з наукової роботи, Харківський національний університет радіоелектроніки, д.т.н., професор, Україна.
Тетяна Полозова, завідувач кафедри економічної кібернетики та управління економічною безпекою, Харківський національний університет радіоелектроніки, д.е.н., професор, Україна.
Світлана Гришко, професор кафедри економічної кібернетики та управління економічною безпекою, Харківський національний університет радіоелектроніки, к.е.н., доцент, Україна.
Людмила Горохова, директор Української асоціації з розвитку менеджменту та бізнес-освіти, Україна.
Надія Белікова, учений секретар Науково-дослідного центру індустріальних проблем розвитку НАН України, д.е.н., професор, Україна.
Вікторія Маргасова, директор науково-дослідного інституту економіки, Київський національний університет технологій та дизайну, д.е.н., професор, Україна.
Георгій Іоффе, президент асоціації «Міжнародний науково-освітній траст», Україна.
Максим Колісник, головний спеціаліст відділу «Офіс Горизонт Європа в Україні» Національного фонду досліджень України, к.держ.упр., доцент, Україна.
Євгеній Ситниченко, директор ТОВ «Компанія з управління активами «Реноме-2008», к.ф.н., Україна.
Kostadin Kolarov, PhD, Associate Professor, Director Institute of Entrepreneurship University of National and World Economy, Bulgaria.
Svetlana Drobyazko, Doctor of Economics, Professor, President of The European Academy of Sciences Ltd, United Kingdom.
Baiba Šavriņa, Dr.oec., Professor, University of Latvia, Riga, Latvia.
Adriana Tiron Tudor, Dr., Prof. univ., Babeş-Bolyai University, Cluj-Napoca, Romania.

Олена Мурзабулатова, доцент кафедри економічної кібернетики та управління економічною безпекою, Харківський національний університет радіоелектроніки, к.е.н., доцент, Україна, *секретар конференції.*

Ministry of Education and Science of Ukraine
Kharkiv National University of Radio Electronics
Ukrainian Association for Management Development and Business Education
Research Center for Industrial Development Problems of National Academy of Sciences
Kyiv National University of Technologies and Design
International Scientific and Educational Trust Association Non-governmental organization
National Research Foundation of Ukraine
Assets Management Company «Renome-2008» LTD
University of National and World Economy, Bulgaria
The European Academy of Sciences Ltd, United Kingdom
University of Latvia, Latvia
Babeș-Bolyai University, Cluj-Napoca, Romania

MEMBERS OF THE CONFERENCE ORGANIZING COMMITTEE

Igor Ruban, Acting Rector of Kharkiv National University of Radio Electronics, Doctor of Technical Sciences, Professor, Ukraine.
Yuri Romanenkov, Vice-Rector for Scientific Work, Kharkiv National University of Radio Electronics, Doctor of Technical Sciences, Professor, Ukraine.
Tetiana Polozova, Head of Department of Economic Cybernetics and Management of Economic Security, Kharkiv National University of Radio Electronics, Doctor of Economic Sciences, Professor, Ukraine.
Svitlana Gryshko, Professor of Department of Economic Cybernetics and Management of Economic Security, Kharkiv National University of Radio Electronics, Candidate of Economic Sciences, Associate Professor, Ukraine.
Lyudmyla Gorokhova, Director of Ukrainian Association for Management Development and Business Education, Ukraine.
Nadiia Bielikova, Academic Secretary of Research Center for Industrial Development Problems of National Academy of Sciences, Doctor of Economic Sciences, Professor, Ukraine.
Viktoriia Marhasova, Director of Research Institute of Economics, Kyiv National University of Technologies and Design, Doctor of Economic Sciences, Professor, Ukraine.
Georgii Ioffe, President Association «International Scientific and Educational Trust», Ukraine.
Maksym Kolisnyk, Pillar Officer at Horizon Europe Office in Ukraine, National Research Foundation of Ukraine, PhD in Public Administration, Associate Professor.
Yevhenii Sytnychenko, Director of Assets Management Company «Renome-2008» LTD, PhD, Ukraine.
Kostadin Kolarov, PhD, Associate Professor, Director Institute of Entrepreneurship University of National and World Economy, Bulgaria.
Svetlana Drobyazko, Doctor of Economics, Professor, President of The European Academy of Sciences Ltd, United Kingdom.
Baiba Šavriņa, Dr.oec., Professor, University of Latvia, Riga, Latvia.
Adriana Tiron Tudor, Dr., Prof. univ., Babeș-Bolyai University, Cluj-Napoca, Romania.

Olena Murzabulatova, Associate Professor of Department of Economic Cybernetics and Management of Economic Security, Kharkiv National University of Radio Electronics, Candidate of Economic Sciences, Associate Professor, Ukraine, ***Secretary of the Conference.***

ЗМІСТ

Batih V.
FEATURES OF ENTERPRISE DEVELOPMENT MANAGEMENT IN THE CONTEXT OF INCLUSIVE DEVELOPMENT 9
Budyansky V.S., Boichenko M.Y.
SELF-MANAGEMENT AS A METHOD OF INCREASING THE EFFICIENCY OF AN ENTERPRISE'S ECONOMIC ACTIVITY USING THE PARETO PRINCIPLE AND PARKINSON'S LAW 13
Mazhuta V., Zhang Qin
LEVERAGING THE BALANCED SCORECARD FOR MANAGING SUSTAINABLE ENTERPRISE DEVELOPMENT 18
Murzabulatova O., Suknov O.
RELATIONSHIP BETWEEN ENTERPRISE DEVELOPMENT POTENTIAL AND ECONOMIC SECURITY 21
Romanenkov Yu.O. Mursalzade Ziya, Mazepa A.S.
PERSPECTIVES AND RISKS OF INVESTMENTS IN OIL, FINANCIAL ASSETS AND CRYPTOCURRENCY 24
Sheiko I., Martynenko M., Krasnomovets H.
THE ROLE OF DIGITAL TECHNOLOGIES IN COMBATING CYBERATTACKS 27
Sheiko I., Huo Huizhu, Ahazada Elnur
ANALYSIS OF THE METHODS FOR ECONOMIC SECURITY ASSESSMENT 30
Sheiko I., Wan Wei, Dolina K.
DIGITAL RISKS FOR IT COMPANIES 33
Близнюк Т.П., Хунхай Ван
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ: СУТНІСТЬ ТА СКЛАДОВІ 36
Вешкін Є.П., Осадчук І.О., Осадчук М.О.
ТЕОРЕТИЧНІ ЗАСАДИ ФОРМУВАННЯ ІНВЕСТИЦІЙНОГО ПОТЕНЦІАЛУ ПІДПРИЄМСТВА В УМОВАХ ЕКОНОМІЧНОЇ БЕЗПЕКИ 38
Гришко С.В., Ступак О.М.
УПРАВЛІННЯ СИСТЕМОЮ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА В УМОВАХ ВІДДАЛЕНОЇ РОБОТИ 41
Гришко С.В., Черніков Д.І.
ІНСТРУМЕНТ МІНІМІЗАЦІЇ ВПЛИВУ ГІБРИДНИХ ЗАГРОЗ НА ЕКОНОМІЧНИЙ РОЗВИТОК СУЧАСНОГО ПІДПРИЄМНИЦТВА 44
Гусейнлі Ш.Р. огли
КОНТРОЛІНГОВЕ УПРАВЛІННЯ В УМОВАХ ЦИФРОВІЗАЦІЇ 47
Гуца О.М., Ігуменцева Н.В., Макуйлов О.В.
МОТИВАЦІЯ ПЕРСОНАЛУ ЯК ЕЛЕМЕНТ СИСТЕМИ KPI 49
Ду Ханьюй
МІСЦЕ І РОЛЬ БІЗНЕС-ОСВІТИ В СИСТЕМІ ОСВІТНІХ ПОСЛУГ 53

