МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Сумський державний університет
Навчально-науковий інститут бізнесу, економіки та менеджменту

Цифрові трансформації та інноваційні технології в економіці: виклики, реалії, стратегії

Digital transformations and innovative technologies in the economy: challenges, realities, strategies

Матеріали
ІІІ Міжнародної науково-практичної конференції
(Україна, Суми, 27-29 травня 2024 р.)

Суми
Сумський державний університет
2024

УДК [330.34+330.336](063)
Е45

Рекомендовано вченою радою
Сумського державного університету
(протокол № 14 від 5 червня 2024 р.)

Е45 Цифрові трансформації та інноваційні технології в економіці: виклики, реалії, стратегії**:** матеріали III Міжнародної науково-практичної конференції «Цифрові трансформації та інноваційні технології в економіці: виклики, реалії, стратегії» (Суми, 27-29 травня 2024 р.) / за заг. ред.: Л. Л. Гриценко, І. В. Тютюник. Суми : Сумський державний університет, 2024. – 146 с.

Матеріали III Міжнародної науково-практичної конференції «Цифрові трансформації та інноваційні технології в економіці: виклики, реалії, стратегії» містять результати наукових досліджень присвячених пошуку системного вирішення мультидисциплінарних проблем в галузі електронного бізнесу і технологічних інновацій, цифрової трансформації освітніх систем, запровадження інноваційних технологій у фінансовому секторі.

Для науковців, науковців, студентів, аспірантів, представників бізнесу та громадських організацій і вищих навчальних закладів та широкого кола читачів.

The materials of the International scientific and practical conference "Digital transformations and innovative technologies in the economy:challenges, realities, strategies" provide the results of scientific research focused on the search for a systematic solution to multidisciplinary problems in the field of electronic business and technological innovations, digital transformation of educational systems, the introduction of innovative technologies in financial sector. .

For scientists, researchers, students, postgraduates, representatives of business and public organizations and higher education institutions and a wide range of readers.

УДК [330.34+330.336](063)

ЗМІСТ

Олена Журавка
Аліна Азарова
Антон Журавка
Основні проблеми розвитку ринку добровільного медичного страхування в Україні та шляхи їх вирішення..…….…..…… 6

Олена Криклій
Лілія Деркач
Нормативи капіталу банківського сектору України: аналіз та прогнозування……...…… 9

Олександра Тверезовська
Богдан Чернешенко
Маркетингові стратегії для поколінь Z: виклики та можливості…..……..…..……..…..…… 13

Тетяна Кубах
Артем Сергєєв
Дослідження сутності та актуальності категорії «ефективність банківської системи»….. ……. 17

Олена Журавка
Аліна Голик
Особливості формування та управління страховим портфелем страхової компанії…….. 21

Світлана Похилько
Людмила Рябушка
Богдан Ільченко
Роль місцевого самоврядування в підтримці бізнесу та стимулюванні ідприємництва в умовах воєнного стану……..……. 25

Аліна Бухтіарова
Дар'я Тимошик
Оцінка ефективності регуляторних змін у боротьбі з кіберзлочинністю: географічна і часова складові…….. 28

Андрій Раков
Верифікація та ідентифікація клієнтів при дистанційному банківському обслуговуванні…. 32

Олександра Тверезовська
Крістіна Попова
Вплив цифрової трансформації банківського маркетингу на приватних клієнтів банку..…… 36

Людмила Захаркіна
Юлія Швидка
Сучасні тенденції розвитку цифрових технологій у страхуванні ….…….…….. 40

Ганна Салтикова
Аліна Голик
Поняття інвестиційної привабливості та її оцінка на різних рівнях управління.…… 43

Олена Криклій
Людмила Рябушка
Андрій Придуха
Управління комплаєнс-ризиком банку……... 47

Євген Руденко
Використанні штучного інтелекту при оцінюванні стійкості фінансової системи…….. 50

Ганна Салтикова
Аліна Рубан Капітальні інвестиції в економіці України……. 54

Людмила Захаркіна
Катерина Сердюк Потенціал та виклики використання криптовалют у якості платіжних систем……. 57

Олександра Тверезовська
Ростислав Гончаренко Роль емоцій у банківському маркетингу: вплив на рішення клієнтів ……...…..……. 60

Liudmyla Riabushka
Danylo Salov The role of local budget in regional development.. 64

