DOI: https://doi.org/10.32782/2524-0072/2024-69-114

УДК 330.131.7

ЛАТЕНТНІ ВПЛИВИ КІБЕРЗЛОЧИНІВ, КОРУПЦІЇ ТА ОПЕРАЦІЙ ТІНЬОВОЇ ЕКОНОМІКИ НА ДІЯЛЬНІСТЬ СУБ'ЄКТІВ ЕКОНОМІКИ: АНАЛІЗ ТЕОРІЇ ТА ПРАКТИКИ[1]

LATENT INFLUENCES OF CYBERCRIMES, CORRUPTION AND SHADOW ECONOMY OPERATIONS ON THE ACTIVITIES OF ECONOMIC ENTITIES: ANALYSIS OF THEORY AND PRACTICE

Яровенко Ганна Миколаївна
доктор економічних наук, доцент,
Сумський державний університет
OPCID: https://orcid.org/0000-0002-8760-6835

Yarovenko Hanna
Sumy State University

У статті проаналізовано латентні впливи незаконних практик – кіберзлочинів, корупції та операцій тіньового сектору – на діяльність суб'єктів економіки. Використовуючи дані бази Scopus та програмний додаток VOSviewer, виявлено п'ять кластерів ключових слів, які ідентифікують теоретичні напрями досліджень. Червоний кластер акцентує увагу на кіберзлочинах, штучному інтелекті та мережевій безпеці, підкреслюючи роль сучасних технологій у захисті бізнесу. Зелений охоплює тіньову економіку, висвітлюючи її вплив на економічний розвиток. Синя група зосереджується на прозорості, боротьбі з корупцією та якості управління. Жовтий і бузковий кластери розглядають етику, гендерні аспекти, цифровізацію та вплив пандемії. Аналіз практики показав реальні наслідки кібератак (Colonial Pipeline, Garmin, Maersk), корупційних скандалів (Petrobras, Siemens, Odebrecht) та криз, спричинених тіньовою економікою (HSBC, Volkswagen). Окреслено наслідки незаконних практик для України: кібератаки на державні й приватні установи демонструють уразливість цифрової інфраструктури; корупційні схеми, як-от ухиляння від мобілізації, підривають довіру до держави; тіньова економіка створює виклики для бізнесу, вимагаючи нових стратегій та регуляції. Результати аналізу теорії та практики підкреслюють актуальність боротьби з цими явищами для формування стійкого бізнес-середовища в країні.

Ключові слова: корупція, кіберзлочин, тіньова економіка, бізнес, латентний вплив.

This study delves into the latent effects of illegal practices – cybercrime, corruption, and shadow economy operations - on the activities of economic entities. To analyse its theoretical aspects, a dataset of scientific publications indexed in the Scopus database was selected based on keywords such as "cybercrime," "corruption," "shadow economy," "business," and "latent." They were analysed and visualised using the VOSviewer software. The result showed five thematic clusters defining the primary research directions concerning the impact of illegal practices. The red group emphasises digital technologies, cybersecurity, artificial intelligence, data analytics, and network security. The green one is centred on economic growth, resilience, shadow economy, and taxation, stressing the need to examine illegal economic processes and their implications for macroeconomic indicators and public policy efficiency. The blue cluster addresses transparency, anti-corruption measures, institutional quality, and public governance, showcasing the importance of institutional capacity-building for fostering trust and accountability in both public and private sectors. Meanwhile, the yellow and purple groups explore secondary topics, including gender aspects, ethics, public policy, e-governance, entrepreneurship, and the human and social implications of COVID-19. The theoretical findings underline the interconnected nature of corruption, cyber threats, and shadow economy practices, demonstrating their cumulative effect. Corruption undermines trust, distorts market mechanisms, and exacerbates economic inefficiencies, as evidenced by high-profile scandals like the Petrobras case in Brazil and Siemens'

[1] Робота виконана в рамках науково-дослідної роботи № 0124U000544 «Кібербезпекові та цифрові трансформації економіки країни воєнного часу: боротьба із кіберзлочинами, корупцією та тіньовим сектором».

bribery revelations. Shadow economy practices, such as tax evasion, further erode public policy efficiency and diminish state revenues. Concurrently, cyber threats, exemplified by ransomware attacks on Colonial Pipeline and Garmin or large-scale data breaches affecting companies like Target, disrupt digital infrastructure and necessitate the adoption of innovative cybersecurity strategies. The analysis also highlights regional case studies, such as Ukraine's cyberattacks on critical infrastructure and government systems, revealing vulnerabilities in national and business security frameworks. Additionally, corruption and shadow economy practices in Ukraine remain substantial barriers to business growth, evidenced by the exposure of systemic bribery schemes and judicial inefficiencies. This research contributes to understanding the latent dimensions of illegal practices, offering actionable insights for policymakers and business leaders to address the multidimensional challenges posed by corruption, cybercrime, and the shadow economy.

Keywords: corruption, cybercrime, shadow economy, business, latent influence.

Постановка проблеми. У сучасних умовах цифровізації економіки суб'єкти господарювання стикаються з численними викликами, які впливають на їхню діяльність. Серед них особливе місце займають кіберзлочини, корупція та операції тіньового сектору. Ці форми незаконної діяльності мають значний вплив через свою латентність, що суттєво ускладнює їхнє виявлення і протидію. Незважаючи на наявність інших явних економічних і соціальних факторів, які впливають на бізнес, таких як макроекономічна та політична нестабільність, регуляторний тиск чи ринкові коливання, саме латентні незаконні практики завдають прихованого, але водночас глибокого руйнівного ефекту.

