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)

ЗМІСТ

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

проєкти мають сприяти створенню нових продуктів або технологій, які можуть бути конкурентоспроможними на цих ринках. Крім того, інновації мають бути інтегровані у виробничі процеси для підвищення ефективності та зменшення витрат. Оцінка інноваційних проєктів повинна враховувати їхню здатність підтримувати зростання ринкової частки, підвищувати продуктивність або відкривати нові джерела доходу.

Оцінка ефективності інноваційно-інвестиційних проєктів є необхідною складовою для прийняття обґрунтованих управлінських рішень у контексті стратегічного розвитку підприємства. Така оцінка має бути комплексною, включаючи фінансові, стратегічні та ризикові аспекти. Підприємства, які ефективно оцінюють свої інноваційні проєкти, можуть краще адаптуватися до змін ринкових умов, оптимізувати внутрішні процеси та підвищити свою конкурентоспроможність.

Таким чином, оцінка ефективності інноваційно-інвестиційних проєктів є стратегічним інструментом, який дозволяє підприємствам орієнтуватися на довгострокові цілі, досягати фінансової стабільності та успішно впроваджувати інновації в умовах мінливого ринкового середовища.

Перелік джерел посилання

1. Микитюк П., Микитюк Ю., Завитій Я. Дослідження концепції організації проєктування та оцінка факторів формування економічної ефективності інвестиційних проектів. *Вісник економіки*. 2022. Вип. 3. С. 169-182.

2. Гумега В. В. Фактор ризику і невизначеності при оцінці ефективності інвестиційних проектів. *Міжнародний науковий журнал «Інтернаука»*. 2021. № 4. С. 22-26.

3. Швед В. В., Горобець А. П. Стратегія розвитку підприємства: сутність та значення. *Науковий вісник Херсонського державного університету. Серія: Економічні науки*. 2023. Вип. 49. С. 36-43.

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
Кузовкіна К.Р.,
здобувач вищої освіти,
Харківський національний університет радіоелектроніки
ORCID: https://orcid.org/0009-0001-8097-3907

РИЗИКИ ТА ЗАГРОЗИ ЕКОНОМІЧНІЙ БЕЗПЕЦІ ПІДПРИЄМСТВА В КОНТЕКСТІ ЦИФРОВОГО РОЗВИТКУ

Цифровізація економіки відкриває значні можливості для зростання та інновацій, але також створює нові ризики та загрози для економічної безпеки. Основними викликами у цифрову епоху є кіберзлочинність, технологічна залежність, порушення конфіденційності даних та соціально-економічна нерівність.

Кіберзлочинність стала одним із найсерйозніших ризиків для бізнесу та держав. Атаки на фінансові установи, викрадення даних і збої в роботі критичних інфраструктур можуть призвести до значних економічних втрат і зниження довіри до цифрових систем. Зокрема, збільшення кількості атак програм-вимагачів і фішингових схем є прямою загрозою для компаній та громадян. За даними Європейського агентства з кібербезпеки ENISA, найбільш розповсюдженими типами кібератак з червня 2023 по липень 2024 стали

відмова у доступі (DoS/DDoS – атаки), програми вимагачі, витік даних, загрози соціальної інженерії (провокування персоналу компаній на дії, що сприяють порушенню кібербезпеки), шкідливе програмне забезпечення (рисунок 1) [1].

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

Кібератаки негативно впливають на діяльність усіх секторів економіки та суспільного життя, проте особливо активними стали кібератаки на такі сектори (рисунок 2) [1]: публічне управління, транспорт, банківській сектор, бізнес-послуги та цифрова інфраструктура.

Збереження конфіденційності даних у цифрову епоху стає все більш проблематичним. Витоки персональної та фінансової інформації можуть не лише завдати шкоди окремим користувачам, але й негативно впливати на національну безпеку. Так, за даними європейського агентства з кібербезпеки щомісяця викрадається понад 10 терабайт даних, програмне забезпечення-вимагач є однією з найбільших кіберзагроз у ЄС, а фішинг зараз визначено як найпоширеніший вихідний вектор таких атак. За оцінками, на кінець 2020 року річний збиток світової економіки від кіберзлочинності сягнув 5,5 трильйонів євро, що вдвічі перевищує показник 2015 року [2].

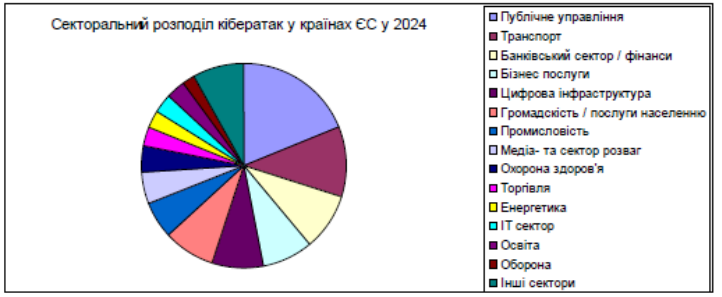


Рисунок 2 – Секторальний розподіл кібератак у країнах ЄС у 2024 р. [1]

Технологічна залежність також є суттєвим фактором ризику. Використання іноземного програмного забезпечення та обладнання без належного контролю може створювати вразливості для стратегічних галузей економіки. Крім того, швидкий розвиток технологій потребує постійних інвестицій, що ускладнює ситуацію для країн із обмеженими ресурсами.