Довгопол Н.В., Цицилін А.О.
ОСНОВНІ АСПЕКТИ ВПРОВАДЖЕННЯ ЦИРКУЛЯРНОЇ ЕКОНОМІКИ В УКРАЇНІ..... 56
Іванов І.О.
ПОНЯТТЯ ІННОВАЦІЙНО-ІНВЕСТИЦІЙНОГО РОЗВИТКУ ПІДПРИЄМСТВА..... 59
Ігуменцева Н.В., Мануйлов О.В.
СТАТИСТИЧНЕ ОЦІНЮВАННЯ ВІДПОВІДНОСТІ ЯКОСТІ РОБОЧОЇ СИЛИ СПЕЦИФІЦІ ПРАЦІ..... 62
Кирій В.В., Кравець М.Ю.
КРЕДИТОСПРОМОЖНІСТЬ ЯК КОМПОНЕНТ ФІНАНСОВОГО ПОТЕНЦІАЛУ ПІДПРИЄМСТВА..... 65
Кирій В.В., Твердохлібов М.В., Краснощок В.І.,
РОЗВИТОК СУЧАСНОГО ПІДПРИЄМНИЦТВА В УМОВАХ ВПЛИВУ ТА ПРОТИДІЇ ГІБРИДНИМ ЗАГРОЗАМ..... 68
Крамаренко К.М., Мадера В.С.
ДЖЕРЕЛА ФОРМУВАННЯ СПЕЦІАЛЬНОГО ФОНДУ ОБОРОННОГО БЮДЖЕТУ УКРАЇНИ..... 71
Курденко О.В., Моісеєнко А.Ю.
ЗАСТОСУВАННЯ ESG В ПРИЙНЯТТІ ІНВЕСТИЦІЙНИХ РІШЕНЬ..... 74
Курденко О.В., Моісеєнко Є.Ю.
СПЕЦИФІКА ІНВЕСТУВАННЯ В ІНТЕЛЕКТУАЛЬНИЙ КАПІТАЛ..... 77
Марченко Р.О., Глушков А.В.
ШЛЯХИ ЗМЕНШЕННЯ ВТРАТ НА НЕБАЛАНСАХ ЯК ОДИН З ШЛЯХІВ РОЗВИТКУ ПІДПРИЄМСТВА В УМОВАХ ВПЛИВУ ТА ПРОТИДІЇ ГІБРИДНИМ ЗАГРОЗАМ..... 79
Мізін Д.С., Неронов П.Є., Салай М.В.
ДОСВІД ВИКОРИСТАННЯ ЦИФРОВИХ ІНСТРУМЕНТІВ ДЛЯ ПОСИЛЕННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ..... 82
Морозова Н.Л., Девчик І.С.
ЦИФРОВА ЕКОНОМІКА В УКРАЇНІ: МОЖЛИВОСТІ, ВИКЛИКИ ТА ПЕРСПЕКТИВИ..... 85
Морозов Д.П.
УДОСКОНАЛЕННЯ УПРАВЛІННЯ ПЕРСОНАЛОМ ПІДПРИЄМСТВ АГРАРНОГО СЕКТОРУ ЕКОНОМІКИ В УМОВАХ ВОЄННОГО СТАНУ..... 88
Мурзабулатова О.В., Білоус П.В., Саричева М.В.
ОРГАНІЗАЦІЙНО-УПРАВЛІНСЬКІ АСПЕКТИ ФУНКЦІОНУВАННЯ ПРИВАТНИХ ОСВІТНІХ ЦЕНТРІВ В УМОВАХ ПАНДЕМІЇ ТА ВОЄННОГО СТАНУ..... 91
Мурзабулатова О.В., Кравцов О.О.
ЕКОНОМІЧНА ДІАГНОСТИКА ІННОВАЦІЙНОЇ АКТИВНОСТІ ПІДПРИЄМСТВА..... 94

Петренко Д.А.
ІНКЛЮЗИВНЕ ПІДПРИЄМНИЦТВО ЯК ВЕКТОР РОЗВИТКУ БІЗНЕСУ..... 97
Перепелюкова О.В., Полозов О.Б.
ПРОБЛЕМИ РОЗВИТКУ РЕГІОНІВ В КОНТЕКСТІ ЗАБЕЗПЕЧЕННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ..... 102
Помогалова Н.В., Мороз М.Ю.
МЕТОДИ МІНІМІЗАЦІЇ ІНВЕСТИЦІЙНИХ РИЗИКІВ..... 105
Помогалова Н.В., Тесленко І.В., Полозова О.О.
МЕХАНІЗМИ СТИМУЛЮВАННЯ ІННОВАЦІЙНОГО РОЗВИТКУ ПІДПРИЄМСТВ..... 108
Пономарьов С.В., Мороз М.Ю.
ТЕОРЕТИЧНІ ЗАСАДИ УПРАВЛІННЯ РИЗИКАМИ В ІННОВАЦІЙНОМУ ПІДПРИЄМНИЦТВІ..... 111
Пономарьов С.В., Москальова М.С.
УПРАВЛІННЯ МАРКЕТИНГОВИМИ РИЗИКАМИ..... 114
Пономарьов С.В., Мурзабулатова М.С.
ПЕРЕДУМОВИ ВИНИКНЕННЯ ТА ШЛЯХИ ПОДОЛАННЯ КРИЗИ НА ПІДПРИЄМСТВІ..... 117
Прібильнова І.Б., Антонович В.Д.
ЗАСТОСУВАННЯ СУЧАСНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ДЛЯ МОНІТОРИНГУ МАКРОЕКОНОМІЧНИХ ТЕНДЕНЦІЙ..... 120
Прібильнова І.Б., Дзівінська А.О.
МОДЕЛІ ПЕРЕДБАЧУВАНОЇ АНАЛІТИКИ ДЛЯ ЗАПОБІГАННЯ КІБЕРЗАГРОЗАМ НА ПІДПРИЄМСТВАХ..... 123
Прібильнова І.Б., Кравцов О.О.
ІНТЕГРАЦІЯ АНАЛІТИЧНИХ ПЛАТФОРМ ДЛЯ КОМПЛЕКСНОЇ БЕЗПЕКИ НА ПІДПРИЄМСТВАХ..... 126
Прібильнова І.Б., Мороз М.Ю.
СПЕЦИФІКА УПРАВЛІННЯ РИЗИКАМИ В СТАРТАПАХ..... 129
Прібильнова І.Б., Москальова М.С.
ЗАСТОСУВАННЯ CRM-СИСТЕМ В МАРКЕТИНГОВІЙ ДІЯЛЬНОСТІ..... 132
Прібильнова І.Б., Носарєва А.Е.
ФОРМУВАННЯ МАРКЕТИНГОВОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ ПІДПРИЄМСТВА..... 135
Прібильнова І.Б., Пересада О.В.
ПРОБЛЕМИ СТАЛОГО РОЗВИТКУ ПІДПРИЄМСТВ УКРАЇНИ..... 138
Салманов Ельбей Зака огли
ПІДХОДИ ДО УПРАВЛІННЯ МІЖКУЛЬТУРНИМИ КОМУНІКАЦІЯМИ..... 140
Синіговець О.М.
ГАЛУЗЕВА КОНКУРЕНТОСПРОМОЖНІСТЬ У СВІТОВОМУ ГОСПОДАРСТВІ ТА ВИКЛИКИ ГЛОБАЛІЗАЦІЇ..... 142
Соколова Л.В., Антонович В.Д.
ІННОВАЦІЙНІ СТРАТЕГІЇ У РОЗВИТКУ ПОТЕНЦІАЛУ ПІДПРИЄМСТВА..... 145

