Методологічний бюлетень

Серійний номер: МінФін-AML-2025-16

Квітень 2025

“Ви не переможете, якщо не почнете”

Гелен Роуленд

Мета

Методологічний Бюлетень видається Міністерством Фінансів України на регулярній основі починаючи з січня 2025 р. та містить інформацію щодо національних та світових тенденцій у сфері протидії відмиванню коштів, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення (ПВК/ФТ/ФР). Розроблено для суб'єктів первинного фінансового моніторингу (СПФМ), регуляторів та правоохоронних органів.

Включає актуальні дані про нові методи та схеми ВК і ФТ, що дозволяє СПФМ адаптувати свої процедури моніторингу та контролю.

Для регуляторів та правоохоронних органів є інструментом для розробки ефективних стратегій боротьби з ВК, включаючи навчання та координацію дій між різними установами для забезпечення належної співпраці та обміну інформацією.

Звіти міжнародних організацій та окремих юрисдикцій

Консультативна інформація FinCEN щодо фінансування Ісламської держави Іраку та Сирії (ІДІЛ) та її глобальних філій [1]

FinCEN ADVISORY

FIN-2025-A001 April 1, 2025

FinCEN Advisory on the Financing of the Islamic State of Iraq and Syria (ISIS) and its Global Affiliates

Suspicious Activity Report (SAR) Filing Request:

FinCEN requests that financial institutions reference this Advisory by including the key term “**ISIS-2025-A001**” in SAR field 2 (Filing Institution Note to FinCEN) and the narrative and select SAR field 33(a) (Terrorist Financing-Known or suspected terrorist/terrorist organization).

The Financial Crimes Enforcement Network (FinCEN) is issuing this Advisory to assist financial institutions in identifying and reporting suspicious activity related to the financing of the Islamic State of Iraq and Syria (ISIS).[1] ISIS is a Sunni terrorist organization that has conducted and inspired terrorist attacks worldwide for more than a decade, killing or injuring thousands of people.[2] The U.S. Department of the Treasury’s (Treasury) 2024 National Terrorist Financing Risk Assessment notes that ISIS, which separated from al-Qa’ida (AQ) and declared itself a caliphate in 2014, remains a regional and global threat.[3] While elements of ISIS’ central leadership remain in parts of Iraq and Syria where ISIS previously controlled large swaths of territory,[4] the group has numerous affiliates operating around the world, particularly in Africa, the Middle East, and Central Asia.[5] Last year’s mass casualty attacks in Iran and Moscow by ISIS’s’ branch in Central Asia, known as ISIS-Khorasan (ISIS-K),[6] as well as the 2025 New Year’s Day attack in New Orleans, carried out by an ISIS-inspired homegrown violent extremist

FinCEN оприлюднило спеціальне попередження для фінансових установ, спрямоване на виявлення та припинення підозрілої діяльності, пов’язаної з фінансуванням терористичної організації Ісламська держава Іраку та Сирії (ISIS) і її глобальних афілійованих структур. Документ відображає зростаючий рівень загроз, що походять від як централізованого керівництва ISIS, так і децентралізованих регіональних осередків, зокрема ISIS-K (Корасан) — афілійованого підрозділу, відповідального за

[1] https://www.fincen.gov/sites/default/files/advisory/2025-04-01/FinCEN-Advisory-ISIS-508C.pdf

нещодавні масштабні атаки в Ірані, Москві та США.

FinCEN зазначає, що після втрати територій у 2019 році ISIS трансформувалась у мережу автономних осередків із потужними горизонтальними зв'язками. Окремі підрозділи продовжують отримувати фінансування від центрального керівництва через так звану «Генеральну дирекцію провінцій» — адміністративну структуру, яка координує чотири регіональні офіси. Організація також підтримує контроль у таборах для переміщених осіб, зокрема в Аль-Холі (Сирія), де відбувається вербування, радикалізація і фінансова підтримка утримуваних осіб, включаючи жінок та дітей.

FinCEN детально описує основні методи збору коштів: здирництво і оподаткування місцевого населення (зокрема у Сомалі, Західній Африці, Центральній Азії), експлуатація природних ресурсів (особливо в Демократичній Республіці Конго), викрадення для викупу (що використовується практично в усіх регіонах присутності ISIS), краудфандинг і пожертви, зокрема через криптовалюти. Останнє набуває особливої ваги: групи, пов'язані з ISIS, використовують криптогаманці, QR-коди у власних публікаціях, багаторівневі ланцюги переказів і активну децентралізацію через unhosted wallets. Використання стейблкоїнів, зокрема USDT, відзначається як одна з особливо поширених практик.