Кіберзлочини стали проблемою номер один для бізнесу в умовах COVID-19 та після пандемії. Їх вплив проявляється у фінансових витратах, пов'язаних з відновленням зламаних систем та баз даних, втратою довіри клієнтів через компрометацію конфіденційних даних, а також у штрафах за недотримання регуляторних вимог у сфері захисту інформації. Хакерські атаки, цифровий шантаж та викрадення даних дедалі частіше стають інструментами дестабілізації бізнесу, вплив яких важко передбачити.

Корупція є ще одним критичним фактором, що спотворює економічну діяльність. Використання владних повноважень для особистого збагачення створює нерівні умови для учасників ринку, підвищує транзакційні витрати та негативно впливає на конкурентоспроможність бізнесу. Невидимість корупційних схем і складність у доведенні фактів зловживань лише посилюють їхній руйнівний вплив, підриваючи довіру інвесторів і партнерів до місцевих ринків.

Тіньова економіка, яка включає нелегальну торгівлю, ухилення від сплати податків та інші незаконні операції, також створює значні перешкоди для розвитку бізнесу. Компанії, що діють легально, змушені конкурувати з учасниками ринку, які використовують непрозорі методи зниження витрат, що унеможливлює чесну конкуренцію. Збитки, які завдаються державному бюджету внаслідок тіньових операцій, не лише підривають економіку, але й посилюють фінансовий тиск на бізнес через збільшення податкового навантаження.

Таким чином, перелічені форми незаконної діяльності мають прихований характер впливу на бізнес середовище, що ускладнює їх своєчасне виявлення. Їх латентність проявляється у складності їх діагностики на початкових етапах, непрямій природі наслідків та відсутності очевидної кореляції з негайними результатами діяльності бізнесу. Як наслідок, їхній вплив може стати помітним лише тоді, коли завдані збитки набувають системного характеру, завдаючи значної шкоди бізнесу та економіці в цілому.

Аналіз останніх досліджень і публікацій. Проблематика корупції, кіберзлочинів та операцій тіньового сектору є актуальною в контексті вирішення даних проблем для формування сприятливого інвестиційного клімату, підвищення рівня конкурентоздатності бізнесу та покращення економічного розвитку країни. Саме тому, ці питання активно досліджуються провідними фахівцями-теоретиками та практиками в науковій літературі.

Так, найбільший внесок у дослідження питань тіньової економіки зробили Фрідріх Шнайдер та Домінік Х. Енсте, які мають значний науковий доробок у даній сфері. Слід відмітити їх найбільш популярну працю, в якій вони оцінили розмір тіньової економіки в 76 країнах, що розвиваються, з перехідною економікою та ОЕСР [1]. Алм Дж. та Ембай А. у своїх дослідженнях пішли далі та оцінили розміри тіньової економіки для 111 країн за 1984–2006 роки на основі підходу попиту на валюту [2]. Також дослідження поєднуються для виявлення зв'язків між тіньовим сектором та корупцією. Дрегер А. та Шнайдер Ф. довели гіпотезу, що корупція та тіньова еко-

номіка доповнюють один одного в країнах з низьким рівнем доходу, але не в країнах з високим доходом, що робить даний результат важливим для дослідження перетину цих незаконних практик [3].

Куерво-Казурра А. виявив кореляцію між корупцією та прямими іноземними інвестиціями і сформував два важливих для наукової спільноти висновки, що закони проти хабарництва за кордоном можуть діяти як стримуючий фактор проти участі в корупції в інших країнах, а також інвестори-хабарники шукають країни для інвестування, де поширена корупція [4]. Анохін С. та Шульце В. С. підтвердили для 64 країн наявність сильного зв'язку між підприємництвом, інноваціями та корупцією, що дозволило їм визначити ефективність контролю за корупцією за рахунок зростання рівня інновацій та підприємництва [5]. Пінто Дж., Леана К. Р. та Піл Ф. К. досліджували фундаментальні виміри корупції в організаціях, що сприяло формуванню її нової концептуалізації, як організації корумпованих осіб [6].

Хоча тематика кіберзлочин є досить важливою, але вона набула популярності останні п'ять років, тригером чому слугувала світова пандемія. Так, Найду Р. розробив багаторівневу модель, яка дозволяє оцінити фактори, жертви, джерела, методи атак, які були пов'язані саме з COVID-19 [7]. Дана модель сприяла формуванню висновку щодо розвитку широти та різноманіття кіберзлочинів у відповідь на ситуаційні фактори. Окрім руйнівних наслідків для різних суб'єктів економіки, деякі компанії намагаються будувати свій бізнес на кіберзлочинах. Так, Кшетрі Н. зосередив свою увагу на індустрії кіберзлочинності та розглянув її економічні, інституційні, бізнес-аспекти для компаній, основна діяльність яких побудована на кіберзлочинах [8]. Група вчених з Великобританії, США, Німеччини та Нідерландів провели системне дослідження щодо вартості кіберзлочинності, яке дозволило прийти до висновку, що треба більше витрачати на виявлення кіберзлочинців та притягнення їх до відповідальності, а ніж на збільшення витрат на додаткові заходи протидії таким злочинам [9].

Таким чином, тема впливу корупції, кіберзлочинів та операцій тіньової економіки є досить актуальною та практично значущою. Хоча й існує велика кількість наукових робіт, присвячена різним їх аспектам, але існують певні прогалини в теоретико-методологічній та практичній базах з економічної точки зору, що й потребує подальших досліджень.

Мета статті полягає у проведені аналізу теорії та практики латентних впливів трьох видів незаконних практик, таких як кіберзлочини, корупція та операції тіньового сектору, на діяльність суб'єктів економіки.

