

ФОРМИ ПРОЯВУ ТРАНСНАЦІОНАЛЬНОЇ ЕКОНОМІЧНОЇ ЗЛОЧИННОСТІ В УМОВАХ ГЛОБАЛЬНОЇ ЦИФРОВІЗАЦІЇ

Ю. І. Пилипенко, д. е. н., професор, pylypenkoYI@gmail.com, orcid.org/0000-0002-4772-1492,
А. Д. Сусліяєва, бакалавр, Susliaieva.A.D@nmu.one,
НТУ «Дніпровська політехніка»

Методологія дослідження. При виконанні дослідження було використано методи наукового узагальнення – при виокремленні основних форм прояву сучасної транснаціональної організованої економічної злочинності; аналізу та синтезу – при з'ясуванні механізмів реалізації тіньової економічної діяльності та їх соціально-економічних наслідків; логічного аналізу – при обґрунтуванні механізмів протидії тіньовій економічній діяльності.

Результати дослідження. У статті проаналізовано основні форми прояву сучасної транснаціональної організованої економічної злочинності, а також обґрунтовано механізми протидії тіньовій економічній діяльності на національному та міждержавному рівнях. Наведено сучасні приклади діяльності організованої економічної злочинності, підкреслено її транснаціональний характер. Узагальнено основні форми прояву економічної організованої злочинності на сучасному етапі розвитку світової економіки, розглянуто механізми реалізації тіньової економічної діяльності на основі використання новітніх технологій четвертої промислової революції.

Проаналізовано глобальні фінансові втрати від інтернет-шахрайства та застосування шкідливого програмного забезпечення. Підкреслено системний вплив на мікро-, макро- та мегаекономічних рівнях від діяльності організованої економічної злочинності. Проаналізовано динаміку розриву в надходженнях ПДВ у 2013-2022 рр. в ЄС та наголошено на критичному рівні щорічних втрат у бюджетах країн-учасниць з огляду на їх економічну безпеку. Досліджено динаміку нелегальних фінансових потоків у країнах Східної Європи, Центральної Азії, Балкан і Туреччини. Узагальнено форми прояву, механізми та соціально-економічні наслідки діяльності сучасної організованої економічної злочинності. Запропоновано механізми протидії тіньовій економічній діяльності на основі рекомендацій міжнародної групи з протидії відмиванню брудних грошей (FATF).

Новизна. Узагальнено новітні форми транснаціональної економічної злочинності та їх соціально-економічні наслідки, запропоновано механізми протидії тіньовій економічній діяльності.

Практична значущість. Результати дослідження можуть бути використані при розробці та реалізації державної політики протидії тіньовій економічній діяльності.

Ключові слова: тіньова економіка, організована економічна злочинність, форми тіньової економічної діяльності, цифровізація, промислова революція.

Постановка проблеми. У сучасному світі організована злочинність перестала бути локальною проблемою всередині держави або навіть цілого регіону, оскільки вона перетворилася на дестабілізуючий фактор для світової економіки, який завдає шкоди кожній сфері життя суспільства. Процеси міжнародної інтеграції, лібералізація торговельних бар'єрів та стрімкий розвиток

цифрових технологій не лише відкрили нові можливості для легального бізнесу, а й сформували сприятливі умови для появи нових форм транснаціональної злочинності. Сьогодні транскордонний кримінал дедалі більше набуває ознак інтелектуальної та економічної діяльності, де класичне насильство та тероризм поступаються місцем складним фінансовим махінаціям.

Впровадження інструментів цифровізації та технологій останнього десятиліття, а саме: штучного інтелекту, блокчейну, криптовалют та інших засобів автоматизації, створило сприятливі умови для прискорення проведення нелегальних фінансових операцій. У той час, як держави та міжнародні правоохоронні інституції обмежені бюрократією та розбіжностями у законодавствах, транскордонні кримінальні угруповання використовують сучасні інструменти без юридичних бар'єрів. Високий рівень анонімності цифрових активів (криптовалюти) і швидкість транскордонних операцій дозволяють злочинним організаціям виводити сотні мільярдів доларів із легального обігу, підриваючи національні економіки. Відтак виникає проблема в ідентифікації новітніх форм транскордонної економічної злочинності та потреба у пошуку потенційних механізмів протидії.

Аналіз останніх досліджень і публікацій. Проблематика новітніх форм прояву транснаціональної економічної злочинності достатньо активно обговорюється вітчизняною та світовою економічною спільнотою. Так, наприклад, у вітчизняних наукових дослідженнях акцентується увага на цільових результатах такої злочинності та сферах її застосування. Підкреслюється, що найбільш розповсюдженою кінцевою метою скоєння злочину є відмивання грошей. О. Хороновський виділяє вісім сфер господарської діяльності – торгівлю та посередництво, транспорт і будівництво, інноваційно-інвестиційну сферу, фінансово-економічну та зовнішньоекономічну діяльність, де, на його думку, суб'єкти найчастіше вдаються до скоєння економічних злочинів [1]. О. Хороновський та В. Тацієнко поділяють думку, що сфери скоєння злочину майже завжди переплітаються між собою, відбувається так звана допоміжна тіньова діяльність, коли основний злочин (викрадення чи вимивання грошей) приховується через кіберзлочинність, фіктивний документообіг, корупцію та інші види тіньової активності [1, 2].