Соколова Л.В., Горгуль К.Р.
ТЕОРЕТИКО-МЕТОДИЧНІ АСПЕКТИ ОЦІНКИ ФІНАНСОВОГО ПОТЕНЦІАЛУ ПІДПРИЄМСТВА В УМОВАХ МІНЛИВОГО ЕКОНОМІЧНОГО СЕРЕДОВИЩА.....148
Соколова Л.В., Дзівінська А.О., Бабаєв М.М.
КОНКУРЕНТНИЙ АНАЛІЗ В ЕРУ ШТУЧНОГО ІНТЕЛЕКТУ.....152
Соколова Л.В., Деменчук В.Д.
ТЕОРЕТИЧНІ АСПЕКТИ ФОРМУВАННЯ ІННОВАЦІЙНОЇ ЛОГІСТИЧНОЇ СТРАТЕГІЇ.....155
Соколова Л.В., Орлов В.О.
СУТНІСТЬ ПОНЯТТЯ ЕФЕКТИВНОСТІ ДІЯЛЬНОСТІ ПІДПРИЄМСТВА.....158
Соколова Л.В., Соловйов М.С.
ХАРАКТЕРИСТИКА НАПРЯМІВ ВИКОРИСТАННЯ ІНСТРУМЕНТАРІЮ ФІНАНСОВОГО АНАЛІЗУ ДЛЯ ОЦІНКИ ФІНАНСОВО-ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА.....161
Станьковська І.М., Смага Л.Р.
АНАЛІЗ ПОКАЗНИКІВ ОЦІНЮВАННЯ ДІЯЛЬНОСТІ ПРОМИСЛОВИХ ПІДПРИЄМСТВ НА ЗАСАДАХ СТАЛОГО РОЗВИТКУ.....164
Ткаченко А.Г., Герасимюк Д.Ю., Гуреєва К.А.
РОЛЬ КОМПЕТЕНТНОСТЕЙ В ІННОВАЦІЙНОМУ РОЗВИТКУ ПІДПРИЄМСТВА.....167
Тохтамиш Н.І., Дзівінська А.О., Гуляєв Н.Ю.
ВЗАЄМОДІЯ БІЗНЕСУ ТА ВІЙСЬКОВИХ СТРУКТУР ПІД ЧАС ВІЙНИ.....170
Турчин О.А., Матвєєва Д.А., Полозов М.О.
АНАЛІЗ ІСНУЮЧИХ ПРАКТИК ВПРОВАДЖЕННЯ КОНЦЕПЦІЇ РОЗУМНОГО МІСТА В УКРАЇНІ.....173
Худяков Д.Л., Зінов'єв А.П., Какуник Є.В.
ОЦІНКА ЕФЕКТИВНОСТІ ІННОВАЦІЙНО-ІНВЕСТИЦІЙНИХ ПРОЄКТІВ В КОНТЕКСТІ СТРАТЕГІЧНОГО РОЗВИТКУ ПІДПРИЄМСТВА.....176
Шейко І.А., Степаненко Р.Д., Кузовкіна К.Р.
РИЗИКИ ТА ЗАГРОЗИ ЕКОНОМІЧНІЙ БЕЗПЕЦІ ПІДПРИЄМСТВА В КОНТЕКСТІ ЦИФРОВОГО РОЗВИТКУ.....179
Штанько В.І., Герсимюк Д.Ю.
ЕТИКА ШТУЧНОГО ІНТЕЛЕКТУ У ФІНАНСОВИХ СИСТЕМАХ: ВИКЛИКИ ТА ПЕРСПЕКТИВИ.....182
Штанько В.І., Кушнір І.С.
ВПЛИВ ЦИФРОВИХ ТЕХНОЛОГІЙ НА КОНЦЕПЦІЮ ЗМІНИ РОЗУМІННЯ РЕСУРСІВ У ПРОЄКТНОМУ УПРАВЛІННІ.....186
Штанько В.І., Мізін Д.С.
МОРАЛЬНІ ДИЛЕМИ ГЛОБАЛІЗАЦІЇ: ЕКОНОМІЧНА ЕФЕКТИВНІСТЬ АБО КУЛЬТУРНА ІДЕНТИЧНІСТЬ.....189

Batih V.,
PhD student,
Kharkiv National University of Radio Electronics
ORCID: https://orcid.org/0009-0007-3883-3648

FEATURES OF ENTERPRISE DEVELOPMENT MANAGEMENT IN THE CONTEXT OF INCLUSIVE DEVELOPMENT

For a long time, Ukraine was dominated by an outdated economic and social development model, which limited opportunities for sustainable growth and social integration. Such a model contributed to the preservation of a high level of poverty and prevented the provision of conditions for the effective participation of all segments of the population in public life and economic activity. It has also contributed to the growth of environmental challenges due to the unwise use of natural resources and neglect of rational production and consumption principles. This led to deepening social inequality and slowing down the country's economic development, increasing social tensions and reducing the economy's overall competitiveness.

At the beginning of 2022, the situation remained difficult: pensioners amounted to more than 10.8 million people, of which 8 million were pensioners by age [2, p. 23]. At the same time, the number of people with disabilities who, due to their restrictions, were not able to fully participate in social activities amounted to 316.1 thousand people (11.6% of the total number of people with disabilities). Unemployment also remained a severe problem, covering 171.6 thousand people. Which negatively affected both the individual well-being of citizens and the economic stability of the country as a whole.

Another critical aspect of social inequality is widespread poverty among the population. In 2021, more than 1 million households in Ukraine received an average per capita income that did not exceed UAH 3000, which indicates a profound social and economic crisis. The large number of such households means that millions need

Мізін Д.С.,
здобувач вищої освіти,
Харківський національний університет радіоелектроніки
ORCID: https://orcid.org/0009-0005-5692-5859
Нєронов П.Є.,
здобувач вищої освіти,
Харківський національний університет радіоелектроніки
ORCID: https://orcid.org/0009-0003-7597-1346
Салай М.В.,
здобувач вищої освіти,
Харківський національний університет радіоелектроніки
ORCID: https://orcid.org/0009-0007-3583-7715

ДОСВІД ВИКОРИСТАННЯ ЦИФРОВИХ ІНСТРУМЕНТІВ ДЛЯ ПОСИЛЕННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ

Цифрові технології стають ключовим фактором у забезпеченні економічної безпеки. Використання цифрових інструментів сприяє боротьбі з кіберзагрозами, покращенню державного управління, оптимізації економічних процесів і підвищенню конкурентоспроможності. В даному дослідженні розглядається досвід впровадження цифрових технологій у державне управління країн світу.

Естонію часто визнають однією з найбільш розвинутих у цифровому відношенні країн світу з надійною цифровою інфраструктурою та великим акцентом на кібербезпеці. Урядова ініціатива електронної Естонії перетворила країну на модель цифрового управління. Країна перевела в онлайн майже всі державні послуги, використовуючи захищену систему електронного урядування, яка надає громадянам доступ до онлайн-медичних послуг, банківських послуг і послуг голосування. Після кібератаки в 2007 році Естонія створила потужну

інфраструктуру кібербезпеки, включаючи створення посольств даних для безпечного зберігання державних даних за межами Естонії [1].

Сінгапур став лідером цифрової економіки в Південно-Східній Азії завдяки своїй ініціативі Smart Nation, метою якої є інтеграція цифрових технологій у державний і приватний сектори. Уряд Сінгапуру оцифрував багато своїх послуг і сприяє безготівковим транзакціям і міському плануванню на основі даних. У галузі кібербезпеки Сінгапур запровадив Закон про захист персональних даних (PDPA) і створив Агентство кібербезпеки Сінгапуру для захисту критичної інфраструктури та просування стандартів кібербезпеки.

Одним із світових лідерів у галузі кібербезпеки є Ізраїль. Уряд активно підтримує стартапи в галузі кібербезпеки через програми фінансування та розвитку, створюючи Ізраїль як глобальний центр кібербезпеки. Досвід Ізраїлю в галузі кібербезпеки підкріплюється підготовкою у військовому та академічному секторах, коли колишні співробітники розвідувальних підрозділів засновують компанії з кібербезпеки або приєднуються до них [1].

ЄС прийняв Акт про кібербезпеку та Акт про Єдиний цифровий ринок [2] для посилення цифрового суверенітету та захисту економічних інтересів. Крім того, Європейський Союз встановив Загальний регламент захисту даних (GDPR), який містить протоколи обробки та зберігання даних [2].

Країни Європейського Союзу часто піддаються кібератакам, через що відбувається витік конфіденційних даних, страждає цифрова інфраструктура. Так, у 2014 році Європейський центральний банк оголосив, що вони зазнали витоку даних: хакери зламали безпеку бази даних банку та викрали 20 000 електронних листів. та контактну інформацію реєстрантів європейських заходів. У 2020 році невідомі злодії викрали два жорсткі диски зі сховища уряду Нідерландів, на яких містилися особисті дані приблизно 6,9 мільйонів зареєстрованих донорів органів, майже половини населення Нідерландів. Також у 2020 р. Norfund, норвезький державний інвестиційний фонд для країн, що розвиваються, і найбільший у світі суверенний фонд, виявив, що став жертвою

шахрайства на 10 мільйонів доларів. Norfund стверджує, що хакери маніпулювали комунікаціями, фальсифікували конфіденційну інформацію, документи та деталі платежів між установою-позичальником та інвестиційним фондом [3].

США впровадили програму щодо захисту критичної інфраструктури, як-от енергетика та фінанси, в рамках своєї стратегії економічної безпеки. Було створено Агентство з кібербезпеки та безпеки інфраструктури (CISA) для координації ініціатив у галузі кібербезпеки в державному та приватному секторах. Запроваджуються ініціативи у секторальній кібербезпеці, завдяки чому забезпечується цілеспрямований захист для таких секторів, як фінанси та оборона, допомагаючи запобігти масштабним збоям [1].