Виклад основного матеріалу дослідження. Для аналізу теорії латентних впливів трьох видів незаконних практик, таких як кіберзлочини, корупція та операції тіньового сектору, було відібрано наукові публікації з бази даних Scopus, які відповідали ключовим словам «кіберзлочини», «корупція», «тіньова економіка», «бізнес» та «латентний». В результаті даного запиту було сформовано базу даних з 480 документів, ключові слова яких було проаналізовано з використанням програмного додатку VOSviewer та візуалізовано на рис. 1.

В результаті було визначено 5 кластерів ключових слів, які ідентифікують напрями досліджень, пов'язані з трьома видами незаконних практик та їх впливом на бізнес. Червоний кластер (рис. 1) зосереджений на аспектах цифрових технологій, кіберзлочинів, штучного інтелекту, аналізу даних та мережевої безпеки. Це свідчить про значний інтерес до вивчення сучасних інформаційних технологій та їхньої ролі у забезпеченні безпеки бізнесу та економіки. Зокрема, підвищена увага до кіберзлочинів і кібербезпеки підкреслює актуальність проблем, пов'язаних із захистом цифрової інфраструктури.

Зелений кластер (рис. 1) акцентує увагу на економічному розвитку, стійкості, тіньовій економіці та податковій системі. Це вказує на необхідність дослідження економічних процесів, що впливають на ефективність державної політики та соціально-економічний розвиток. Зокрема, аналіз тіньової економіки та податкового навантаження є важливим для розуміння впливу нелегальних операцій на макроекономічні показники та регуляторну політику.

Синій кластер (рис. 1) зосереджується на питаннях прозорості, боротьби з корупцією, якості інституцій та державного управління. Це підкреслює важливість створення ефективної інституційної бази для боротьби з корупцією, покращення управлінських процесів у публічному секторі та підвищення підзвітності. Теми кластеру відображають прагнення до підвищення інституційної спроможності та забезпечення прозорості в державному і приватному секторах.

Жовтий та бузковий кластери є суміжні і відображають питання, які розглядаються як вторинні, що можуть допомагати вирішувати

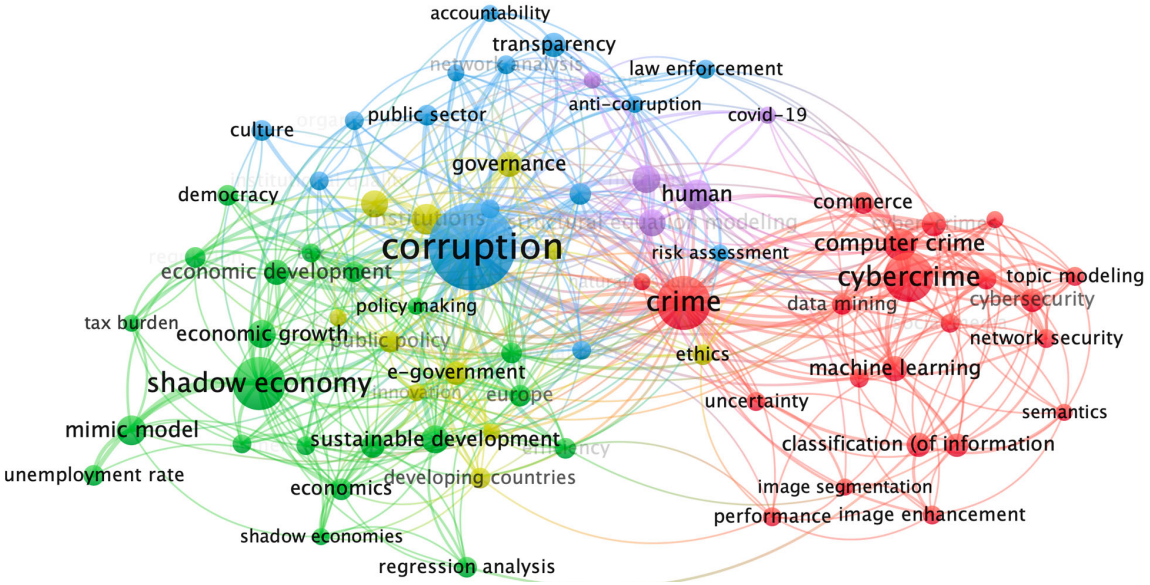

Рис. 1. Результати бібліометричного аналізу

Джерело: побудовано самостійно автором з використанням аналітичного додатку VOSviewer

проблеми корупції, кіберзлочинів та тіньової економіки. Так, жовтий кластер (рис. 1) робить акцент на гендерних аспектах, питаннях етики, державної політики, цифрового уряду та підприємництва. Підвищення гендерної рівності та етичних стандартів сприяє зменшенню корупції, а розвиток цифрового уряду підвищує прозорість і допомагає боротися з незаконними операціями, зокрема через автоматизацію процесів. Цифровізація створює нові ризики, пов'язані із захистом даних громадян і кібербезпекою державних систем, але водночас дозволяє ефективніше відстежувати та зупиняти незаконні операції.

Бузковий кластер (рис. 1), зосереджений на COVID-19 і людських аспектах, висвітлює вплив пандемії на зростання тіньової економіки та кіберзлочинності. Пандемія сприяла збільшенню нелегальної зайнятості й кібератак через перехід бізнесу в онлайн. Людський фактор також став ключовим у кіберзлочинності, особливо через соціальну інженерію.