Звіти міжнародної організації FATF підтверджують подібні тенденції, зазначаючи, що зараз головними фігурантами професійного відмивання грошей є юристи, фінансисти, бухгалтери та IT-спеціалісти, які мають доступ до конфіденційних файлів та баз

даних компанії або іншої інституції, завдяки чому їм легше проникати у корпоративну структуру і витягувати звідси потрібну для тіньової схеми інформацію [3]. В аналітичних дослідженнях цієї та інших міжнародних організацій підкреслюється, що проблема відмивання грошей є одним з найзначніших факторів, які сповільнюють зростання економіки як у глобальному, так і в регіональному вимірі. Особливо подібні соціально-економічні наслідки внаслідок транснаціональної економічної злочинності відчутні в країнах Східної Європи та Центральної Азії [4].

Через нестійке положення деяких інституцій в апаратах управління та постійне проходження товарів через ускладнений митний контроль (з причини різних економічних зон або відсутності торгових угод між державами) створюються сприятливі умови для махінацій з деклараціями та інвойсами. Варто зазначити, що розвинуті країни також стикаються з проблемою недоотриманого бюджету. Аналіз баз даних Європейської Комісії у цифровому вимірі демонструє як діджиталізація фінансового сектору дозволяє злочинним організаціям набагато легше виводити капітал у тіньовий сектор [5].

У цілому міжнародна спільнота та провідні організації сьогодні виділяють тенденцію зростання відмивання грошей саме за допомогою кібертехнологій. Підкреслюється, що управління ризиками, пов'язаними з нелегальними фінансовими потоками, наразі є одним з ключових питань порядку денного багатьох держав, особливо тих, які повністю виводять з обігу готівку. Події останніх декількох років у Південно-Східній Азії є яскравим прикладом того, як організована злочинність може бути сконцентрована в одному місті, але завдавати економічної шкоди мільйонам людей по всьому світу. Наочним кейсом наразі є вже зруйнований скам-центр KK Park, що було збудовано на південному кордоні М'янми з Таїландом. Задля функціонування такого хабу були задіяні усі можливі інструменти тіньової діяльності: від корупції до торгівлі людьми [6].

Формулювання мети статті. Метою статті є дослідження основних форм прояву сучасної економічної організованої злочинності на транснаціональному рівні, а також

обґрунтування механізмів протидії тіньовій економічній діяльності.

Виклад основного матеріалу дослідження. Четверта хвиля індустріалізації подарувала суспільству такі блага, як глобальну мережу інтернет, блокчейн та хмарні технології. Лише пів століття тому було важко повірити у те, що люди матимуть можливість контактувати один з одним на відстані в реальному часі. А сьогодні вже обертів набирає розробка штучного інтелекту, який підлаштовується під конкретні потреби, обробляючи запити, та виконує рутинні завдання. Як результат, кордони багатьох країн стали більш відкритими, міжнародна торгівля процвітає і обмеження на платежі між резидентами різних країн зменшуються. Здавалось би, що перешкод для ведення бізнесу та державного співробітництва мало б ставати менше і менше. Проте статистика останніх років говорить про те, що кількість нелегальних фінансових потоків тільки прогресує, бо кримінальний світ значно швидше адаптується до сучасних технологій.

У якості прикладу наведемо діяльність КК Park – відомого центру інтернет-шахрайства за останніх п'ять років у світі транснаціональної організованої злочинності. Це був величезний комплекс на півдні М'янми, неподалік від кордону із Таїландом, який функціонував під фасадом бізнес-центру для залучення інвестицій. Проте за цим офіційним прикриттям від самого початку ховався величезний скам-центр, де працівників добровільно чи насильно змушували займатися незаконною діяльністю – інтернет шахрайством. Були задіяні майже всі методи кіберзлочинності: від схеми «pig-butcher» до махінацій з реальними інвестиціями та кредитами, а викрадені кошти найчастіше виводилися через криптогаманці. До того ж, злочинцями у багатьох випадках могли бути такі ж самі жертви, яких обманним шляхом було викрадено до КК Park. Згідно зі звітами правозахисної організації Human Development Forum Foundation (HDFF), у комплексі примусово утримувалося близько 60 тисяч осіб, які під загрозою насильства займалися інтернет-шахрайством. Функціонував цей хаб з 2021 по 2025 рр. через нестабільну політичну ситуацію в регіоні, прикриття з боку китайських злочинних угруповань та вдалому

розташуванню [6]. У жовтні 2025 р. під жорстким тиском з боку Китаю, США та сусіднього Таїланду армія М'янми розпочала масштабну операцію та штурм комплексу. За даними незалежної британської організації Centre for Information Resilience, під час проведення цих заходів було знесено 635 будівель, в яких розміщувалися шахрайські центри та відбулась повна евакуація міста Ятай Нью-Сіті [7].