Досвід Естонії, Сінгапуру, Ізраїлю, ЄС та США демонструє, що цифрові інструменти є ефективними засобами посилення економічної безпеки. Інтеграція таких технологій, як блокчейн, ШІ та IoT, у державне управління та бізнес сприяє стійкості економік до викликів глобалізації та цифровізації. Україні слід враховувати цей досвід для розробки власної стратегії цифрової трансформації.

Перелік джерел посилання

1. Herpig S., Morgus R., Sheniak A. Active Cyber Defense- A comparative study on US, Israeli and German approaches. January 2020 URL: https://www.interface-eu.org/storage/archive/files/active_cyber_defense-_a_comparative_study_on_us_israeli_and_german_approaches.pdf.

2. European Commission. The digital market's act. URL: https://digital-markets-act.ec.europa.eu/index_en.

3. Chin K. Biggest Data Breaches in Europe. UpGuard. 18 November, 2024. URL: https://www.upguard.com/blog/biggest-data-breaches-europe.

Морозова Н.Л.,
к.е.н., доцент кафедри менеджменту,
бізнесу та професійних комунікацій
Харківський національний університет ім. В.Н. Каразіна
ORCID: https://orcid.org/0000-0002-4082-2960
Денчик І.С.,
здобувач вищої освіти,
Харківський національний університет ім. В.Н. Каразіна
ORCID: https://orcid.org/0000-0003-1594-1084

ЦИФРОВА ЕКОНОМІКА В УКРАЇНІ: МОЖЛИВОСТІ, ВИКЛИКИ ТА ПЕРСПЕКТИВИ

Цифрова економіка є основою сучасного світу, трансформуючи економічні, соціальні та культурні процеси. Вона формує нові бізнес-моделі, змінює традиційні підходи до управління та стимулює інновації у виробництві, освіті та охороні здоров'я. Водночас вона створює нові виклики, пов'язані з адаптацією суспільства та бізнесу до динамічних змін.

Зростання ролі інформаційно-комунікаційних технологій (ІКТ) сприяє інтеграції цифрових рішень у всі аспекти життєдіяльності. Виробництво стає більш автоматизованим, управління – прозорішим і ефективнішим, а освіта – доступнішою завдяки онлайн-ресурсам. Сучасні медичні технології, засновані на ІКТ, забезпечують точність діагностики та ефективність лікування.

Одним із ключових аспектів є цифровізація – процес переходу від аналогових до цифрових технологій, що формує основу для інтеграції інноваційних рішень і підвищення ефективності економічних процесів. Вона охоплює впровадження сучасних технологій, таких як великі дані (Big Data), інтернет речей (IoT) і штучний інтелект (AI). Ці елементи забезпечують

Наукове видання

СУЧАСНІ СТРАТЕГІЇ ЕКОНОМІЧНОГО РОЗВИТКУ:
НАУКА, ІННОВАЦІЇ ТА БІЗНЕС-ОСВІТА

Матеріали
V Міжнародної науково-практичної конференції

3 грудня 2024 року
м. Харків, Україна

За загальною редакцією
доктора економічних наук, професора Т.В. Полозової

Редактор:
кандидат економічних наук, доцент О.В. Мурзабулатова

Файл надано:
Харківський національний університет радіоелектроніки,
Кафедра економічної кібернетики та управління економічною безпекою,
61166, Україна, м. Харків, пр. Науки, 14,
тел. (057) 702-14-90,
e-mail: sser.conf@gmail.com

Підп. до друку 20.12.2024. Формат 60x84 1/16.
Друк цифровий. Ум. друк. арк. 8,72.
Тираж 100 прим. Ціна договірна.

Віддруковано в типографії ФОП Андреєв К.В.
61166, Харків, вул. Богомольця, 9, кв. 50.
Свідоцтво про державну реєстрацію
№ 24800170000045020 від 30.05.2003.
ep.zakaz@gmail.com
тел. 063-993-62-73

Kharkiv National University of Radio Electronics

Department of Economic Cybernetics and Management of Economic Security

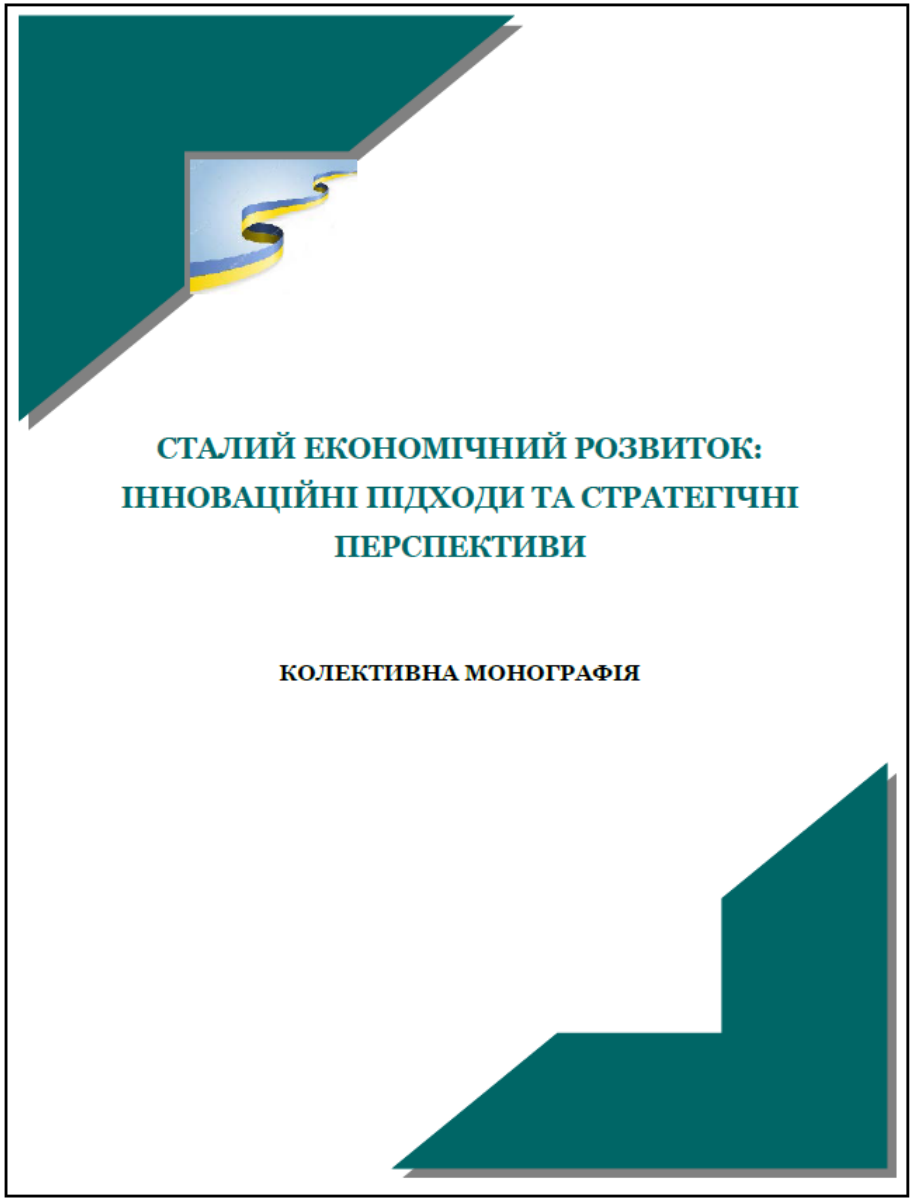
MODERN STRATEGIES OF ECONOMIC DEVELOPMENT: SCIENCE, INNOVATION AND BUSINESS EDUCATION

Proceedings of the Conference

V International Scientific and Practical Conference

December 3, 2024

Kharkiv, Ukraine



МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ

Кафедра економічної кібернетики та управління економічною безпекою

СТАЛИЙ ЕКОНОМІЧНИЙ РОЗВИТОК: ІННОВАЦІЙНІ ПІДХОДИ ТА СТРАТЕГІЧНІ ПЕРСПЕКТИВИ

Колективна монографія

Харків 2024

УДК 330.131
С91

Рекомендовано Науково-технічною радою
Харківського національного університету радіоелектроніки
(протокол від 26.12.2024 № 13)

Рецензенти

Бєлікова Н. В., доктор економічних наук, професор, Учений секретар Науково-дослідного центру індустріальних проблем розвитку НАН України.