Для мінімізації ризиків необхідно впроваджувати комплексні стратегії, що включають розвиток кібербезпеки, регулювання технологічного сектору та підтримку інновацій. Лише баланс між використанням цифрових можливостей та управлінням загрозами дозволить забезпечити стійку економічну безпеку у цифрову епоху.

Перелік джерел посилання

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

2. European Consil Top cyber threats in the EU. URL: https://www.consilium.europa.eu/en/infographics/cyber-threats-eu/.

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

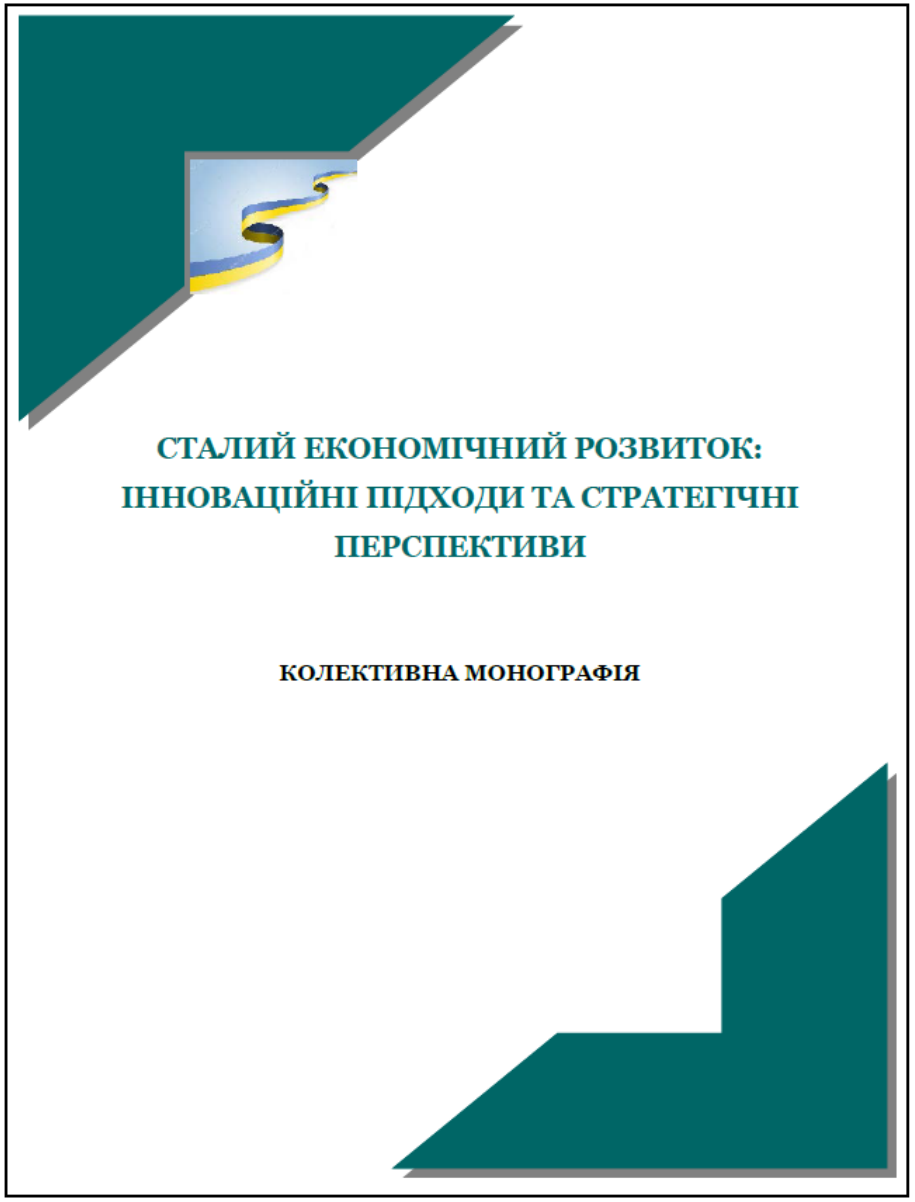
MODERN STRATEGIES OF ECONOMIC DEVELOPMENT: SCIENCE, INNOVATION AND BUSINESS EDUCATION

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

ЗМІСТ

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).

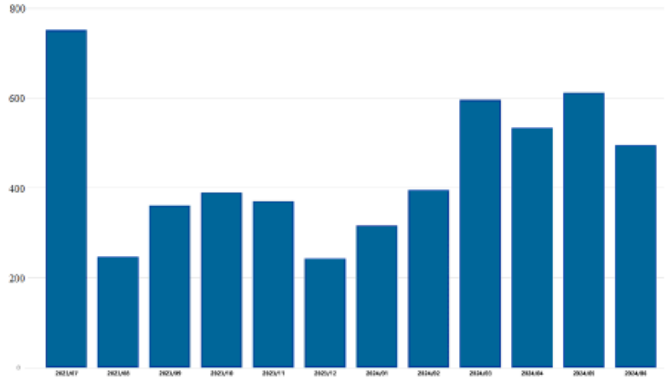


Рисунок 2 – Кількість інцидентів кібербезпеки у країнах ЄС за липень 2023-червень 2024 [1]

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

432