Головний парадокс КК Park був у тому, що будучи розташованим в Азійській частині світу його діяльність завдала шкоди майже по всіх континентах. Подібні закриті скам-центри заробляють у мільярдах, створюючи фінансові прогалини у державних бюджетах, банках та інших установах. Жертва шахрайської діяльності може перебувати за тисячі кілометрів від злочинця, але сучасні технології дозволяють переказувати гроші швидко та з мінімальними обмеженнями. Таким чином це перестає бути локальною загрозою, а створює прецедент по всьому світу.

Згідно з оприлюдненими оцінками, лише за 2025 рік глобальні фінансові втрати від шахрайства сягнули 442 мільярдів дол. США [8]. Причому існує думка, що реальний обсяг збитків може бути набагато більшим, оскільки багато злочинів можуть бути ще не розкритими або втрати досі незадекларовані. За даними аналітичних звітів Інтерполу, розвиток технології штучного інтелекту буде тільки збільшувати нелегальні прибутки – за попередніми прогнозами у 4,5 рази [8]. Нейромережа здатна набагато швидше обробляти потреби потенційних жертв, генерувати фішингові сторінки та дипфейки, роблячи кожен взаємодію більш переконливою.

Проте організована кіберзлочинність проявляє себе не лише через шахрайські скам-центри, які у більшості випадків орієнтовані на кошти фізичних осіб на невеликих підприємств. Транснаціональні корпорації стикнулися з іншою загрозою – Ransomware-as-a-Service (RaaS), що у перекладі може трактуватися як програми-вимагачі. Цей вид шкідливого програмного забезпечення проникає в мережі міжнародних корпорацій та фінансових установ, щоб повністю заблокувати їхні бази даних. Після зупинки операційної діяльності компанії-жертви транснаціональні злочинні синдикати вимагають сплату

багатомільйонного викупу (переважно в криптовалюті) за відновлення доступу до інформації. Таким чином, традиційне організоване вимагання трансформувалося у масштабну економічну загрозу, здатну дистанційно паралізувати глобальні ланцюги постачання.

За даними міжнародних організацій у 2023 році корпорації у цілому сплатили більше 1 млрд дол. США лише за викуп своїх вкрадених даних. Проте через простоти у роботі, витрати на відновлення баз даних та подальшу сплату штрафів мікроекономічні наслідки можуть бути ще значнішими. Дослідження показують, що 66% організацій, постраждалих від програм-вимагачів, зазнали значного зниження доходів. Крім того, 53% компаній повідомили про шкоду, завдану іміджу їхнього бренду, тоді як 29% вдалися до звільнень, щоб компенсувати фінансові втрати [9]. Якщо ж розглядати макрорівень, то найвизначнішим прикладом є атака RaaS на систему центрального банку Лесото у 2024 році. Цей прецедент паралізував роботу усього фінансового сектору країни, поставивши під загрозу стабільність національної економіки. До того ж, за попередніми оцінками страхового ринку Lloyd's of London, подібні атаки шкідливих ПЗ на основні пла-

тижні системи можуть призвести до збитків у розмірі 3,5 трлн дол. США протягом наступних п'яти років [9].

Транснаціональні кримінальні угруповання не обмежуються лише прямими кібератаками та шахрайством, що націлене на пересічних громадян. Паралельно з цим активно розвиваються схеми махінацій зі створенням фіктивних фірм, дробленням доходів, а також із залученням людей поза угрупованням (зазвичай студентів) для відкриття банківських акаунтів на їх ім'я для подальшого перенаправлення фінансових потоків. Наслідком цього є величезні недоотримання у державних бюджетах, при чому як і у бідних регіонах, так і у розвинених. Наприклад, у Європейському Союзі подібні махінації стають основою для податкових каруселей – шахрайства з ПДВ. У таких схемах фіктивні компанії отримують від покупців суми з ПДВ, зникають без їх сплати до бюджету, після чого їхні партнери вимагають від держави відшкодування цього ПДВ. Наслідком таких махінацій є системний розрив у надходженнях ПДВ (VAT Gap) у ЄС, який щорічно складає десятки млрд євро на рік (див. рис. 1).