Для переміщення коштів терористична організація вдається до поєднання офіційної та неформальної фінансової інфраструктури: банківські рахунки в юрисдикціях із слабким регулюванням, нелегальні або незареєстровані постачальники грошових послуг (особливо хавали), а також соціальні мережі та неформальні канали передачі грошей. Багато операцій здійснюються через Туреччину — ключовий транзитний вузол.

Окрему увагу в документі приділено внутрішньоамериканській загрозі — «домашнім насильницьким екстремістам», натхненним ідеологією ISIS. FinCEN підкреслює ризик раптових конверсій активів, закриття рахунків, накопичення кредитів без очевидної мети, або використання P2P платформ, банкоматів, криптовалют для виводу коштів у готівку. Рекомендації також містять набір конкретних червоних прапорців (red flags), зокрема щодо одночасного доступу до акаунтів з різних країн, транзакцій у регіони з активністю ISIS без очевидної причини, або неочікуваних грошових потоків, пов'язаних із кампаніями «гуманітарної допомоги».

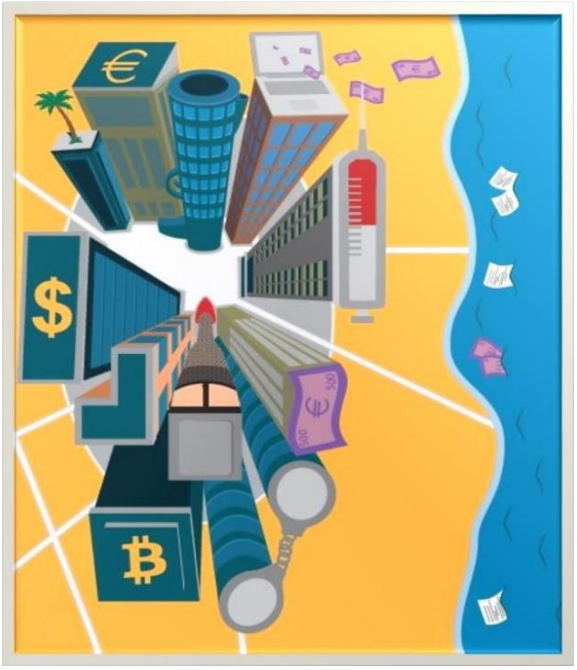
FinCEN закликає фінансові установи позначати відповідні Звіти про підозрілу активність (SARs) ключовим словом "ISIS-2025-A001" та нагадує про правові обов'язки, включаючи ведення документації, зберігання звітів, та співпрацю з правоохоронними органами. Також

Висновки:

- **ISIS та її філіали адаптувались до втрати територій шляхом децентралізації фінансових потоків**, при цьому потужні підрозділи підтримують фінансово слабші, а групи, що діють в таборах переміщених осіб, залучають кошти з понад 40 країн через хавали, готівку та криптовалюти.
- **Криптовалюти, зокрема стейблкоїни та платформи без належного контролю ПВК/ФТ, використовуються для фінансування терактів**, включно з недавніми атаками в США. Фінансова інфраструктура, як-от Binance, вже фігурувала в розслідуваннях за недотримання вимог BSA.
- **FinCEN надало конкретний набір індикаторів ризику**, зокрема підозрілі транзакції на користь осіб у Туреччині, дивні паттерни кредитування та переказів, і краудфандингові кампанії в соцмережах із символікою ISIS — що є інструментами для своєчасного виявлення фінансування тероризму.
- **Фінансові установи повинні активізувати міжвідомчий обмін інформацією**, а також забезпечити ефективний моніторинг клієнтів, зокрема щодо приватного банкінгу іноземних політиків та осіб, пов'язаних із гуманітарною діяльністю в ризикових регіонах.

підкреслюється важливість міжінституційного обміну інформацією на основі §314(b) Закону PATRIOT, зокрема в контексті виявлення активності, пов'язаної з визначеними іноземними терористичними організаціями.