Маргасова В. Г., доктор економічних наук, професор, директор Науково-дослідного інституту економіки Київського національного університету технологій та дизайну.

Ларіна Т. Ф., доктор економічних наук, професор, декан факультету економічних відносин та фінансів Державного біотехнологічного університету.

Сталий економічний розвиток: інноваційні підходи та стратегічні перспективи: колективна монографія / За заг. ред. д.е.н., проф. Т. В. Полозової. Харків: ХНУРЕ, 2024. 432 с.

Монографію присвячено дослідженню особливостей функціонування соціально-економічних систем в контексті цілей сталого розвитку. Висвітлено проблеми господарювання економічних агентів на всіх рівнях управління в умовах цифрової трансформації та протидії гібридним загрозам, питання забезпечення економічної безпеки окремих підприємств, галузей, регіонів та країни в цілому. Монографія є результатом теоретичних і практичних досліджень з удосконалення методологічного та науково-методичного забезпечення функціонування соціально-економічних систем на мікро-, мезо- та макроекономічному рівнях.

Монографія призначена для науковців, викладачів, здобувачів всіх рівнів вищої освіти, фахівців, професіоналів-практиків, які займаються дослідженням механізмів функціонування соціально-економічних систем, напрямів цифрової трансформації в умовах протидії гібридним загрозам, забезпечення економічної безпеки підприємств, галузей, регіонів та країни в контексті цілей сталого розвитку.

Відповідальність за зміст та достовірність матеріалів несуть автори. Думка авторів може не співпадати з думкою членів редколегії.

ISBN 978-966-659-401-6
DOI: 10.30837/ЕК.2024

© Кафедра економічної кібернетики та управління економічною безпекою, 2024
© Харківський національний університет радіоелектроніки, 2024
© Колектив авторів, 2024

ЗМІСТ

ВСТУП 6

Ovsiuchenko Y.V., Peresada O.V., Budyansky V.S.
WAYS OF IMPROVING THE FINANCIAL CONDITION OF AN ENTERPRISE AT THE MENTAL LEVEL 9

Romanenkov Yu., Wei Wan, Siusiuk S., Mazepa A.
NAVIGATING DIGITAL RISKS IN IT COMPANIES: CHALLENGES AND STRATEGIES FOR MITIGATION 18

Stepanenko S., Huo Yun Zhu, Tselik V., Ahazada E.
MODELING OF ECONOMIC SECURITY INDEX CALCULATION FOR TENCENT COMPANY 30

Wang Honghai
INFORMATION TECHNOLOGIES AS A COMPONENT OF THE SOCIAL AND COMMUNICATION SUPPORT OF AN ORGANIZATION 48

Zhang Qin
A HOLISTIC APPROACH TO IMPLEMENTING AN INTEGRATED SUSTAINABILITY MANAGEMENT SYSTEM 57

Безлепкін А.О., Тохтамиш Н.І., Толмачов Д.А., Турчин О.А.
ЦИРКУЛЯРНА ЕКОНОМІКА ЯК ОСНОВА СТРАТЕГІЧНОГО ПЛАНУВАННЯ ТА АНТИКРИЗОВОГО УПРАВЛІННЯ ПІДПРИЄМСТВОМ 71

Геселева Н.В., Пронюк Г.В., Стіценко Т.Є.
СИСТЕМНИЙ АНАЛІЗ ПСИХОФІЗІОЛОГІЧНИХ ОСОБЛИВОСТЕЙ ЛЮДИНИ В КОНТЕКСТІ СТАЛОГО РОЗВИТКУ ПІДПРИЄМСТВА 84

Гришко С.В., Черніков Д.І.
СТРАТЕГІЧНІ ПРІОРИТЕТИ РОЗВИТКУ ПРОМИСЛОВИХ ПІДПРИЄМСТВ В СУЧАСНИХ УМОВАХ 99

Гуца О.М., Ігуменцева Н.В., Мануйлов О.В.
СИСТЕМНИЙ ПІДХІД ПОБУДОВИ СИСТЕМИ КРІ ТА МОТИВАЦІЇ ПЕРСОНАЛУ 110

Довгопол Н.В., Цицилін А.О.
ВИКОРИСТАННЯ ЦИФРОВИХ ТЕХНОЛОГІЙ ЯК ОДИН З ПРИНЦИПІВ ЦИРКУЛЯРНОЇ ЕКОНОМІКИ 123

Другова О.С., Гусейнлі Ш.Р. огли
ТЕОРЕТИЧНІ АСПЕКТИ КОНТРОЛІНГУ В СИСТЕМІ УПРАВЛІННЯ РОЗВИТКОМ ПІДПРИЄМСТВА..... 130
Ду Ханьюй
СУТНІСТЬ І МІСЦЕ БІЗНЕС-ОСВІТИ В СИСТЕМІ ОСВІТНІХ ПОСЛУГ..... 144
Кирій В.В., Брюхно О.В., Глушков А.В.
ІНВЕСТИЦІЙНИЙ ПІДХІД ДО ОЦІНКИ РІВНЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ ЕНЕРГЕТИЧНИХ ПІДПРИЄМСТВ..... 154
Легеза О.М., Тесленко І.В., Полозова О.О., Полозов М.О.
ВПЛИВ КІБЕРЗАГРОЗ ТА ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ НА ЗАБЕЗПЕЧЕННЯ ФІНАНСОВОЇ БЕЗПЕКИ ПІДПРИЄМСТВА..... 167
Мізін Д.С., Вешкін Є.П., Зінов'єв А.П.
ДІАГНОСТИКА ЕФЕКТИВНОСТІ ДІЯЛЬНОСТІ ПІДПРИЄМСТВА ЯК ІНСТРУМЕНТ ЗАБЕЗПЕЧЕННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ ТА ІННОВАЦІЙНОГО РОЗВИТКУ..... 177
Мурзабулатова О.В., Сукнов О.М.
ФІНАНСОВА БЕЗПЕКА ЯК КЛЮЧОВИЙ ЕЛЕМЕНТ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА..... 189
Перепелюкова О.В., Полозов О.Б.
СТРАТЕГІЧНІ ПРІОРИТЕТИ РЕГІОНАЛЬНОГО РОЗВИТКУ В УМОВАХ ПОВОЄННОГО ВІДНОВЛЕННЯ ДЕРЖАВИ..... 198
Полозова Т.В., Гурєєва К.А., Доліна К.А., Бессараб І.В.
ТЕОЕРТИЧНІ АСПЕКТИ ОЦІНКИ ЕФЕКТИВНОСТІ ТА РИЗИКІВ ІННОВАЦІЙНО-ІНВЕСТИЦІЙНОЇ ДІЯЛЬНОСТІ ПІДПРИЄМСТВА..... 208
Полозова Т.В., Іванов І.О.
ПОНЯТТЯ ТА ОСОБЛИВОСТІ ІННОВАЦІЙНО-ІНВЕСТИЦІЙНОЇ ДІЯЛЬНОСТІ ПІДПРИЄМСТВ 220
Полозова Т.В., Кануник Є.В., Матвєєва Д.А., Мурсалзаде З.
ЕНЕРГЕТИЧНА БЕЗПЕКА УКРАЇНИ: ФОРМУВАННЯ МЕХАНІЗМУ ЗАБЕЗПЕЧЕННЯ..... 233
Полозова Т.В., Ткаченко А.Г., Осадчук І.О., Осадчук М.О.
МЕХАНІЗМИ МІНІМІЗАЦІЇ РИЗИКІВ ЕКОНОМІЧНОЇ БЕЗПЕКИ В ПРОЦЕСІ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ ПІДПРИЄМСТВ..... 248
Полозова Т.В., Харченко В.В.
СУЧАСНІ МЕТОДИ ОЦІНКИ ЕФЕКТИВНОСТІ ДІЯЛЬНОСТІ ПІДПРИЄМСТВА..... 262
Помогалова Н.В., Худяков Д.Л., Герасимюк Д.Ю.
ІННОВАЦІЙНА ДІЯЛЬНІСТЬ ПІДПРИЄМСТВА ЯК ОСНОВА СТАЛОГО ЕКОНОМІЧНОГО РОЗВИТКУ..... 274