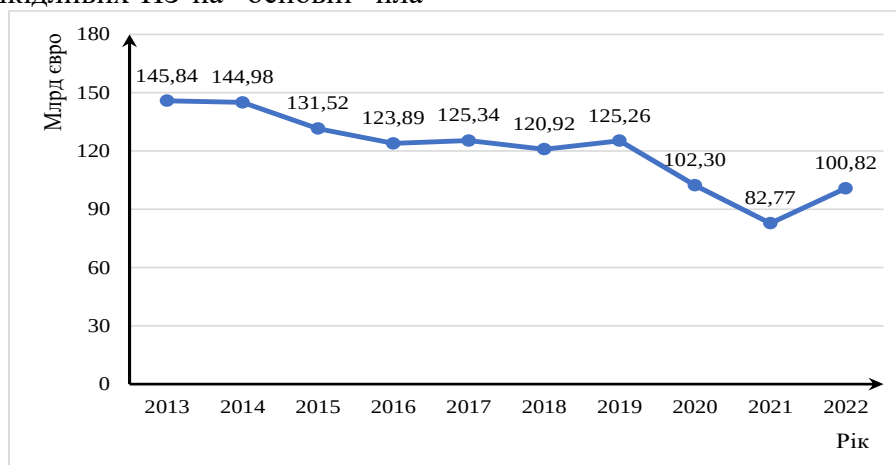


Рисунок 1. Динаміка розриву в надходженнях ПДВ у 2013–2022 рр. у ЄС, млрд євро [5]

Аналізуючи наведену статистику, можна стверджувати, що за останнє десятиліття недоплати ПДВ мали тенденцію до зниження. Якщо у 2018–2019 рр. щорічні втрати бюджетів країн ЄС перевищували 120 млрд євро, то у 2021–2022 рр. цей показник стабілізувався на рівні 80–100 млрд євро. Таке зниження є результатом посилення фінансового моніторингу, цифровізації податкового адміністрування та початку роботи

Європейської прокуратури (EPPO). Проте, з точки зору економічної безпеки, навіть такий рівень щорічних втрат залишається критичним. Цей колосальний обсяг тіньового капіталу не лише вилучається з легального сектору та соціальних програм ЄС, але й стає фінансовою базою для транснаціональних злочинних організацій, забезпечуючи їхню здатність до корумпування інститутів влади та

подальшої інтеграції у легалізовану господарську діяльність.

Прямим підтвердженням масштабів проблеми ПДВ-каруселей є матеріали розслідування Європейської прокуратури під кодовою назвою «Адмірал» (Investigation Admiral). Розслідування розпочалося у 2021 році, коли португальська податкова висунула підозру невеликій компанії, яка займалася роздрібною торгівлею смартфонів та інших девайсів. Після початку діяльності Європейської прокуратури справу було передано туди, не зважаючи на те, що з точки зору контролю на національному рівні Португалії компанія пройшла попередню перевірку. Залучивши ресурси Європолу, місцевих прокуратор та Європейської прокуратури було встановлено зв'язок між вже згаданою португальською компанією та майже 9000 іншими юридичними особами, а також понад 600 фізичними особами, які були зареєстровані у 15 країнах ЄС. Усі вони були залучені до схеми ПДВ-каруселі [10].

Первинна оцінка збитків склала 2,2 млрд євро, що зробило розслідування найбільшим в історії ЄС. Згодом, у 2024 році відбулося ще одне проведення слідства – «Адмірал 2.0», під час якого було викрито діяльність іншої злочинної мережі, що базувалася в країнах Балтії. Зазначається, що злочинці за час своєї діяльності продали техніку на суму 1,8 млрд євро через онлайн-маркетплейси, з яких вивели 297 млн євро податку. Таким чином загальна оцінка збитків від цієї транскордонної злочинної схеми зросла до 2,9 млрд

євро [11]. Особливо показовим є висновок Європейської прокуратури про те, що нове кримінальне угруповання використовувало аналогічний алгоритм дій та частково ту саму організаційну схему, що й фігуранти зі справи «Адмірал». Це є прямим підтвердженням того, що карусельні схеми з ПДВ спираються на єдину інфраструктуру та ті ж самі інструменти фінансового сектору – заздалегідь створені мережі фіктивних компаній, необанків та підставних осіб, якими можуть паралельно користуватися різні транснаціональні злочинні угруповання для виведення та легалізації капіталу [12].

Якщо у ЄС одним з головних інструментів нелегального збагачення є схеми з несплати ПДВ, то для багатьох інших країн існує проблема маніпуляцій з інвойсами та митними деклараціями при проведенні експортно-імпорتنих операцій. На рисунку 2 відображено поступове збільшення за останнє десятиліття цінового розриву в торговельних операціях у регіонах Східної Європи, Центральної Азії, Балкан і Туреччини. У даному випадку під ціновим розривом мається на увазі абсолютна розбіжність між вартістю товарів, задекларованою країною-експортером, та вартістю тих самих товарів, офіційно зафіксованою країною-імпортером. У межах даного дослідження цей розрив розглядається як цифрове відображення нелегальних фінансових потоків, що виникають внаслідок навмисного викривлення митної документації та платіжних квитанцій для прихованого переміщення капіталу.