Теоретичні аспекти впливу корупції, кіберзагроз та тіньового сектору на бізнес свідчать про комплексність і взаємозв'язок цих явищ. Корупція та недостатня прозорість у державних інституціях створюють передумови для економічних дисфункцій, а тіньовий сектор, зокрема через ухилення від оподаткування та нелегальну діяльність, суттєво знижує ефективність державної економічної політики. Кіберзагрози, зокрема у вигляді кібератак та злочинів, що сприяють витоку даних і шахрайству, ставлять під загрозу цифрову інфраструктуру бізнесу, що потребує розробки нових стратегій кібербезпеки. Водночас, цифровізація та впровадження етичних стандартів можуть допомогти зменшити рівень корупції та створити ефективніші механізми боротьби з незаконними практиками, сприяючи розвитку стійкого бізнес-середовища.

Щодо практики впливу незаконних практик на бізнес, то слід навести реальні приклади, які демонструють їх приховане значення для формування стійкого, ефективного та безпекового бізнес-середовища.

У 2021 році одна з найбільших трубопровідних компаній США Colonial Pipeline стала жертвою атаки програмою-вимагачем, яка паралізувала постачання палива на декілька днів. Для відновлення роботи вона була змушена виплатити хакерам 75 біткоїнів, що становило приблизно 4,4 мільйона доларів США [10]. Подібні випадки відбувалися й раніше. У 2020 році виробник розумних годинників та навігаційних пристроїв Garmin зазнав атаки, яка призвела до відключення їхніх сервісів, завдавши збитків на суму понад 10 мільйонів доларів [11]. Одним із найгучніших інцидентів стала атака NotPetya у 2017 році, яка вразила численні компанії по всьому світу, включаючи логістичну компанію Maersk. Наслідки атаки коштували Maersk до 300 мільйонів доларів збитків через паралізовані операції [12].

Ще один резонансний інцидент трапився в 2014 році з компанією Sony Pictures

Entertainment. Хакери проникли в мережу компанії та викрали конфіденційну інформацію, включаючи особисті дані співробітників і ще не випущені фільми, що спричинило фінансові втрати, оцінені в понад 100 мільйонів доларів [13]. Аналогічно, у 2013 році компанія Target Corporation зазнала масованої кібератаки, під час якої були викрадені дані про кредитні та дебетові картки понад 40 мільйонів клієнтів. Це спричинило прямі витрати на суму 162 мільйони доларів, без урахування репутаційних збитків.

Кіберзлочини суттєво впливають на бізнес та державні інституції в Україні, створюючи значні економічні та соціальні виклики. Відомий випадок стався у грудні 2015 року, коли було атаковано енергетичну інфраструктуру України. Хакери спрямували свої дії на кілька енергокомпаній, включаючи «Прикарпаттяобленерго», що призвело до масштабного відключення електропостачання. Близько 230 тисяч споживачів залишилися без електрики, а повне відновлення роботи тривало до шести годин. Ця атака стала першою в світі відомою кібератакою на енергосистему та продемонструвала вразливість критичної інфраструктури до цифрових загроз, викликавши занепокоєння як у державному секторі, так і серед підприємств, які залежать від електропостачання.

У грудні 2023 року мобільний оператор «Київстар», що обслуговує понад 24 мільйони клієнтів, став мішенню для хакерів. Кібератака спричинила серйозні перебої в роботі послуг, що залишило мільйони абонентів без зв'язку [14]. Для бізнесу та звичайних користувачів це стало нагадуванням про залежність сучасного суспільства від цифрових технологій. Відновлення нормальної роботи зайняло кілька днів, а компанія зазнала суттєвих фінансових та репутаційних втрат.

Ще одним значним інцидентом стала атака у січні 2024 року на дата-центр «Парковий», який надає послуги низці ключових державних та приватних організацій. Серед постраждалих опинилися такі компанії, як «Нафтогаз», «Укрпошта» та «Укрзалізниця», а також система перетину кордону «Шлях» [14]. Цей випадок продемонстрував, наскільки важливою є кібербезпека для забезпечення безперебійної роботи логістичних і транспортних процесів. Атака спричинила серйозні збої в роботі, що вплинуло як на діяльність підприємств, так і на життя громадян, які користувалися їхніми послугами.

У січні 2022 року відбулася одна з масштабніших кібератак, яка вразила понад 20 урядових сайтів України. Серед постраждалих опинилися вебресурси Міністерства закордонних справ, Кабінету Міністрів, Державної казначейської служби та інші. Атака паралізувала роботу сайтів, спричинила втрату доступу до державних послуг та порушила комунікацію з громадянами [15]. Цей інцидент став одним із найбільших за своїм впливом, змусивши державу значно підвищити заходи кіберзахисту.

Ще однією подією стала кібератака на державні реєстри у 2024 році. Хакери тимчасово припинили роботу всіх реєстрів Міністерства юстиції, що спричинило серйозні затримки в оформленні документів, реєстрації угод та інших юридичних операцій [16]. Цей випадок підкреслив, наскільки серйозними можуть бути наслідки таких атак для бізнесу, особливо тих компаній, які покладаються на державні послуги у своїй щоденній діяльності.

Корупція підриває довіру, спотворює ринкові механізми та призводить до значних фінансових втрат бізнесу та держави. Її можна віднести до латентних негативних факторів впливу, які призводять до зниження довіри до уряду, зниження ефективності бізнесу. Наприклад, у 2014 році в Бразилії розпочалося розслідування корупційних схем у державній нафтовій компанії Petrobras. Виявилося, що її топ-менеджери отримували «відкати» у розмірі 3% від контрактів з будівельними компаніями в обмін на укладення угод за завищеними цінами. Загальний обсяг хабарів досяг $2 млрд, а Petrobras втратила близько $14 млрд через завищені ціни за контрактами. Цей скандал призвів до політичних наслідків, включаючи імпічмент президента та ув'язнення екс-президента країни у 2016 році [17].