Олена Журавка
Аліна Рубан Фінансові ресурси страхових компаній…..……. 66

Ганна Салтикова
Людмила Сокол Політика капітальних вкладень та проблеми їх фінансування ...…….. 69

Євгенія Мордань
Крістіни Чередніченко Системний підхід у побудові механізм формування та реалізації кредитної політики банку…… 73

Дар'я Свірідова
Людмила Захаркіна
Владислав Батанін Фінансова діяльність підприємства: ключові аспекти…… 77

Олена Криклій
Людмила Рябушка
Ігор Придуха Механізм формування та реалізації кредитної політики банку……...……. 80

Olena Zhuravka
Viktoria Alekseieva Assessment of financial state of the state-owned enterprise……..…….…… 82

Liudmyla Riabushka
Vladyslav Fedchenko Financial sustainability of local budgets in the context of martial law…….. 85

Тетяна Кубах
Ганна Гребенюк Фінансова стійкість банку: сутність, види та фактори впливу…….. 87

Олена Журавка
Людмила Сокол Особливості забезпечення фінансової безпеки страхових компаній ……...…..…… 91

Олександра Тверезовська
Анастасія Федан
Уляна Вініченко Маркетингові аспекти впровадження fintech технологій в банківські послуги…..……. 95

Луїза Уніат
Людмила Захаркіна Аналіз фінансування та розвитку insurtech сектору: глобальні тенденції…… 99

Тетяна Касьяненко
Вікторія Данилова Теоретичні аспекти аналізу фінансової діяльності підприємства…… 102

Ганна Салтикова
Віра Бардакова Сучасний стан інвестиційного процесу та особливості його стимулювання……..…… 106

Larysa Hrytsenko
Oleksandra Tverezovska
Iryna Kozhushko Analysis of publication activity on the digitalization of banking marketing……..…….... 110

Denys Kolomiiets Integrating energy efficiency indicators into the financial analysis of enterprises..……..……..….. 114

Vladyslav Piven
Tetiana Kasianenko Blockchain technology for enhancing competitive advantage in financial services...……..……..…… 116

Євгеній Пігуль Вплив цифровізації у забезпеченні розвитку ринку праці……..…..…..……..…..…..……... 118

Світлана Похилько
Анна Приходько Вплив сучасного воєнного стану на розвиток цифрових процесів в економіці та бізнесі в Україні в 2024 році……..……..……..……..... 120

Наталія Пігуль
Аліна Медвідь Вплив цифровізації на розвиток банківського сектору України……...……..……..……..……. 123

Дмитро Ткаченко Напрямки удосконалення системи страхування вкладів в Україні: пройдений шлях та подальші кроки..……..……..……..……. 127

Тетяна Касьяненко
Ярина Шевченко Управління фінансовими ризиками на підприємстві в умовах війни……..…..……..... 132

Павло Рубанов
Вікторія Білошапка Підходи до формування і наслідки забезпечення цифрової транспарентності підприємств…… 136

Олександр Грищенко Вплив трудової міграції на конкурентоспроможність національної економіки України в умовах глобалізації…..…. 141

Євген Чванкін
Євген Рекун Діджиталізація громадського здоров'я як чинник забезпечення економічної безпеки держави……... 144

ОЦІНКА ЕФЕКТИВНОСТІ РЕГУЛЯТОРНИХ ЗМІН У БОРОТЬБІ З КІБЕРЗЛОЧИННІСТЮ: ГЕОГРАФІЧНА І ЧАСОВА СКЛАДОВІ

Бухтіарова Аліна Геннадіївна
к.е.н, докторантка
Сумський державний університет, Суми
Тимошик Дар'я Дмитрівна
аспірантка
Сумський державний університет, Суми

Стрімкий розвиток цифрових технологій призвів до кардинальної трансформації суспільних відносин у сфері економіки та бізнесу, забезпечення національної та особистої безпеки. Цифровізація економіки відкрила нові можливості для розвитку бізнесу, сприяла створенню нових моделей публічного та корпоративного управління, поліпшення якості життя суспільства. В той же час, дані процеси призвели до посилення ризиків протиправної діяльності, що пов'язані із використанням цифрових технологій.

Одним з найбільш динамічних викликів сучасності, що завдає суттєвих економічних і соціальних збитків є кіберзлочинність. Вона включає незаконне отримання доступу до даних, здійснення фінансових махінацій, атак на критичну інфраструктуру та розповсюдження шкідливого програмного забезпечення. Постійно зростаючі масштаби та динаміка кіберзлочинності спричиняють значні економічні збитки для суспільства та держави в цілому та створюють загрози для стабільного та сталого розвитку суспільства.