Типології схем відмивання грошей, виявлених CTIF [2]



Цей документ, підготовлений бельгійським ПФР (CTIF), є комплексним зібранням типологій схем відмивання коштів, які були виявлені в рамках стратегічного аналізу. Документ спрямований на імплементацію Рекомендації 1 FATF, зокрема на підвищення обізнаності учасників системи фінансового моніторингу щодо актуальних ризиків. У ньому представлено 18 тематичних типологій схем відмивання, що ґрунтуються на реальних кейсах, а також охоплено низку особливо вразливих секторів економіки.

Ключовими тематиками є використання схем компенсації (обміну готівки на банківські перекази між злочинними угрупованнями), відмивання через комерційні угоди (TBML), діяльність професійних відмивачів коштів, використання гейткіперів — бухгалтерів, юристів, нотаріусів — як посередників, механізми підпільного банкінгу (зокрема через неофіційні системи переказу вартості (IVTS) та китайські фей-чен), зловживання корпоративними структурами (швидке створення та ліквідація компаній), платежі на користь третіх осіб, операції з нерухомістю, криптоактиви, азартні ігри, предмети розкоші, сектор готельно-ресторанного та кейтерингового бізнесу, торгівля діамантами, творами мистецтва та автомобілями, а також футбол та торгівля золотом.

Типології структуруються за єдиним принципом: вступний опис, детальний приклад конкретного випадку, зазначення основних предикатних злочинів, а також ключових термінів. Переважна більшість типологій демонструє мультикримінальну природу ВК: тіньова готівка походить із наркотрафіку, торгівлі людьми, шахрайства або ухилення від сплати податків і надалі легалізується через різноманітні схеми. Особливу увагу приділено використанню "компаній-оболонок", підставних осіб, підроблених рахунків-фактур, а також паралельних фінансових структур.

В окремих розділах розглядається відмивання через:

- сектор азартних ігор — через "гравців", що не грають, а лише змінюють готівку на жетони та повертають її як "виграш", а також використання онлайн-рахунків для платежів третіми особами;
- сектор предметів розкоші — використання коштовностей, елітних годинників та автомобілів як форм збереження або переміщення вартості;
- ринок мистецтва — фальшиві аукціони, підроблені оцінки та підконтрольні галереї;
- ринок криптоактивів — використання платформ у нерегульованих юрисдикціях, міксерів, VASPів та "мулів", які отримують кошти, конвертують у криптовалюту, а далі — у фіат.

[2] https://www.ctif-cfi.be/images/documents/French/Vademecum_blanchiment_de_capitaux.pdf

Типології також демонструють, що інструменти відмивання дедалі частіше переплітаються: одна схема може одночасно використовувати TBML, оплату за третіх осіб, і криптоактиви. Крім того, звіт звертає увагу на поширену участь фахівців (адвокатів, нотаріусів, бухгалтерів) у створенні або обслуговуванні інфраструктури ВК.

Насамкінець, CTIF наголошує, що своєчасне виявлення підозрілих фінансових паттернів можливе лише за умови глибокого розуміння таких типологій та співпраці між підзвітними установами, регуляторами та правоохоронними органами.

Висновки:

- **Компенсаційні схеми є одним з найпоширеніших інструментів професійного відмивання коштів у Бельгії**, що забезпечує "позабанківський" обмін готівки на перекази за підробленими рахунками — їх виявлення можливе через аналіз розбіжностей у секторах діяльності та відсутність економічного сенсу операцій.
- **Багато схем ВК мають транскордонний характер і спираються на використання фіктивних компаній та IVTS**, які дозволяють уникати як податкового, так і банківського нагляду, зокрема у співпраці з мережами в Китаї, ОАЕ та інших країнах з високим рівнем ризику.
- **Сектори, де обіг готівки є значним — сектор готельно-ресторанного та кейтерингового бізнесу, будівництво, ринок вживаних автомобілів, ринок діамантів — залишаються найвразливішими до ВК**, особливо при участі компаній-оболонок і повторюваних схем переказів з/на рахунки без економічного обґрунтування.
- **Професійні посередники та мультисекторальне використання схем (комбінація TBML, криптовалют, мистецтва, нерухомості тощо)** вимагають від підзвітних установ міждисциплінарного підходу, глибокого аналізу профілів клієнтів та контексту транзакцій, а також тісної міжнародної співпраці для обміну оперативною інформацією.