Прібильнова І.Б., Пересада О.В.
СИСТЕМИ ВИМІРЮВАННЯ ПОКАЗНИКІВ СТАЛОГО РОЗВИТКУ ПІДПРИЄМСТВ УКРАЇНИ..... 286
Салманов Ельбей Зака огли
ОБҐРУНТУВАННЯ ЗАСТОСУВАННЯ КОМПЕТЕНТНІСНОГО ПІДХОДУ ДО УПРАВЛІННЯ МІЖКУЛЬТУРНИМИ КОМУНІКАЦІЯМИ..... 297
Соколова Л.В., Горгуль К.Р.
МЕТОДИ РЕЙТИНГУВАННЯ ФІНАНСОВОГО ПОТЕНЦІАЛУ ПІДПРИЄМСТВА..... 306
Соколова Л.В., Деменчук В.Д.
АНАЛІЗ КЛЮЧОВИХ ХАРАКТЕРИСТИК ІННОВАЦІЙНИХ ЛОГІСТИЧНИХ СТРАТЕГІЙ..... 322
Соколова Л.В., Орлов В.Б.
НАУКОВО-ПРАКТИЧНІ ПІДХОДИ ДО ВИЗНАЧЕННЯ ЕКОНОМІЧНОЇ ЕФЕКТИВНОСТІ ДІЯЛЬНОСТІ ПІДПРИЄМСТВА..... 335
Соколова Л.В., Соловйов М.С.
ПРОГНОЗУВАННЯ ЙМОВІРНОСТІ БАНКРУТСТВА ЯК МЕТОД ОЦІНКИ ФІНАНСОВОЇ СТІЙКОСТІ ПІДПРИЄМСТВА..... 344
Степаненко С.В., Леоненко О.В., Мар'єнко О.М., Красномовець Г.О.
ТЕОРЕТИКО-МЕТОДИЧНІ АСПЕКТИ ОЦІНКИ ПРИБУТКОВОСТІ ТА ОПТИМАЛЬНОГО РОЗПОДІЛУ БАНКІВСЬКИХ РЕСУРСІВ..... 354
Тардаскіна Т.М.
КОМПЛЕКСНА ОЦІНКА РОЗВИТКУ ІТ-ГАЛУЗІ В УКРАЇНІ..... 365
Тардаскіна Т.М., Толкачова Г.В., Терешко Ю.В.
ВПРОВАДЖЕННЯ ІННОВАЦІЙ У ДІЯЛЬНІСТЬ НАЦІОНАЛЬНОГО ОПЕРАТОРА ПОШТОВОГО ЗВ'ЯЗКУ З УРАХУВАННЯМ МІЖНАРОДНОГО ДОСВІДУ В УМОВАХ ЦИФРОВИХ ТРАНСФОРМАЦІЙ..... 377
Шейко І.А., Мартиненко М.С., Нєронов П.Є., Кузовкіна К.Р.
РИЗИКИ КІБЕРБЕЗПЕКИ ДЛЯ СУЧАСНОГО БІЗНЕСУ..... 389
Шейко І.А., Степаненко Р.Д., Батіг В.В.
РИЗИКИ ТА ЗАГРОЗИ ЕКОНОМІЧНІЙ БЕЗПЕЦІ ПІДПРИЄМСТВА В КОНТЕКСТІ ЦИФРОВОГО РОЗВИТКУ..... 399
Штанько В.І., Мартиненко М.С.
ФІЛОСОФСЬКЕ ОСМИСЛЕННЯ ЦІННОСТІ ПРАЦІ В УМОВАХ ЦИФРОВОЇ ЕКОНОМІКИ..... 412
Штанько В.І., Полозов О.Б., Галін П.К.
СОЦІАЛЬНІ ПРОБЛЕМИ ТА ЦИФРОВА ТРАНСФОРМАЦІЯ НА РИНКУ ПРАЦІ..... 420

artificial intelligence in the Google Advertising service. *Journal of Information Technology Management.* 2024. 16(4), 79-99. URL: https://doi.org/10.22059/jitm.2024.99052

5. Кайтановська О. Вплив цифровізації поштових послуг на структуру і зміст професійної компетентності операторів поштового зв'язку. *Вісник Черкаського національного університету імені Богдана Хмельницького. Серія: «Педагогічні науки»*. 2023. Вип. 4. С. 162-70. URL: https://doi.org/10.31651/2524-2660-2023-4-162-170 (дата звернення: 05.12.2024).

6. Горбаньова В. О. Вплив цифрової трансформації бізнесу на механізми корпоративного управління. *Український економічний часопис*. 2024. Вип. 4. С. 5-10.

7. Мельник Л., Карінцева О., Калініченко Л., Харченко М., Тарасенко С. Цифрова трансформація бізнес-процесів в Україні: кращі практики вітчизняного бізнесу та сучасні виклики. *Mechanism of an economic regulation*. 2024. 2(104). С. 54-60.

8. Мельничук Г. С., Марченко О. І. Окремі аспекти цифровізації бізнес-процесів підприємства в сучасних умовах. *Збірник наукових праць Державного податкового університету*. 2021. Вип. 1. С. 169-185.

9. Васильєва Н., Нижниченко Я., Заболотна О. Вплив цифровізації на трансформацію бізнес-моделей у традиційних галузях економіки. *Академічні візії*. 2024. № 37. С. 1-9. URL: https://www.academy-vision.org/index.php/av/article/view/1497/1373 (дата звернення: 08.12.2024).

10. Butcher L. Postal services adapt to changing demands due to Covid-19. URL: https://www.parcelandpostaltechnologyinternational.com/features/postal-services-adapt-tochanging-demands-due-to-covid-19.html (дата звернення: 10.12.2024).

11. The essential role of European Postal Operators during the COVID-19 pandemic. URL:https://www.posteurop.org/showNews?selectedEventId=37262. (дата звернення: 010.12.2024).

DOI: https://doi.org/10.30837/EK.2024.033

Шейко І.А.,
к.е.н., доцент, доцент кафедри економічної кібернетики та управління економічною безпекою,
Харківський національний університет радіоелектроніки,
ORCID: https://orcid.org/0000-0002-5770-3677
Мартиненко М.С.,
здобувач вищої освіти,
Харківський національний університет радіоелектроніки
ORCID: https://orcid.org/0009-0002-8926-2703
Нєронов П.Є.,
здобувач вищої освіти,
Харківський національний університет радіоелектроніки
ORCID: https://orcid.org/0009-0003-7597-1346
Кузовкіна К.Р.,
здобувач вищої освіти,
Харківський національний університет радіоелектроніки
ORCID: https://orcid.org/0009-0001-8097-3907

РИЗИКИ КІБЕРБЕЗПЕКИ ДЛЯ СУЧАСНОГО БІЗНЕСУ

З розвитком цифрового ландшафту організації стикаються з дедалі складнішими проблемами щодо захисту своїх активів від складних кіберзагроз. Інтеграція цифрових технологій у стратегії кібербезпеки стала ключовою для пом'якшення цих ризиків. Наслідки кібератак можуть бути катастрофічними: від фінансових втрат до втрати репутації,. Тому, ефективна протидія кіберзагрозам є одним з ключових завдань для забезпечення безперебійної роботи бізнесу.

Згідно зі звітами Європейського Агентства з кібербезпеки (ENISA) [1], найбільш поширеними інцидентами кібербезпеки у країнах Європейського Союзу з червня 2023 по липень 2024 стали (рис. 1):

– відмова у доступі (DoS/DDoS – атаки);

– програми вимагачі;

– витік даних та інциденти втрати конфіденційності;

– загрози соціальної інженерії (провокування персоналу компаній на дії, що сприяють порушенню кібербезпеки);

– шкідливе програмне забезпечення.

Рисунок 1 – Найбільш розповсюджені типи кібератак у країнах ЄС з червня 2023 р. по липень 2024 [1]

За аналізований період щомісячна кількість зафіксованих інцидентів кібербезпеки у країнах ЄС змінювалася від 250 до 700 інцидентів (рис. 2) [1].

У звіті ENISA також визначено чотири різних типів мотивації, які можна пов'язати з суб'єктами загрози [1]:

– фінансова вигода: будь-яка фінансово пов'язана дія (здійснюється здебільшого групами кіберзлочинців);

– шпигунство: отримання інформації про ІВ (інтелектуальну власність), конфіденційні дані, секретні дані (здебільшого здійснюється групами, спонсорованими державою);

– знищення: будь-яка руйнівна дія, яка може мати незворотні наслідки;

– ідеологічні: будь-яка дія, підкріплена ідеологією, що стоїть за нею (наприклад, хактивізм).