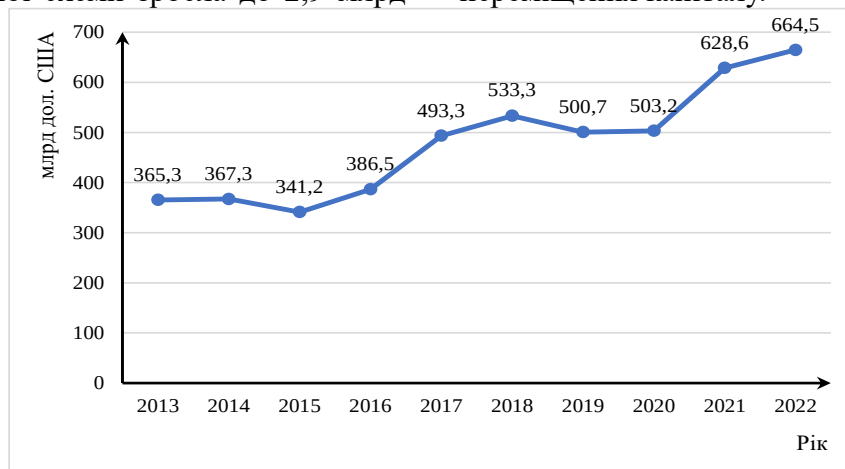


Рисунок 2. Динаміка нелегальних фінансових потоків у країнах Східної Європи, Центральної Азії, Балкан і Туреччини за 2013–2022 рр., млрд дол. США [4]

На графіку видно, що у 2022 р. ціновий розрив досяг свого піку в регіоні – 664,5 млрд

дол. США. Це майже вдвічі більше, ніж на початку розглянутого періоду. Такий

масштаб торгівельних маніпуляцій становить загрозу для бюджету країн. Використання схем заниження вартості імпорту призводить до масового недоотримання митних зборів та ПДВ. У контексті транснаціональної економічної злочинності кожна четверта операція з розвиненими країнами (близько 24,4% обсягу торгівлі) має ознаки маніпуляцій, що свідчить про глибоку інтеграцію криміналу в легальні торговельні ланцюги.

Таке зростання може бути обумовлено розвитком криптовалютних інструментів, які виступають субституту класичних банківських розрахунків. Кримінальні елементи використовують крипто-платежі задля приховання типових індикаторів ризиків, що встановлені валютним та податковим законодавством. Схема працює наступним чином: компанія-оболочка укладає імпортерний контракт із нерезидентом та надає банківській установі супровідні документи із значно заниженою митною вартістю товару. На виконання цього інвойсу через банк перераховується лише незначна частина коштів, що дозволяє мінімізувати податкові платежі та пройти моніторинг. Основний же обсяг фінансово-торговельного розрахунку (незадекларована різниця ціни) здійснюється в обхід банківської

системи напряму постачальнику за допомогою стейблкоїнів (USDT). У результаті митні органи бачать лише частину угоди, тоді як більша частка капіталу виводиться у тіньовий сектор. Найбільш привабливими для подібних схем є вільні економічні зони, великі логістичні хаби (зокрема такі порти, як Констанца у Румунії та Мерсін у Туреччині), а також сектори, у яких розповсюджена оплата у криптовалюті. До таких можна віднести торгівлю електронікою, автозапчастинами, дорожніми металами та агросектор. Для фінансового моніторингу майже неможливо відслідкувати такі платежі, бо вищеперераховані приклади утворюють сліпі зони для банківського нагляду [4].

Таким чином, в сучасних умовах глобальної цифровізації транснаціональна організована економічна діяльність набуває нових форм прояву на основі використання новітніх технологій нинішньої промислової революції. Це спричиняє не тільки збільшення обсягів такої злочинної діяльності, але й зростання негативних соціально-економічних наслідків як для окремих економічних суб'єктів, так і для національних економік та світового господарства у цілому (див. табл. 1).

Таблиця 1

Форми прояву, механізми та соціально-економічні наслідки діяльності сучасної організованої економічної злочинності

Форми прояву	Механізми	Соціально-економічні наслідки
Транскордонне шахрайство	Скам-центри, дипфейки, ШП, фішингові платформи, криптовалюта	Мільярдні збитки громадян та малого/середнього бізнесу, торгівля людьми та примусова праця
Шкідливе ПЗ	Програми-вимагачі (Ransomware-as-a-Service), криптовалюта	Витік конфіденційних даних, зупинка роботи та величезні збитки крупних компаній
ПДВ-каруселі	Мережа фіктивних компаній, онлайн-банкінг, викривлення електронного документообігу	Системне недоотримання у бюджетах країн, створення дисбалансу у ціноутворенні на ринку
Махінації з митними деклараціями / інвойсами	Умисне викривлення ціноутворення (завищення / заниження вартості), повторне використання інвойсів, криптовалюта	Масштабний витік капіталу з країн, системне недоотримання митних зборів, легалізація доходів від тіньової діяльності

Джерело: узагальнено автором.