Будівельний гігант Odebrecht став фігурантом найбільшого міжнародного корупційного скандалу. Компанія платила хабарі, щоб отримувати прибуткові замовлення в різних країнах Латинської Америки. У 2016 році Odebrecht визнала дачу хабарів на суму понад $3 млрд і погодилася сплатити рекордний штраф у розмірі $3,5 млрд. Цей скандал мав негативні наслідки для економіки Бразилії, яка у 2015–2016 роках увійшла у найбільшу рецесію з 1901 року [17].

У 2015 році вибухнув корупційний скандал у ФІФА, коли було затримано 7 високопосадовців Федерації за підозрою в отриманні хабарів на загальну суму понад $100 млн. Скандал призвів до відставки президента

ФІФА Йозефа Блаттера та очільника УЄФА Мішеля Платіні, а також негативно позначився на репутації Федерації, що ускладнило пошук спонсорів для проведення Чемпіонату світу 2018 року [17].

У 2014 році з трьох молдовських банків – Banca de Economii, Banca Socială та Unibank – зникла сума в розмірі €1 млрд, що становило 12% ВВП країни. Це призвело до фінансової кризи, знецінення національної валюти та падіння економіки. Скандал спричинив політичну нестабільність, включаючи відставку двох урядів та розпад правлячої коаліції [17]. У 2008 році німецький концерн Siemens був визнаний винним у систематичному підкупі урядовців у різних країнах для отримання контрактів. Розслідування виявило, що компанія витратила понад $1,4 мільярда на хабарі. У результаті Siemens погодився сплатити штрафи на суму $1,6 мільярда, що стало одним із найбільших корпоративних штрафів за корупцію на той час [18]. Цей скандал негативно вплинув на репутацію Siemens та призвів до масштабних внутрішніх реформ.

Корупція в Україні залишається серйозною перешкодою для розвитку бізнесу, призводячи до фінансових втрат, підриву довіри та спотворення ринкових механізмів. Можна навести наступні яскраві приклади впливу корупції на бізнес-середовище. Так, у 2024 році в Одеському територіальному центрі комплектування було викрито корупційну схему, організовану начальником відділу Приморського РТЦК та СП Одеси. Посадовець за хабарі від 4,5 до 7 тисяч доларів США допомагав ухилянтам уникнути мобілізації, що призвело до незаконного збагачення на суму понад 1 мільйон доларів США. Загалом послугами скористалися 138 осіб. Після викриття схеми посадовцю було повідомлено про підозру в несанкціонованому втручанні в роботу інформаційно-комунікаційних систем, що передбачає покарання до 15 років позбавлення волі [19].

Аналіз судової практики в Україні показує, що у 98% вироків за корупційні злочини суди обмежуються штрафами, а лише у 1,5% випадків призначають покарання у вигляді позбавлення волі [20]. Така м'якість вироків не створює достатнього стримуючого ефекту для потенційних корупціонерів та підриває довіру до судової системи. У 2024 році Верховна Рада України підтримала в першому читанні законопроєкт № 11340, який передбачає можливість для корупціонерів уникнути кримінального покарання шляхом сплати значних штрафів. Розміри відшкодувань варіюються від 204 тисяч до 204 мільйонів гривень залежно від тяжкості злочину. Ця ініціатива викликала суспільне обурення та критику експертів, оскільки може легалізувати корупційні практики та послабити боротьбу з корупцією в країні [21].

Тіньова економіка, що включає незаконні та нерегульовані операції, може мати значний негативний вплив на легальний бізнес, призводячи до фінансових втрат, репутаційних ризиків та юридичних санкцій. Наприклад, у 2012 році британський банк HSBC був звинувачений у сприянні відмиванню грошей мексиканських наркокартелів та інших незаконних операцій. Розслідування виявило, що банк не забезпечив належного контролю за підозрілими транзакціями, що дозволило відмити мільярди доларів. У результаті HSBC погодився сплатити штраф у розмірі $1,9 мільярда, що стало одним із найбільших штрафів, накладених на фінансову установу за порушення законів про боротьбу з відмиванням грошей [22].

У 2015 році з'ясувалося, що компанія Volkswagen встановлювала на свої дизельні автомобілі програмне забезпечення, яке занижувало показники викидів під час тестувань. Ця практика, відома як «Дизельгейт», дозволила компанії продавати автомобілі, що не відповідали екологічним стандартам. Після виявлення шахрайства Volkswagen зазнав значних фінансових втрат, включаючи штрафи та компенсації, загальна сума яких перевищила $30 мільярдів [23]. У 2001 році енергетична компанія Enron збанкрутувала після виявлення масштабних фінансових махінацій, включаючи приховування боргів та завищення прибутків. Ці дії були частиною тіньових операцій, спрямованих на введення в оману інвесторів та регуляторів. Банкрутство Enron призвело до втрат інвесторів на суму близько $74 мільярдів та стало одним із найбільших корпоративних скандалів в історії США [24].

У 2018 році стало відомо, що через естонську філію Danske Bank було відмито близько €200 мільярдів сумнівного походження, переважно з росії та інших пострадянських країн. Банк не забезпечив належного контролю за підозрілими транзакціями, що дозволило здійснювати масштабні тіньові операції. Після виявлення цього скандалу Danske Bank зазнав значних репутаційних втрат, а також був змушений сплатити штрафи та стикнувся з розслідуваннями в кількох країнах [25].