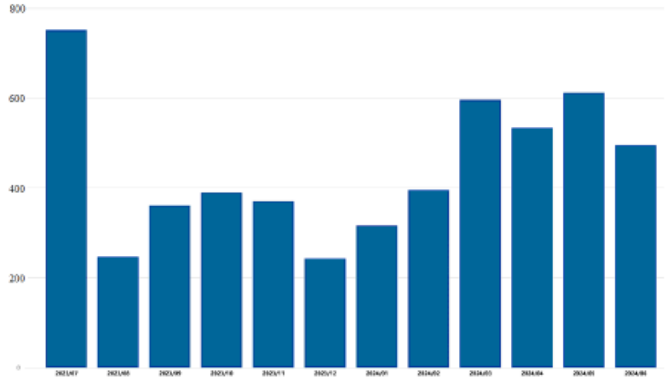


Рисунок 2 – Кількість інцидентів кібербезпеки у країнах ЄС за липень 2023-червень 2024 [1]

У більшості випадків основні загрози можна віднести до однієї або кількох мотивацій, причому певні мотиви виявляються більш домінуючими, ніж інші. Як і у випадку з попередньою ітерацією у сфері атак програм-вимагачів, хоча основною мотивацією зазвичай є фінансова вигода, є невеликий відсоток випадків, коли руйнівний мотив також відіграє певну роль. Крім того, більшість загроз, пов'язаних із даними, були пов'язані з кількома мотиваціями, головною причиною

яких була фінансова вигода. Ідеологія та шпигунство також відігравали значну роль, оскільки зловмисники прагнули просувати конкретні плани або викрадати стратегічну інформацію. Це підкреслює різноманітні мотиви, що стоять за кіберзагрозами, починаючи від фінансових стимулів і закінчуючи ідеологічними цілями та цілями збору розвідувальної інформації [1].

Для ефективної протидії кіберзагрозам компанії повинні впроваджувати комплексний підхід, який включає:

– *технічні засоби захисту*: антивірусні програми, системи виявлення вторгнень, шифрування даних тощо;

– *організаційні заходи*: розробка політик безпеки, проведення регулярних тренінгів для співробітників, створення резервних копій даних;

– *інженерія безпеки*: вбудовування безпеки в усі аспекти розробки програмного забезпечення.

Сучасні цифрові пристрої вразливі до кібератак. Особливо це стосується пристроїв Інтернету речей. Інтернет речей (IoT) – це революційна концепція, яка об'єднує фізичні пристрої, програмне забезпечення, датчики, актуатори та мережі, дозволяючи їм збирати та обмінюватися даними. Хоча IoT відкриває безліч нових можливостей, він також створює значні ризики для кібербезпеки.

До причин вразливості IoT до кібератак можна віднести [2]:

– *величезну кількість пристроїв:* зростання кількості підключених пристроїв створює величезну атакуючу поверхню, що ускладнює захист всієї мережі;

– *слабка безпека:* багато IoT-пристроїв мають слабкі або відсутні механізми безпеки, такі як застаріле програмне забезпечення, стандартні паролі та відсутність шифрування. Багато IoT-пристроїв або не використовують шифрування взагалі, або використовують слабкі алгоритми шифрування, що робить дані, які передаються між пристроями, вразливими для перехоплення та

дешифрування. Крім того, заводські налаштування з використанням стандартних і легко здогаданих паролів є поширеною проблемою в IoT-пристроях. Це дозволяє хакерам легко отримати доступ до пристрою;

– *децентралізацію управління:* різноманітність IoT-пристроїв ускладнює їх централізоване управління та оновлення Багато виробників IoT-пристроїв не забезпечують регулярних оновлень програмного забезпечення для усунення виявлених вразливостей, що робить пристрої вразливими до відомих атак;

– *вразливі протоколи:* Для забезпечення низького енергоспоживання та мінімальних обчислювальних ресурсів, IoT-пристрої часто використовують спрощені протоколи, які можуть мати менший рівень безпеки порівняно зі складнішими протоколами, що використовуються в традиційних комп'ютерних мережах.

Зловмисники можуть отримати несанкціонований доступ до пристроїв IoT і використовувати їх для різних цілей, таких як збір даних, відмова в обслуговуванні або навіть фізичний контроль над пристроєм. Типові загрози для мереж Інтернету речей можна поділити на такі типи [2-4]:

– *дистанційне управління:* зловмисники можуть отримати дистанційний доступ до пристроїв і використовувати їх для своїх цілей;

– *витік даних:* конфіденційні дані, зібрані IoT-пристроями, можуть бути викрадені. Вразливі IoT-пристрої можуть бути використані для збору приватної інформації про користувачів і її подальшого використання в злочинних цілях;

– *відмова в обслуговуванні (DOS/DDOS-атаки):* зловмисники можуть перевантажити мережу або пристрої, що призведе до відмови в обслуговуванні;

– *ботанети:* зламані IoT-пристрої можуть бути об'єднані в ботанети для проведення масштабних кібератак. Вразливі IoT-пристрої можуть бути використані як плацдарм для розповсюдження шкідливого програмного забезпечення в інші частини мережі;

– *фізичний доступ:* у деяких випадках зловмисники можуть отримати фізичний доступ до пристроїв і модифікувати їх програмне забезпечення.

Я наслідки кібератак на IoT компанії можуть понести матеріальні збитки (через фізичних пошкоджень обладнання та інфраструктури), фінансові втрати (дія програм-вимагачів, витік конфіденційних даних), втрату репутації компанії та соціальні наслідки у разі порушення критичної інфраструктури.

Для захисту мереж Інтернету речей стануть у нагоді такі дії [2-4]:

– *оновлення програмного забезпечення:* регулярне оновлення програмного забезпечення всіх IoT-пристроїв усуває вже виявлені вразливості;

– *сильні паролі:* використання складних, унікальних паролей для кожного пристрою знизить вірогідність інцидентів кібербезпеки.

– *шифрування:* обов'язкове шифрування даних, що передаються між пристроями.

– *сегментація мережі:* можна створити окрему мережу для IoT-пристроїв, щоб обмежити потенційну шкоду в разі зараження або розділити IoT-мережу на сегменти для обмеження поширення зловмисного програмного забезпечення.

– *моніторинг мережі:* регулярний моніторинг мережі на предмет підозрілої активності дозволить виявити зовнішнє втручання.

– *навчання персоналу:* навчання персоналу основам захисту даних, створенню безпечних паролей, роботи з конфіденційною інформацією знизить вірогідність людської помилки;

– *співпраця між компаніями та урядами:* компанії та урядові організації почали тісніше співпрацювати для обміну інформацією про загрози та розробки спільних стратегій захисту.

Як приклад однієї із успішних кібератак на пристрої Інтернету речей можна виділити Mirai. Mirai – це масштабна атака, здійснена за допомогою ботнету Mirai, який вперше з'явився у 2016 році. Mirai орієнтований на пристрої Інтернету речей

(IoT), такі як камери спостереження, роутери, тощо. Він використовує слабкі місця в захисті цих пристроїв, зокрема стандартні паролі та некоректно налаштовані системи. Mirai сканує мережі на наявність пристроїв IoT, використовуючи відомі облікові дані для входу. Після зламу пристрій стає частиною ботнету та використовується для запуску DDoS-атак (розподілених атак на відмову в обслуговуванні). У жовтні 2016 року Mirai був використаний для DDoS-атаки на DNS-провайдера Dyn. В результаті низка великих вебсайтів, включаючи Twitter, Netflix, і Spotify, стали недоступними [3].

Mirai став небезпечним прецедентом, продемонструвавши, наскільки вразливі пристрої IoT. Розробників Mirai затримали в 2017 році, але код ботнету був викладений у відкритий доступ, що призвело до появи численних його модифікацій. Постраждали не тільки компанії, а й кінцеві користувачі через порушення сервісів та зловживання ресурсами пристроїв.

У 2013 році хакери успішно зламали мережу Target і викрали інформацію про кредитні картки з мільйонів транзакцій. Вони вкрали облікові дані для входу у постачальника HVAC, який використовував датчики IoT, щоб допомогти Target контролювати споживання енергії та підвищувати ефективність своїх систем [4].

У 2017 році управління США з харчових продуктів та ліків (FDA) оголосило, що понад 465 000 імплантованих кардіостимуляторів були вразливі до зламу. Контролюючи один із цих пристроїв, хакер міг би буквально вбити когось, розрядивши батарею, змінивши частоту серцевих скорочень або застосувавши електрошок. Порушення безпеки IoT фактично перетворило рятівний пристрій на потенційно смертоносну зброю [4].