Як свідчить практика, без таких інновацій як штучний інтелект, цифровий банкінг та криптовалюта здійснення злочинів такого масштабу було б неможливим. Поодинокі

випадки правопорушень перетворилися на складні кримінальні схеми із залученням людей з різних куточків землі. Шкідливе ПЗ, скам-фабрики, податкові каруселі та

маніпуляції з митною документацією – інструменти транснаціональної економічної злочинності, які функціонують виключно завдяки розробкам четвертої та п'ятої хвилі індустріалізації.

Висновки. Проведений аналіз форм прояву транснаціональної організованої економічної злочинності засвідчив зростання їх масштабів за рахунок використання технологічних досягнень сучасної промислової революції. Все це вимагає застосування національними урядами та відповідними міжнародними організаціями заходів по їх ефективній протидії, нагального вирішення питання щодо правильного реагування та механізмів скоординованих дій при виявленні підозрілих операцій. Силкові заходи стовідсотково вже не є тим варіантом, який повністю зупинив би сучасну організовану злочинність. Доказом того є ліквідація вже згаданого КК Park, яка не призвела до бажаних результатів і не знищила шахрайську мережу. Місцеві волонтери повідомляють, що за декілька кілометрів від знесеного комплексу існує забудована територія, відома як парк Цінсонг, яка швидко розширюється і вже носить назву КК Park 2.0. Шахрайська індустрія М'янми вдалася до іншої стратегії та тепер ховає скам'яні центри глибоко в джунглях та горах [7].

Такий «ефект гідри» доводить, що спроби боротьби з сучасною транскордонною злочинністю локальними силовими методами є неефективними. Оскільки збагачення – основна ціль скоєння кримінальних діянь, то й заходи протидії мають бути проведені саме у системі врегулювання фінансового сектору на міжнародному рівні. З огляду на це, можна запропонувати таке рішення, як перегляд політики щодо рекомендацій FATF (FATF 40 Recommendations). На нашу думку, їх дотримання має бути не рекомендованим, а жорстко регульованим. Сьогодні Рекомендації FATF не є примусовими, що дозволяє державам по-різному інтерпретувати їх у національному законодавстві. Через ці розбіжності правоохоронці часто не можуть отримати дозвіл на арешт рахунків або видачу підозрюваного, оскільки юридичні підстави в різних країнах не уніфікованими.

Подоланню подібних правових розбіжностей та вирішенню проблеми неконтрольованих фінансових потоків може, на наше

переконання, сприяти імплантація в національну практику протидії тіньовим економічним операціям деяких рекомендацій FATF. Наприклад, рекомендація 1 («Оцінка ризиків та ризик-орієнтований підхід») передбачає, зокрема, створення єдиної інтегрованої бази даних ринкових цін для митних органів, підрозділів фінансової розвідки та банківської системи. Кожна з цих інституцій при перевірці платежів та супровідної документації зможе об'єктивно оцінювати вартість товарів та своєчасно виявляти відхилення від норми у митних інвойсах. Реалізація цієї рекомендації не передбачає створення нових бюрократичних ускладнень для легального бізнесу, а навпаки дасть можливість оперативніше реагувати на схеми відмивання коштів. Крім того, на сучасному етапі критично важливим є приєднання провайдерів віртуальних активів (VASP) до загальної системи фінансового моніторингу задля змоги відслідковувати кінцевих бенефіціарних власників.

Рекомендація 4 («Конфіскація та запобіжні заходи») вимагає розмежування процедур тимчасового запобіжного обмеження та остаточної конфіскації. Реалізація цієї рекомендації передбачає надання підрозділам фінансової розвідки та правоохоронним органам повноважень щодо негайного досудового заморожування банківських рахунків та криптогаманців для відвернення ризику виведення капіталу. При цьому остаточна конфіскація майна здійснюється виключно за рішенням суду із дотриманням презумпції невинуватості.

Рекомендація 9 («Закони про банківську таємницю») визначає, що закони про банківську таємницю не мають ставати перешкодою для розслідування злочинів та обміном інформацією між юрисдикціями. Впровадження цієї рекомендації не означає вільного доступу до персональних рахунків фізичних осіб, а передбачає створення порядку дій за наявності обґрунтованої підозри з боку місцевих прокуратур, Європейської прокуратури чи фінансової розвідки. Банківська таємниця не має слугувати юридичною підставою для відмови у наданні даних.

Рекомендація 15 («Нові технології») стосується попередньої ретельної перевірки відповідними державними службами безпеки нових продуктів чи фінансових установ

(наприклад, фінтех та необанки) перед їх виходами на ринки. Таким чином має бути обов'язкове ліцензування або реєстрація та повноцінний AML-нагляд за провайдерами віртуальних активів – криптобіржами, обмінниками, P2P-платформами.