Всі ці факти дозволяють прийти до висновку, що випадки корупції, кіберзлочинів та тіньових операцій призводять до негативних наслідків для бізнес-середовища. Хоча вони не є ключовими проблемами, але їх практика може свідчити про те, що вони є тими прихованими факторами, які дестабілізують діяльність суб'єктів економіки та можуть привести до втрати репутації, банкрутства чи значних фінансових втрат.

Висновки. Аналіз латентних впливів таких незаконних практик, як кіберзлочини, корупція та операції тіньового сектору, на діяльність суб'єктів економіки, демонструє значну роль цих явищ у сучасних економічних процесах. Хоча вони не є ключовими, але все ж таки мають суттєвий вплив на стабільність бізнес-середовища, підривають довіру до державних інститутів та бізнесу, знижують ефективність економічної діяльності, викликають суспільні незадоволення, призводять до гальмування розвитку національної економіки.

Аналіз теорії дослідження латентних впливів кіберзлочинів, корупції та тіньової економіки демонструє 5 кластерів, які відображають тісний зв'язок корупції, кіберзлочинів та тіньової економіки, підкреслюючи важливість урядових, технічних, цифрових, етичних, соціальних та інших аспектів у протидії цим викликам. Різноманітні дослідження підтверджують, що кіберзлочини не тільки порушують інформаційну безпеку, але й спричиняють значні фінансові збитки для бізнесу, як свідчать приклади з компаніями Colonial Pipeline, Garmin та Maersk. Водночас, корупція виявляється як один з головних факторів, що спотворює ринкові механізми, знижує конкурентоспроможність бізнесу, а також призводить до економічних втрат, як це було в разі скандалів з Petrobras, Odebrecht та інших компаній.

Тіньова економіка, яка включає незаконні та нерегульовані операції, істотно впливає на легальний бізнес, створюючи ризики для фінансової стабільності та репутації. Приклад з банком HSBC та скандал з Volkswagen чітко ілюструють наслідки тіньових операцій для компаній і економіки загалом. Виявлені випадки корупційних схем, такі як в Україні та інших країнах, також вказують на необхідність значних реформ у боротьбі з корупцією та зміцненні інституційної спроможності держави.

Аналіз теоретичних і практичних аспектів показує, що впровадження цифрових технологій, етичних стандартів і покращення інституційної прозорості можуть бути ключовими чинниками у боротьбі з незаконними практиками. Однак для досягнення ефективних результатів необхідно не лише розвивати законодавчі ініціативи, але й забезпечити їх належне виконання та контроль. Латентний характер цих впливів підкреслює важливість глибшого розуміння їхньої природи та розробки комплексних стратегій для боротьби з ними. Це дозволить створити стійке та безпечне бізнес-середовище, яке сприятиме розвитку економіки в умовах глобальних змін.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Schneider F., Enste D. H. Shadow economies: Size, causes, and consequences. *Journal of economic literature.* 2000. Vol. 38. № 1. P. 77–114. DOI: 10.1257/jel.38.1.77

2. Alm J., Embaye A. Using dynamic panel methods to estimate shadow economies around the world, 1984–2006. *Public Finance Review*. 2013. Vol. 41. № 5. P. 510–543. DOI: 10.1177/1091142113482353

3. Dreher A., Schneider F. Corruption and the shadow economy: an empirical analysis. *Public Choice*. 2010. № 144. P. 215–238. DOI: 10.1007/s11127-009-9513-0

4. Cuervo-Cazurra A. Who cares about corruption?. *Journal of international business studies*. 2006. № 37. P. 807–822. DOI: 10.1057/palgrave.jibs.8400223

5. Anokhin S., Schulze W. S. Entrepreneurship, innovation, and corruption. *Journal of business venturing*. 2009. Vol. 24. № 5. P. 465–476. DOI: 10.1016/j.jbusvent.2008.06.001

6. Pinto J., Leana C. R., Pil F. K. Corrupt organizations or organizations of corrupt individuals? Two types of organization-level corruption. *Academy of Management Review*. 2008. Vol. 33. № 3. P. 685–709. DOI: 10.5465/AMR.2008.32465726

7. Naidoo R. A multi-level influence model of COVID-19 themed cybercrime. *European Journal of Information Systems*. 2020. Vol. 29. № 3. P. 306–321. DOI: 10.1080/0960085X.2020.1771222

8. Kshetri N. The global cybercrime industry: economic, institutional and strategic perspectives. Springer Science & Business Media, 2010. 276 p.

9. Anderson R., Barton C., Böhme R., Clayton R., Van Eeten M. J., Levi M., Moore T., Savage S. (2013). Measuring the cost of cybercrime. *The economics of information security and privacy*. Springer, Berlin, Heidelberg, 2013. P. 265–300. DOI: 10.1007/978-3-642-39498-0_12

10. Easterly J., Fanning T. The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years. *CISA* : web page. URL: https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years (дата звернення: 01.12.2024)

11. Adler S. Incident Of The Week: Garmin Pays $10 Million To Ransomware Hackers Who Rendered Systems Useless. *Cyber Security Hub* : web page. URL: https://www.cshub.com/attacks/articles/incident-of-the-week-garmin-pays-10-million-to-ransomware-hackers-who-rendered-systems-useless (дата звернення: 01.12.2024)

12. Walton H. The Maersk cyber attack - how malware can hit companies of all sizes. *Kordia* : web page. URL: https://www.kordia.co.nz/news-and-views/the-maersk-cyber-attack (дата звернення: 01.12.2024)

13. The Sony Pictures Breach: A Deep Dive into a Landmark Cyber Attack. *Framework Security* : web page. URL: https://www.frameworksec.com/post/the-sony-pictures-breach-a-deep-dive-into-a-landmark-cyber-attack (дата звернення: 01.12.2024)