Регулювання

Нові правила розголошення інформації: Оновлення від AUSTRAC [3]

Прес-реліз AUSTRAC (Австралійського центру аналізу фінансових операцій і звітності) оголошує про набуття чинності нових правопорушень, пов’язаних із розголошенням інформації (tipping off offence) у рамках законодавства про боротьбу з відмиванням коштів та фінансуванням тероризму (AML/CTF). Він деталізує зміни до законодавства, які стосуються захисту інформації про підозрілі фінансові операції (Suspicious Matter Reports, SMR) та інших пов’язаних даних, що можуть зашкодити розслідуванням правоохоронних органів. З 31 березня 2025 року набули чинності оновлені положення, спрямовані на запобігання діям, які можуть перешкодити розслідуванням, а AUSTRAC опублікував нові рекомендації (tipping off guidance), щоб допомогти бізнесам зрозуміти ці зміни та дотримуватися зобов’язань щодо AML/CTF.

Захищена інформація включає дані про SMR, повідомлення, отримані відповідно до розділів 49 або 49B Закону про AML/CTF, запити на інформацію за цими розділами, а також дані про підозрілі транзакції, подані відповідно до скасованого Закону про SMR 1988 року. Розголошення такої інформації вважається правопорушенням, якщо воно може або ймовірно може зашкодити

[3] https://www.austrac.gov.au/new-tipping-offence-now-effect

розслідуванню. Розкриття інформації про підозрілу діяльність може дозволити злочинцям приховати або замаскувати незаконну діяльність, що ускладнює чи унеможливлює розслідування. Бізнеси відіграють ключову роль у запобіганні злочинній діяльності, тому вони повинні оцінювати, чи може розкриття інформації зашкодити поточним або майбутнім розслідуванням, незалежно від того, чи відомо їм про існування такого розслідування.

До 31 березня 2025 року заборонялося розкривати факт подання або вимоги подання SMR, а також будь-яку інформацію, яка могла б дозволити зробити висновок про подання такого повідомлення. Після 31 березня 2025 року забороняється розкривати захищену інформацію іншій особі (окрім уповноважених осіб AUSTRAC), якщо це може або ймовірно може зашкодити розслідуванню, наприклад, якщо інформація потрапить до суб'єкта звіту, його асоційованих осіб або буде оприлюднена публічно. Новий підхід забезпечує баланс між захистом розслідувань і наданням гнучкості для співпраці у боротьбі з відмиванням коштів, фінансуванням тероризму та іншими серйозними злочинами.

Компаніям рекомендовано ознайомитися з оновленим законодавством та новими рекомендаціями AUSTRAC, щоб зрозуміти, що означає «зашкодити розслідуванню» та як уникнути порушення.

Новий підхід зосереджений на оцінці того, чи може розголошення інформації зашкодити розслідуванню, а не на абсолютній забороні розкриття факту подання SMR, що дозволяє бізнесам ефективніше співпрацювати у боротьбі зі злочинністю, зберігаючи захист розслідувань. Бізнеси повинні оновити свої внутрішні правила та процедури навчання персоналу відповідно до нових вимог, щоб уникнути ненавмисних порушень.

Звіти окремих інституцій та експертів

Послаблення боротьби з відмиванням коштів у США: Наслідки для злочинності[4]

InSight Crime аналізує рішення адміністрації президента США Дональда Трампа послабити ключові закони, спрямовані на боротьбу з відмиванням коштів та корупцією, зокрема Закон про корпоративну прозорість (CTA) та Закон про запобігання корупції за кордоном (FCPA). Ці зміни, які адміністрація пояснює прагненням зменшити регуляторне навантаження на бізнес, на думку експертів, полегшують діяльність злочинних груп, особливо в Латинській Америці, сприяючи відмиванню грошей і хабарництву.