Рекомендації 37 і 40 («Взаємна юридична допомога та інші форми міжнародного співробітництва») спрямовані на усунення бюрократичних бар'єрів та складнощів, що пов'язані з розбіжностями у законодавствах різних країн. Задля ефективної протидії транскордонним кримінальним угрупованням, впровадження цих рекомендацій на глобальному рівні допоможе перейти від тривалого реагування до прямого та оперативного обміну інформацією між підрозділами фінансової розвідки, митними органами та місцевими прокуратурами без посередників [13].

Література

1. Хоронівський О.І. Функціональні характеристики сучасних транснаціональних організованих злочинних угруповань, які функціонують на шкоду економічним інтересам держави. *Київський часопис права*. 2023. №4. С. 203-207. URL: <https://doi.org/10.32782/klj/2022.4.30>
2. Тацієнко В. Транснаціональне шахрайство та методика його розслідування. *Вісник Національної академії внутрішніх справ*. 2024. №2. С. 362-369. URL: <https://doi.org/10.32703/2663-6352/2024-2-16-362-369>
3. Professional Money Laundering. Financial Action Task Force (FATF). 2018. URL: <https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Methodsandtrends/Professional-money-laundering.html>
4. Trade-Related Illicit Financial Flows in Developing Europe 2013-2022. Global Financial Integrity. 2024. URL: <https://gointegrity.org/report/trade-related-illicit-financial-flows-in-developing-europe-2013-2022/>
5. VAT Compliance Gap in the EU. European Commission, Taxation and Customs Union. 2023. URL: https://webgate.ec.europa.eu/taxation_customs/redisstat/databrowser/view/vap_compl_gap/default/table
6. Human Development Forum Foundation (HDF). KK Park: One of Southeast Asia's Largest Scam Centers. URL: <https://hdf.org/kk-park-one-of-southeast-asias-largest-scam-centers/>
7. Centre for Information Resilience. Investigation into the destruction of KK Park II. Myanmar Witness. 2025. URL: <https://www.info-res.org/myanmar-witness/articles/investigation-into-the-destruction-of-kk-park-ii/>
8. INTERPOL. Global Financial Fraud Threat Assessment. 2026. URL: <https://www.interpol.int/News-and-Events/News/2026/INTERPOL-report-warns-of-increasingly-sophisticated-global-financial-fraud-threat>
9. Azubuike C.F., Akinwumi O.I., Ezeamu E.O. Assessing the Global Economic Impact of Ransomware

Attacks and Strategic Global Response. *Nnamdi Azikiwe Journal of Political Science*. 2024. Vol. 9, No. 4. Pp. 1-17. URL: <https://najops.org.ng/index.php/najops/article/view/276>

10. EPPO. Operation Admiral: EPPO uncovers organised crime groups responsible for VAT fraud estimated at €2.2 billion. 2022. URL: https://www.eppo.europa.eu/media/news/operation-admiral-eppo-uncovers-organised-crime-groups-responsible-vat-fraud-estimated-eu22-billion-2022-11-29_en

11. European Public Prosecutor's Office (EPPO). Investigation Admiral 2.0: Europe's biggest VAT fraud links to organised crime. 2024. URL: https://www.eppo.europa.eu/media/news/investigation-admiral-20-europes-biggest-vat-fraud-links-organised-crime-2024-11-28_en

12. European Public Prosecutor's Office (EPPO). Investigation Admiral 2.0: Suspected ringleader of large-scale tax evasion and money laundering referred to court. 2025. URL: https://www.eppo.europa.eu/media/news/investigation-admiral-20-suspected-ringleader-large-scale-tax-evasion-and-money-laundering-referred-2025-06-10_en

13. FATF. International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. FATF, Paris, France. 2026. URL: www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html

References

1. Khoronovskiy, O.I. (2023). Funktsionalni kharakterystyky suchasnykh transnatsionalnykh orhanizovanykh zlochynnykh uhrupovan, yaki funktsionuiut na shkodу ekonomichnym interesam derzhavy. *Kyivskiy chasopys prava*, (4), 203-207. URL: <https://doi.org/10.32782/klj/2022.4.30>
2. Tatsienko, V. (2024). Transnatsionalne shakhraystvo ta metodyka yoho rozsliduvannia. *Visnyk Natsionalnoi akademii vnutrishnikh sprav*, (2), 362-369. URL: <https://doi.org/10.32703/2663-6352/2024-2-16-362-369>
3. Financial Action Task Force. (2018). Professional money laundering. FATF. Retrieved from <https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Methodsandtrends/Professional-money-laundering.html>
4. Global Financial Integrity. (2024). Trade-related illicit financial flows in developing Europe 2013-2022. GFI. Retrieved from <https://gointegrity.org/report/trade-related-illicit-financial-flows-in-developing-europe-2013-2022/>
5. European Commission. (2023). VAT compliance gap in the EU. Taxation and Customs Union. Retrieved from https://webgate.ec.europa.eu/taxation_customs/redisstat/databrowser/view/vap_compl_gap/default/table
6. Human Development Forum Foundation. (2024). KK Park: One of Southeast Asia's largest scam centers. HDF. Retrieved from <https://hdf.org/kk-park-one-of-southeast-asias-largest-scam-centers/>
7. Centre for Information Resilience. (2025). Investigation into the destruction of KK Park II. Myanmar