З метою мінімізації негативних наслідків активного запровадження цифрових технологій урядами різних країн здійснюється постійна розробка та впровадження комплексних регуляторних заходів, що охоплюють як законодавчі ініціативи в сфері протидії злочинності в цифровому просторі, так і встановлення стандартів та регламентів інформаційної безпеки, що забезпечує ефективний контроль за використанням інформаційних технологій. Ефективність таких заходів значною мірою визначається специфікою регіонального розвитку та адаптації нормативно-правового середовища до сучасних загроз, здатністю оперативно реагувати на зміну тактики кіберзлочинців. Оцінювання ефективності регуляторних змін у боротьбі з кіберзлочинністю через призму географічного та часового аспекту її розвитку є ключовим аспектом при розробленні стратегій цифрової безпеки, що здатні забезпечити стійкість національних та міжнародних інформаційних систем.

Однією зі специфічних особливостей, що визначають умови запровадження та використання інструментарію боротьби з кіберзлочинністю, є її географічна специфіка. Відмінність у цифровому розвитку та грамотності, правовому регулюванні та міжнародній співпраці у сфері кібербезпеки

формують різний рівень кіберзагроз в країнах. Так, наприклад, у розвинених країнах (США, Японія, країни ЄС) значна увага приділяється впровадженню жорстких регуляторних заходів та стандартів безпеки, що включають не лише законодавче регулювання, а й технологічні інновації, міжнародну співпрацю та активну взаємодію між державними і приватними структурами. У США діє Закон про боротьбу з кіберзлочинністю (CFAA), створена Національна стратегія кібербезпеки, а також розвинута співпраця між державними органами та приватними компаніями, що дозволяє швидко реагувати на кіберзагрози.

Натомість у країнах, що розвиваються, нестача кваліфікованих кадрів у сфері кібербезпеки та недостатній рівень фінансування призводять до появи проблем з впровадженням ефективних механізмів боротьби з кіберзлочинністю. Слабкий контроль, в свою чергу, призводить до того, що кіберзлочинці дедалі частіше починають використовувати ці регіони для здійснення кібератак. Наприклад, слабка правоохоронна система та нерозвинена цифрова інфраструктура у країнах Африки та Латинської Америки призводить до високого рівня кіберзлочинності в них. Дослідження показують, що у цих регіонах часто діють транснаціональні хакерські угруповання, які здійснюють фішингові атаки, розповсюджують шкідливе програмне забезпечення та займаються фінансовим шахрайством.

Одним із проявів географічного аспекту розвитку кіберзлочинності є її транснаціональний характер. Відсутність чітких територіальних меж і залучення міжнародних хакерських угруповань робить дану злочинність однією з ключових загроз сучасного світу. Дані угруповання атакують державні установи, корпорації та фінансові системи, використовуючи передові технології та різні методи обходу систем безпеки. Одним із прикладів є діяльність таких угруповань як REvil та Conti, які займаються розповсюдженням програм-вимагачів, атакуючи компанії та органи влади по всьому світу. Інша важлива проблема даного типу злочинності полягає у використанні країн із слабким кіберзахистом як плацдармів для проведення атак на глобальному рівні. Наприклад, у Латинській Америці та Південно-Східній Азії через недостатнє правове регулювання та низьку цифрову грамотність частішають випадки хостингу нелегальних серверів, що використовуються для атак на країни з високим рівнем кіберзахисту.

В Україні сучасний розвиток кіберзлочинності визначається специфікою розвитку країни в умовах військових дій. Державні установи, стратегічні підприємства та фінансовий сектор регулярно зазнають атак з боку російських хакерських груп, що використовують різні методи – від DDoS-атак до складних операцій із компрометації державних систем. За даними Державної служби спеціального зв'язку та захисту інформації України, кількість кібератак на критичну інфраструктуру країни значно зросла після 2022 року. У відповідь

Україна посилила свою кібербезпеку завдяки міжнародній співпраці, інтеграції стандартів НАТО та підтримці країн-партнерів, що дозволило підвищити рівень стійкості до загроз. Одним із важливих кроків стало створення Державної служби спеціального зв'язку та захисту інформації України, а також посилення кіберпідрозділів у Збройних силах та правоохоронних органах. Додатково було запроваджено посилений моніторинг державних та приватних систем, впроваджено національні протоколи реагування на кіберзагрози.