Адміністрація Трампа оголосила, що припиняє виконання вимог Закону про корпоративну прозорість, який зобов'язував американські компанії повідомляти федеральним органам інформацію про їхніх реальних власників. Цей закон мав на меті ускладнити використання підставних компаній для відмивання грошей, що є поширеним інструментом для злочинних організацій, зокрема в Латинській Америці. За оцінками Міністерства фінансів, США, як один із найбільших фінансових центрів світу, щороку стають майданчиком для відмивання приблизно 300 мільярдів доларів. Скасування вимог щодо розкриття бенефіціарних власників, оголошене 21 березня 2025 року, дозволяє злочинцям продовжувати приховувати проходження незаконних коштів через американські компанії, не побоюючись серйозного переслідування. Експерти, такі як Скотт Грейтак із Transparency

[4] https://insightcrime.org/news/how-trumps-anti-money-laundering-rollback-could-help-latam-criminals/

International та Ян Гері з Коаліції за фінансову підзвітність і корпоративну прозорість, називають це рішення кроком назад у глобальній боротьбі з фінансовими злочинами, що суперечить міжнародним стандартам, підтримуваним такими організаціями, як Група з розробки фінансових заходів боротьби з відмиванням грошей (FATF) та Світовий банк.

Окрім цього, 10 лютого 2025 року Трамп доручив призупинити на 180 днів виконання Закону про запобігання корупції за кордоном, який із 1977 року забороняє хабарництво для отримання ділових переваг на міжнародній арені. Латинська Америка історично є регіоном із високим рівнем справ, пов'язаних із цим законом: 44% усіх випадків його застосування стосувалися хабарів у цьому регіоні. Прикладом є гучна справа бразильської компанії Odebrecht, яка сплатила 3,5 мільярда доларів штрафу за систематичний підкуп посадовців у десятках країн. Призупинення виконання цього закону, за словами адміністрації, має на меті розробку нових рекомендацій для підвищення конкурентоспроможності американських компаній, але експерти побоюються, що це може сприяти зростанню корупції в регіонах із слабкими інституціями, таких як Латинська Америка. Водночас деякі фахівці зазначають, що інші американські та міжнародні закони все ще можуть стримувати компанії від хабарництва.

Висновки:

- **Необхідно відновити виконання Закону про корпоративну прозорість (CTA)**: Негайно поновити вимоги щодо звітності про бенефіціарних власників, виділивши додаткові ресурси Міністерству фінансів США для обробки даних і розширення доступу правоохоронних органів до інформації для виявлення відмивання грошей.
- **Спростити вимоги CTA для малого бізнесу:** Розробити спрощені форми звітності та запустити програми навчання для малих компаній, щоб зменшити регуляторне навантаження, зберігаючи прозорість і протидію використанню підставних компаній злочинцями.
- **Посилити альтернативні антикорупційні заходи:** Уточнити та активізувати застосування інших американських і міжнародних законів проти хабарництва під час призупинення FCPA, особливо в Латинській Америці, де слабкі інституції сприяють корупції.
- **Зберегти спеціалізовані антикорупційні підрозділи:** Скасувати рішення про розформування команд із протидії клептократії в Міністерстві юстиції США, щоб продовжити розслідування корупційних схем еліт у Латинській Америці, як у попередніх справах у Гондурасі та Панамі.

Ще одним важливим аспектом є розформування спеціалізованих підрозділів Міністерства юстиції США, які займалися боротьбою з корупцією. 5 лютого 2025 року генеральний прокурор Пем Бонді оголосила про ліквідацію команд із протидії клептократії, які співпрацювали з партнерами в Латинській Америці для розслідування корупційних схем у таких країнах, як Гондурас, Панама та Перу. Крім того, з'явилися повідомлення про плани скоротити ресурси підрозділу з питань громадської доброчесності, який розслідує корупцію всередині США, зокрема справу конгресмена Генрі Куельяра, якого звинувачують у отриманні хабарів від мексиканського банку. Хоча адміністрація заявляє про пріоритетність боротьби з картелями та транснаціональними злочинними організаціями, неясно, чи охоплює це протидію корупційним мережам еліт, які є поширеним явищем у Латинській Америці.

Ці зміни суперечать заявленій Трампом меті посилити боротьбу з організованою злочинністю. Послаблення контролю за підставними компаніями ускладнює відстеження потоків незаконних коштів, а призупинення антикорупційних заходів може сприяти безкарності в країнах із слабкими правоохоронними системами. Критики, зокрема представники бізнес-асоціацій, визнають, що виконання Закону про корпоративну прозорість створювало

труднощі для малого бізнесу через складність звітності, але пропонують альтернативні рішення, такі як спрощення форм, уточнення визначення бенефіціарних власників і розширення інформаційної підтримки, замість повного скасування закону. До того ж, навіть до цих змін закон стикався з обмеженнями: брак ресурсів для обробки даних про мільйони компаній і доступ до інформації лише для правоохоронців, що виключало можливість участі журналістів і дослідників у виявленні порушень. Наразі закон оскаржується в судах, і з огляду на ідеологічну близькість Верховного суду США до політики дерегуляції Трампа, його майбутнє залишається невизначеним.