У 2015 році пара експертів з кібербезпеки вирішила зламати новенький Jeep Grand Cherokee за допомогою його мультимедійної системи. Вони були успішними. І вони продемонстрували, що вони можуть використовувати мультимедійну систему для підключення до іншого програмного забезпечення в

автомобілі, перепрограмувати його, а потім керувати двигуном, кермом, гальмами, трансмісією тощо. В епоху безпілотних автомобілів ця демонстрація є наполегливим нагадуванням про те, що ізоляція підключених пристроїв є ключовим компонентом безпеки Інтернету речей [4].

На захисті цифрових пристрої від кібератак можуть стати самі цифрові технології. У нашому дослідженні досліджується використання передових цифрових технологій (таких як штучний інтелект (AI), системи моніторингу в реальному часі та платформи мережевої безпеки) задля підсилення кібербезпеки.

Технології штучного інтелекту та машинного навчання (ML) радикально змінили виявлення та запобігання кіберзагрозам. Ці технології дозволяють організаціям аналізувати великі обсяги даних, виявляти закономірності та аномалії, що вказують на потенційні порушення. Наприклад, фінтех-компанії використовують інструменти на основі ШІ для покращення виявлення шахрайства та оцінки ризиків. Наприклад, Humanize, американський стартап із кібербезпеки, використовує штучний інтелект для кількісної оцінки кіберризиків, оцінки вразливостей і надання дієвих стратегій виправлення. Такі інструменти не тільки спрощують ідентифікацію загроз, але й оптимізують розподіл ресурсів для пом'якшення критичних ризиків [5].

Моніторинг у реальному часі став ключовим інструментом захисту критичної інфраструктури. В енергетичному секторі прикладом цього підходу є ініціатива Міністерства енергетики США «Охоронець сусідства». Завдяки застосуванню технології, яка забезпечує майже миттєву видимість електричних мереж, програма покращила моніторинг системи з 5% до 70%. Розвідувальні дані про загрози, які анонімно передаються зацікавленим сторонам, покращують механізми колективного захисту, забезпечуючи швидке реагування на кібератаки [5].

Платформи мережевої безпеки відіграють важливу роль у захисті систем зв'язку та операційних технологій. Канадський стартап CCX Technologies

розробив «SystemX», платформу кібербезпеки для військових і аерокосмічних програм. Він включає системи виявлення та запобігання вторгненням, які захищають військові мережі зв'язку на повітряних, наземних і морських транспортних засобах [5].

Механізми шифрування та захисту даних широко використовуються для захисту конфіденційної інформації від несанкціонованого доступу. Галузі роздрібної торгівлі та охорони здоров'я значною мірою покладаються на ці технології для захисту даних клієнтів і пацієнтів відповідно. Heal Security, платформа кібербезпеки для охорони здоров'я, усуває ризики, пов'язані з витоком даних і зломом медичних пристроїв, шляхом постійного моніторингу та аналізу загроз у реальному часі. Ці заходи підвищують довіру та забезпечують дотримання суворих правил захисту даних. [5]

Ці приклади підкреслюють інтеграцію передових технологій, таких як штучний інтелект, моніторинг у реальному часі та безпека мережі в різних галузях для ефективної боротьби з кіберзагрозами.

Але у звіті Deloitte також зазначено декілька проблем щодо використання цифрових технологій, які можуть збільшити онлайн-ризики [6]:

– через велику кількість цифрових пристроїв важко захистити всі від кібератак;

– конвергенція цифрового та фізичного світу робить наслідки кібератак важче передбачуваними з більшою потенційною шкодою від атак.

Критичний характер цифрової інфраструктури робить її мішенню для кіберзлочинців, які бачать, що її власники готові заплатити викуп, щоб уникнути дешифрування [6].

Незважаючи на свою ефективність, цифрові технології стикаються з обмеженнями у вирішенні динамічної природи кіберзагроз. Зловмисники постійно адаптують свою тактику, що вимагає постійних інновацій у інструментах

кібербезпеки. Інтеграція цифрових технологій у стратегії кібербезпеки є значним прогресом у боротьбі з кібератаками. Штучний інтелект, моніторинг у реальному часі, безпека мережі та технології шифрування відіграють важливу роль у зниженні ризиків у різних секторах. Оскільки кіберзагрози продовжують розвиватися, постійні інновації та співпраця мають вирішальне значення для забезпечення надійних та адаптивних структур кібербезпеки.

Перелік джерел посилань

1. European Union Agency for Cybersecurity (ENISA). Threat Landscape 2024. September, 2024. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

2. Lee I. Internet of Things (IoT) Cybersecurity: Literature Review and IoT Cyber Risk Management. *Future Internet*. 2020. № 12. p. 157.

3. Radanliev P., De Roure D. C., Maple, C., Nurse J. R., Nicolescu R., Ani U. Cyber Risk in IoT Systems. *Preprints*. 2019. 2019030104. https://doi.org/10.20944/preprints201903.0104.v1

4. Henke C. What is IoT security? Risks, examples and solutions. *Emnify*. 24 February, 2023. URL: http://surl.li/vvqoyv.

5. Startus. 10 Prominent Cybersecurity Examples in 2024. URL: https://www.startus-insights.com/innovators-guide/cybersecurity-examples/

6. Deloitte Insights. Incentives are key to breaking the cycle of cyberattacks on critical infrastructure. 08 March 2022. URL: https://www2.deloitte.com/us/en/insights/industry/public-sector/cyberattack-critical-infrastructure-cybersecurity.html.

DOI: https://doi.org/10.30837/ЕК.2024.034

Шейко І.А.,
к.е.н., доцент, доцент кафедри економічної кібернетики та управління економічною безпекою,
Харківський національний університет радіоелектроніки,
ORCID: https://orcid.org/0000-0002-5770-3677
Степаненко Р.Д.,
здобувач вищої освіти,
Харківський національний університет радіоелектроніки
ORCID: https://orcid.org/0009-0008-0586-0903
Батіг В.В.,
здобувач вищої освіти,
Харківський національний університет радіоелектроніки
ORCID: https://orcid.org/0009-0007-3883-3648

РИЗИКИ ТА ЗАГРОЗИ ЕКОНОМІЧНІЙ БЕЗПЕЦІ ПІДПРИЄМСТВА В КОНТЕКСТІ ЦИФРОВОГО РОЗВИТКУ

Організації в усіх галузях все більше покладаються на цифрові технології для виконання роботи. Зрештою, ці нові технології – штучний інтелект та машинне навчання, Інтернет речей, хмарні обчислення, максимізують швидкість, гнучкість, ефективність і прибутковість для організацій, які їх використовують [1]. Незалежно від того, чи має на меті компанія оптимізувати свою діяльність, прийняти нові бізнес-моделі чи покращити взаємодію з клієнтами, це часто є рушійною силою, що стоїть за рішенням організації прийняти нові цифрові ініціативи [2].

Оскільки технології все більше інтегруються в усі аспекти бізнесу, цифровий ризик стає все більшою проблемою для компаній у всьому світі. Він

Наукове видання

СТАЛИЙ ЕКОНОМІЧНИЙ РОЗВИТОК: ІННОВАЦІЙНІ ПІДХОДИ ТА СТРАТЕГІЧНІ ПЕРСПЕКТИВИ

Колективна монографія

За загальною редакцією
доктора економічних наук, професора Т.В. Полозової

Редактор
кандидат економічних наук, доцент О.В. Мурзабулатова

Комп'ютерна верстка – Мурзабулатова О.В.

Матеріали збірника публікуються в авторському варіанті

Файл надано:
Харківський національний університет радіоелектроніки,
Кафедра економічної кібернетики та управління економічною безпекою,
61166, Україна, м. Харків, пр. Науки, 14,
тел. (057) 702-14-90,
e-mail: sser.conf@gmail.com

Підп. до друку 25.12.2024. Формат 60x84 1/16.
Друк цифровий. Ум. друк. арк. 25,11.
Тираж 100 прим. Ціна договірна.

Віддруковано в типографії ФОП Андреєв К.В.
61166, Харків, вул. Богомольця, 9, кв. 50.
Свідоцтво про державну реєстрацію
№ 24800170000045020 від 30.05.2003.
ep.zakaz@gmail.com
тел. 063-993-62-73