14. Мельник Т. СБУ відбила понад 9000 кібератак за два роки повномасштабної війни. *Forbes* : веб-сторінка. URL: https://forbes.ua/news/sbu-vidbila-ponad-9000-kiberatak-za-dva-roki-povnomasshtabnoi-viyni-05032024-19667?utm_source=chatgpt.com (дата звернення: 01.12.2024)

15. Мигаль М. Найбільша кібератака в історії України. Держспецзв'язку підбила підсумки втрат. *Главком* : веб-сторінка. URL: https://glavcom.ua/world/hitech/naybilsha-kiberataka-v-istoriji-ukrajini-derzhspeczvyazku-pidbila-pidsumki-vtrat-820210.html?utm_source=chatgpt.com (дата звернення: 01.12.2024)

16. Костюкова Ю. В Україні зупинили роботу всіх реєстрів Мін'юсту внаслідок кібератаки (оновлюється). *Mind* : веб-сторінка. URL: https://mind.ua/news/20282922-v-ukrayini-zupinili-robotu-vsih-reestriv-minyustu-vnaslidok-kiberataki-onovlyuetsya?utm_source=chatgpt.com (дата звернення: 01.12.2024)

17. Мошенець О. ТОП-5 найгучніших корупційних бізнес-скандалів у світі. *Investory News* : веб-сторінка. URL: https://investory.news/olena-moshenec-top-5-najguchnishix-korupcijnix-biznes-skandaliv-u-sviti/?utm_source=chatgpt.com (дата звернення: 01.12.2024)

18. Norton Rose Fullbright. Siemens reaches record $1.6 billion settlement with US and German authorities. *Lexology* : web page URL: https://www.lexology.com/library/detail.aspx?g=8899a469-4d50-4ff7-b870-daba60f3821d (дата звернення: 01.12.2024)

19. Лаб'як І. Новий скандал з мобілізацією: Одеський ТЦК заробив мільйон доларів на ухилянтах. *TSN* : веб-сторінка. URL: https://tsn.ua/exclusive/noviy-skandal-z-mobilizaciyeyu-odeskiy-tck-zarobiv-milyon-dolariv-na-uhilyantah-2588160.html?utm_source=chatgpt.com (дата звернення: 01.12.2024)

20. Вишневецький Д. У 98% вироків за корупцію українські суди обмежилися штрафами. *Daycom* : веб-сторінка. URL: https://daycom.com.ua/news/u-98-virokiv-za-korupciyu-ukrayinski-sudi-obmezhilisya-shtrafami?utm_source=chatgpt.com (дата звернення: 01.12.2024)

21. Депутати дозволили корупціонерам в Україні відкупитися від покарання: штраф від 204 тис. до 204 млн гривень залежно від тяжкості злочину. *БукІнфо* : веб-сторінка. URL: https://bukinfo.com.ua/ukrajina/deputaty-dozvolyly-korupcioneram-v-ukrajini-vidkupytysya-vid-pokarannya-shtraf-vid-204-tys-do-204-mln-gryven-zalezhno-vid-tyazhkosti-zlochynu?utm_source=chatgpt.com (дата звернення: 01.12.2024)

22. HSBC to pay $1.9bn in US money laundering penalties. *BBC* : web page. URL: https://www.bbc.com/news/business-20673466 (дата звернення: 01.12.2024)

23. Hotten R. Volkswagen: The scandal explained. *BBC* : web page. URL: https://www.bbc.com/news/business-34324772 (дата звернення: 01.12.2024)

24. Watkins S. Enron Fast Facts. *CNN* : web page. URL: https://edition.cnn.com/2013/07/02/us/enron-fast-facts/index.html (дата звернення: 01.12.2024)

25. Jensen T. Danske Bank's 200 billion euro money laundering scandal. *Reuters* : web page. URL: https://www.reuters.com/article/business/danske-banks-200-billion-euro-money-laundering-scandal-idUSKCN-1NO10D/ (дата звернення: 01.12.2024)

REFERENCES:

1. Schneider, F., & Enste, D. H. (2000). Shadow economies: Size, causes, and consequences. *Journal of economic literature, 38*(1), 77–114. https://doi.org/10.1257/jel.38.1.77

2. Alm, J., & Embaye, A. (2013). Using dynamic panel methods to estimate shadow economies around the world, 1984–2006. *Public Finance Review*, *41*(5), 510–543. https://doi.org/10.1177/1091142113482353

3. Dreher, A., & Schneider, F. (2010). Corruption and the shadow economy: an empirical analysis. *Public Choice*, *144*, 215–238. https://doi.org/10.1007/s11127-009-9513-0

4. Cuervo-Cazurra, A. (2006). Who cares about corruption?. *Journal of international business studies*, *37*, 807–822. https://doi.org/10.1057/palgrave.jibs.8400223

5. Anokhin, S., & Schulze, W. S. (2009). Entrepreneurship, innovation, and corruption. *Journal of business venturing*, *24*(5), 465–476. https://doi.org/10.1016/j.jbusvent.2008.06.001

6. Pinto, J., Leana, C. R., & Pil, F. K. (2008). Corrupt organizations or organizations of corrupt individuals? Two types of organization-level corruption. *Academy of Management Review*, *33*(3), 685–709. https://doi.org/10.5465/AMR.2008.32465726

7. Naidoo, R. (2020). A multi-level influence model of COVID-19 themed cybercrime. *European Journal of Information Systems*, *29*(3), 306–321. https://doi.org/10.1080/0960085X.2020.1771222

8. Kshetri, N. (2010). *The global cybercrime industry: economic, institutional and strategic perspectives*. Springer Science & Business Media.

9. Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M. J., Levi, M., ... & Savage, S. (2013). Measuring the cost of cybercrime. *The economics of information security and privacy*, 265–300. https://doi.org/10.1007/978-3-642-39498-0_12

10. Easterly, J., & Fanning, T. (2023). The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years. Available at: https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years (accessed December 1, 2024)

11. Adler, S. (2020). Incident Of The Week: Garmin Pays $10 Million To Ransomware Hackers Who Rendered Systems Useless. Available at: https://www.cshub.com/attacks/articles/incident-of-the-week-garmin-pays-10-million-to-ransomware-hackers-who-rendered-systems-useless (accessed December 1, 2024)

12. Walton, H. (2020). The Maersk cyber attack - how malware can hit companies of all sizes. Available at: https://www.kordia.co.nz/news-and-views/the-maersk-cyber-attack (accessed December 1, 2024)

13. Framework Security (2024). The Sony Pictures Breach: A Deep Dive into a Landmark Cyber Attack. Available at: https://www.frameworksec.com/post/the-sony-pictures-breach-a-deep-dive-into-a-landmark-cyber-attack (accessed December 1, 2024)

14. Melnyk, T. (2024). SBU vidbyla ponad 9000 kiberatak za dva roky povnomasshtabnoi viiny [The SBU repelled over 9,000 cyberattacks in two years of full-scale war]. Available at: https://forbes.ua/news/sbu-vidbila-ponad-9000-kiberatak-za-dva-roki-povnomasshtabnoi-viyni-05032024-19667?utm_source=chatgpt.com (accessed December 1, 2024)

15. Myhal, M. (2022). Naibilsha kiberataka v istorii Ukrainy. Derzhspetszviazku pidbyla pidsumky vtrat [The largest cyberattack in the history of Ukraine. The State Service for Special Communications summed up the losses]. Available at: https://glavcom.ua/world/hitech/naybilsha-kiberataka-v-istoriji-ukrajini-derzhspeczvyazku-pidbila-pidsumki-vtrat-820210.html?utm_source=chatgpt.com (accessed December 1, 2024)

16. Kostiukova, Yu. (2024). V Ukraini zupynyly robotu vsikh reiestriv Miniustu vnaslidok kiberataky (onovliuietsia) [In Ukraine, all registers of the Ministry of Justice were stopped due to a cyberattack (updated)]. Available at: https://mind.ua/news/20282922-v-ukrayini-zupinili-robotu-vsih-reestriv-minyustu-vnaslidok-kiberataki-onovlyuetsya?utm_source=chatgpt.com (accessed December 1, 2024)

17. Moshenets, O. (2019). TOP-5 naihuchnishykh koruptsiinykh biznes-skandaliv u sviti [TOP-5 most high-profile corruption business scandals in the world]. Available at: https://investory.news/olena-moshenec-top-5-najguchnishix-korupcijnix-biznes-skandaliv-u-sviti/?utm_source=chatgpt.com (accessed December 1, 2024)

18. Norton Rose Fullbright (2008). Siemens reaches record $1.6 billion settlement with US and German authorities. Available at: https://www.lexology.com/library/detail.aspx?g=8899a469-4d50-4ff7-b870-daba60f3821d (accessed December 1, 2024)

19. Lab'iak, I. (2024). Novyi skandal z mobilizatsiieiu: Odeskyi TTsK zarobyv milion dolariv na ukhyliantakh [New mobilization scandal: Odessa TRC earned a million dollars on draft evaders]. Available at: https://tsn.ua/exclusive/noviy-skandal-z-mobilizaciyeyu-odeskiy-tck-zarobiv-milyon-dolariv-na-uhilyantah-2588160.html?utm_source=chatgpt.com (accessed December 1, 2024)

20. Vyshnevetskyi, D. (2024). U 98% vyrokiv za koruptsiiu ukrainski sudy obmezhylysia shtrafamy [In 98% of corruption convictions, Ukrainian courts limited themselves to fines]. Available at: https://daycom.com.ua/news/u-98-virokiv-za-korupciyu-ukrayinski-sudi-obmezhilisya-shtrafami?utm_source=chatgpt.com (accessed December 1, 2024)

21. BukInfo (2024). Deputaty dozvolyly koruptsioneram v Ukraini vidkupytysia vid pokarannia: shtraf vid 204 tys. do 204 mln hryven zalezhno vid tiazhkosti zlochynu [Deputies allowed corrupt officials in Ukraine to avoid punishment: fines from 204 thousand to 204 million hryvnias, depending on the severity of the crime]. Available at: https://bukinfo.com.ua/ukrajina/deputaty-dozvolyly-korupcioneram-v-ukrajini-vidkupytysya-vid-pokarannya-shtraf-vid-204-tys-do-204-mln-gryven-zalezhno-vid-tyazhkosti-zlochynu?utm_source=chatgpt.com (accessed December 1, 2024)

22. BBC News (2012). HSBC to pay $1.9bn in US money laundering penalties. Available at: https://www.bbc.com/news/business-20673466 (accessed December 1, 2024)

23. Hotten, R. (2015). Volkswagen: The scandal explained. Available at: https://www.bbc.com/news/business-34324772 (accessed December 1, 2024)

24. Watkins, S. (2024). Enron Fast Facts. Available at: https://edition.cnn.com/2013/07/02/us/enron-fast-facts/index.html (accessed December 1, 2024)

25. Jensen, T. (2018). Danske Bank's 200 billion euro money laundering scandal. Available at: https://www.reuters.com/article/business/danske-banks-200-billion-euro-money-laundering-scandal-idUSKCN-1NO10D/ (accessed December 1, 2024)