Загалом документ підкреслює, що послаблення антикорупційних і AML заходів у США матиме далекосяжні наслідки, особливо для Латинської Америки, де злочинні організації активно використовують підставні компанії та корупційні схеми. Як глобальний фінансовий центр, США відіграють ключову роль у встановленні стандартів прозорості, і ці зміни можуть підірвати міжнародні зусилля з боротьби з фінансовими злочинами, потенційно заохочуючи інші країни послабити власні регуляції.

Глобальна мережа торговлі фентанілом: Китайський контроль, відмивання та роль TD Bank [5]

Дослідження, опублікована виданням The Bureau, розкриває деталі глобальної мережі торгівлі фентанілом та відмивання коштів, спираючись на ексклюзивне інтерв'ю з високопоставленим експертом уряду США, який проводить нагляд за розслідуваннями транснаціональних злочинів. Документ викриває складну систему, що пов'язує Комуністичну партію Китаю (КПК), китайські хімічні компанії, мексиканські картелі, китайські тріади та фінансові установи, зокрема банк Toronto-Dominion (TD Bank). Основна увага приділяється оперативним центрам у Торонто та Мехіко, які координують постачання прекурсорів, виробництво наркотиків та відмивання мільярдів доларів незаконних доходів, створюючи економіку, що проникає у легальні структури по всьому світу.

Експерт розкриває, що члени КПК володіють так званими "золотими акціями" у китайських хімічних компаніях, які експортують прекурсори для фентанілу. Ці акції забезпечують стратегічний контроль, вказуючи на причетність високопосадовців Китайської Народної Республіки до ланцюга постачання наркотиків. Деякі з цих компаній пов'язані з державними установами, включно з в'язницями, де виробляються компоненти фентанілу. Торонто виступає ключовим центром для відмивання грошей, де китайські злочинні угруповання, діючи безперешкодно між Онтаріо та Нью-Йорком, використовують інфраструктуру TD Bank завдяки його глибокій інтеграції з китайськими діаспорними громадами. Культурні особливості, такі як толерантне ставлення до великих готівкових транзакцій у цих громадах, сприяли нормалізації підозрілих операцій, коли молоді китайські студенти депонували мільйони доларів без належної перевірки.

У Мексиці та Канаді китайські фінансисти укладають угоди з мексиканськими картелями та тріадами, надаючи капітал для закупівлі прекурсорів, фінансові гарантії та механізми відновлення, які забезпечують безперебійну роботу ланцюга постачання. Ці угоди охоплюють не лише дистрибуцію, а й фінансування всієї економіки фентанілу — від виробництва до

[5] https://www.thebureau.news/p/ccp-golden-shares-toronto-laundering

вуличних продажів. Несподіваним елементом мережі є залучення китайських студентів у США, які збирають готівку з складів, пов'язаних із картелями, і перевозять її у сумках до філій TD Bank у Нью-Йорку, Нью-Джерсі та Коннектикуті. Цей процес є чітко структурованим і масштабним, використовуючи відсутність пильної уваги до готівкових операцій.

TD Bank виявився вразливим через слабкий контроль за дотриманням вимог щодо протидії відмиванню грошей. Розслідування показали, що працівники філій знали про підозрілі операції, але не вживали заходів, а регіональний нагляд був недостатнім. У 2024 році канадська фінансова розвідка (Fintrac) оштрафувала банк на 9,2 мільйона канадських доларів за порушення у сфері боротьби з відмиванням грошей, але експерт вважає цей штраф мізерним порівняно з масштабами проблеми. У США інтерес Міністерства юстиції до справи вказує на можливість кримінальних звинувачень. Крім того, доходи від фентанілу не просто осідають на рахунках картелів чи тріад — китайські брокери отримують значну частку, яка реінвестується у приховану економіку, що включає нерухомість, підставні компанії, салони краси, масажні салони та нелегальні виробництва. Це дозволяє інтегрувати незаконні кошти у глобальну економічну присутність Китаю.