Witness. Retrieved from <https://www.info-res.org/myanmar-witness/articles/investigation-into-the-destruction-of-kk-park-ii/>

8. INTERPOL. (2026). Global financial fraud threat assessment. Retrieved from <https://www.interpol.int/News-and-Events/News/2026/INTERPOL-report-warns-of-increasingly-sophisticated-global-financial-fraud-threat>

9. Azubuike, C.F., Akinwumi, O.I., & Ezeamu, E.O. (2024). Assessing the global economic impact of ransomware attacks and strategic global response. Nnamdi Azikiwe Journal of Political Science, Vol. 9 (4), 1-17. Retrieved from <https://najops.org.ng/index.php/najops/article/view/276>

10. European Public Prosecutor's Office. (2022). Operation Admiral: EPPO uncovers organised crime groups responsible for VAT fraud estimated at €2.2 billion. EPPO. Retrieved from [https://www.eppo.europa.eu/media/news/operation-admiral-eppo-uncovers-organised-](https://www.eppo.europa.eu/media/news/operation-admiral-eppo-uncovers-organised-crime-groups-responsible-vat-fraud-estimated-eu22-billion-2022-11-29_en)

[crime-groups-responsible-vat-fraud-estimated-eu22-billion-2022-11-29_en](https://www.eppo.europa.eu/media/news/operation-admiral-eppo-uncovers-organised-crime-groups-responsible-vat-fraud-estimated-eu22-billion-2022-11-29_en)

11. European Public Prosecutor's Office. (2024). Investigation Admiral 2.0: Europe's biggest VAT fraud links to organised crime. EPPO. Retrieved from https://www.eppo.europa.eu/media/news/investigation-admiral-20-europes-biggest-vat-fraud-links-organised-crime-2024-11-28_en

12. European Public Prosecutor's Office. (2025). Investigation Admiral 2.0: Suspected ringleader of large-scale tax evasion and money laundering referred to court. EPPO. Retrieved from https://www.eppo.europa.eu/media/news/investigation-admiral-20-suspected-ringleader-large-scale-tax-evasion-and-money-laundering-referred-2025-06-10_en

13. Financial Action Task Force. (2026). International standards on combating money laundering and the financing of terrorism & proliferation. FATF, Paris, France. Retrieved from www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html

FORMS OF MANIFESTATION OF TRANSNATIONAL ECONOMIC CRIME IN THE CONDITIONS OF GLOBAL DIGITALIZATION

Yu. I. Pylypenko, D.E., Professor,

A. D. Susliaieva. Bachelor Student, Dnipro University of Technology

Methods. The study employs scientific generalization to identify the main forms of contemporary transnational organized economic crime; analysis and synthesis to examine the mechanisms of shadow economic activity and the socio-economic consequences; logical analysis to substantiate the mechanisms for countering shadow economic activity.

Results. This study analyzes the key forms of modern transnational organized economic crime and substantiates the mechanisms for countering shadow economic activity at both national and international levels. It provides contemporary case studies of organized economic crime, highlighting its transnational nature. Furthermore, it synthesizes current patterns of organized economic crime in the global economy and examines the mechanisms of shadow activities driven by advanced Industry 4.0 technologies.

Global financial losses from online fraud and malicious software implementation are analyzed. The systemic impact of organized economic crime at the micro-, macro- and mega-economic levels is emphasized. It evaluates the EU VAT gap dynamics for the 2013–2022 period, highlighting the critical level of annual revenue losses in the budgets of member states in terms of their economic security. Additionally, the dynamics of illicit financial flows in the countries of Eastern Europe, Central Asia, the Balkans and Turkey are examined. The research summarizes the forms of manifestation, mechanisms and socio-economic consequences of modern organized economic crime. Mechanisms for combating the shadow economy are proposed, based on the recommendations of the Financial Action Task Force (FATF).

Novelty. The paper conceptualizes emerging forms of transnational economic crime and their socio-economic consequences, offering targeted strategies to combat the shadow economy.

Practical value. The findings of this study can be used in developing and implementing public policy aimed at countering shadow economic activities.

Keywords: shadow economy, organized economic crime, forms of shadow economic activity, digitalization, Industry 4.0.

Стаття надійшла до редакції 20.08.2026 р.

Прийнята до публікації 05.09.2026 р.

Дата публікації 30.09.2026 р.