Не менша важливим аспектом з точки зору боротьби з кіберзагрозами слугує оцінка ефективності регуляторних заходів у динаміці. Як показує практика, ухвалення нових законів чи посилення вже наявних норм може надати позитивний, але зазвичай тимчасовий ефект. Зловмисники поступово адаптуються до нових вимог, знаходять нові шляхи та застосовують дедалі складніші технології для досягнення своїх цілей. Тому завдання держав та міжнародних організацій полягає не лише в розробці й ухваленні дієвих правил, а й у їхньому постійному оновленні та аналізі реальних результатів.

Подібний ефект спостерігався після впровадження Загального закону про захист персональних даних у Бразилії (LGPD). У перші місяці після набуття його чинності кількість витоків даних зменшилася, але через рік було зафіксовано новий сплеск атак. Його впровадження призвело до зростання відповідальності бізнесу і тимчасового зменшенню витоків даних. Компанії почали ретельніше ставитися до зберігання та обробки персональних даних, адже компанії, які не відповідали встановленим вимогам, були змушені сплачувати багатомільйонні штрафи, що слугувало ефективним та дієвим стимятором зростання обсягу інвестицій від бізнесу у вдосконалення систем кібербезпеки. Це сприяло тимчасовому зниженню рівня маніпулювання персональними даними. Однак згодом хакери змогли адаптувати свої методи, зокрема, шляхом більш частішого здійснення атак за допомогою методів соціальної інженерії (фішингові листи, телефонні дзвінки чи інші методи, спрямовані на витягнення конфіденційної інформації в обхід технічних систем безпеки) та шифрування з метою вимагання (блокування доступу до корпоративних чи особистих даних, вимагання викупу в криптовалюті) тощо. Це свідчить про необхідність постійного вдосконалення правового регулювання та адаптації до нових загроз.

У США після прийняття Закону про боротьбу з кіберзлочинністю (CFAA) також супроводжувалося зниженням рівня фінансового шахрайства в інтернеті. Проте, з розвитком технологій злочинці почали використовувати блокчейн та криптовалюти для анонімізації транзакцій, що ускладнило правоохоронним органам відстеження незаконних фінансових потоків. Це змусило уряд США посилити контроль за криптовалютними біржами, запровадивши нові регулювання у сфері фінансового моніторингу.

В цілому, більшість науковців визнають, що головною проблемою запровадження регуляторних змін у сфері боротьби з кіберзлочинністю є їхній відкладений ефект. Нові норми починають діяти не одразу, а процес адаптації може тривати роками. Окрім того, злочинці знаходять нові методи обходу регуляцій, що потребує оперативного оновлення правового поля. До основних викликів адаптації регуляторних норм належать: глобалізаційний характер кіберзлочинності (міжнародні хакерські угруповання можуть діяти у юрисдикціях, де відсутні жорсткі регуляторні вимоги), відсутність гармонізації регуляцій (різні країни мають власні підходи до кібербезпеки, що ускладнює міжнародне співробітництво у цій сфері), зміна методів атак (зловмисники швидко адаптуються до нових умов, використовуючи штучний інтелект, автоматизовані боти та інші сучасні технології), недостатнє фінансування кібербезпеки (у країнах, що розвиваються, брак ресурсів ускладнює впровадження ефективних заходів захисту).

Таким чином, ефективне регулювання кіберзлочинності є безперервним процесом, а боротьба з кіберзлочинністю вимагає динамічного, багатоаспектного підходу, де ключову роль відіграють як державні ініціативи, так і співпраця з приватним сектором та міжнародними організаціями. Постійний моніторинг кіберзагроз, впровадження новітніх технологічних рішень, обмін інформацією між державами та організаціями відіграють вирішальну роль у стримуванні кіберзлочинності. Крім того, необхідно посилювати рівень обізнаності населення щодо безпеки в цифровому просторі, адже людський фактор залишається одним із найслабших елементів у боротьбі з кіберзагрозами. Розвиток технологій штучного інтелекту та машинного навчання відкриває нові можливості для протидії злочинцям, водночас створюючи нові виклики для законодавців і регуляторних органів, які мають адаптувати нормативну базу до сучасних умов цифрової безпеки.

Робота виконана в рамках науково-дослідної роботи «Моделювання механізмів протидії організованій та транснаціональній кіберзлочинності у воєнний та післявоєнний часи» (№ д/р 0124U000550).