Експерт спростовує твердження про незначну роль Канади у кризі фентанілу, які ґрунтуються на низьких даних про вилучення Службою митного та прикордонного контролю США (CBP) на північному кордоні. Ці дані не враховують вилучень іншими агентствами, такими як DEA, FBI, ICE чи місцева поліція, які фіксують значні потоки фентанілу та чорного ринку марихуани з Канади до США, особливо у регіон Трьох штатів. Китайські злочинні групи використовують спільну інфраструктуру для виробництва пігулок та канали відмивання, діючи між Онтаріо та Нью-Йорком. Мережа демонструє високу організацію, порівнянну з військовими операціями, координуючи логістику через континенти. Ключові постаті, такі як Цзе Чі Лоп, Сізі Лі та Чженлі Є Гун, створюють стійку структуру, що забезпечує постачання не лише наркотиків, а й обладнання, барвників, сполучних речовин та фінансових інструментів для відмивання трильйонів доларів.

На геополітичному рівні докази можуть призвести до визнання КПК транснаціональною організацією з торгівлі наркотиками, що відкриває шлях до санкцій проти лідерів Пекіна. Розслідування щодо TD Bank може спровокувати колективні позови від сімей, постраждалих від кризи. У Канаді правові перепони, такі як правило розкриття інформації Stinchcombe, ускладнюють розслідування, змушуючи поліцію ділитися розвідданими з адвокатами злочинців. Система також зачіпає інші банки, такі як Chase, Wells Fargo та Bank of America, але TD Bank виділяється через масштаби порушень. Позначення мексиканських картелів як терористичних організацій змінює пріоритети національної безпеки США, посилюючи увагу до банків, транспортних компаній та служб доставки, які контактують із цими групами.

Глобальна кіберзагроза з Бразилії: еволюція програми Grandoreiro [6]

Стаття, опублікована InSight Crime авторства Крістофера Ньютона, детально описує походження, еволюцію та глобальне поширення бразильського шкідливого програмного забезпечення Grandoreiro, яке стало серйозною загрозою для банківських систем у всьому світі.

Grandoreiro вперше з'явився у 2016 році як примітивне шкідливе ПЗ, написане на застарілій мові програмування Delphi, атакуючи бразильські банки, що порушувало неписане правило кіберзлочинців уникати атак на власній території, щоб не привертати увагу місцевих правоохоронців. Код містив коментарі португальською мовою, а сервери базувалися в Бразилії, вказуючи на місцевих програмістів. У 2017 році правоохоронці визнали Grandoreiro критичною загрозою, але розробники швидко адаптувалися, вдосконалюючи код і співпрацюючи з іншими

[6] https://insightcrime.org/news/the-global-malware-menace-born-in-brazil/

групами, ділячись кодом із творцями інших бразильських шкідливих програм, таких як Guildma, Javali та Melcoz.

Протягом кількох років Grandoreiro зазнав значних змін: розробники навчилися обходити антивірусне програмне забезпечення, ускладнювати аналіз коду, шифрувати трафік і додавати нові функції. До 2020 року воно перетворилося на складне шкідливе ПЗ типу Remote Access Trojan (RAT), яке дозволяло зловмисникам віддалено керувати зараженими комп'ютерами, створюючи фальшиві вікна чи спливаючі повідомлення, що імітують банківські сайти, викрадаючи логіни, паролі, токени двофакторної автентифікації, контролюючи мишу, записуючи натискання клавіш, копіюючи буфер обміну та навіть активуючи вебкамеру. У 2020 році Grandoreiro розпочав міжнародну експансію, атакуючи банки в Аргентині, Перу, а згодом поширився на Латинську Америку, Європу та інші регіони світу. Для цього мережа запровадила модель malware-as-a-service, де основні розробники створюють і вдосконалюють код, а інші учасники виконують допоміжні ролі, такі як фішинг та переміщення коштів.

Фішингові атаки часто маскувалися під листи від офіційних установ, наприклад, податкової служби Аргентини (AFIP), із закликами перейти за шкідливими посиланнями або завантажити заражені файли, використовуючи тактику троянів, ховаючи шкідливий код у безпечних на вигляд програмах. Grandoreiro функціонує як ієрархічна організація: на вершині — розробники, які створюють і вдосконалюють ПЗ, контролюють сервери та отримують основну частку прибутку; лідери осередків у різних країнах організовують фішингові кампанії та залучають грошових мулів; мули — місцеві жителі, які надають свої банківські рахунки для переміщення вкрадених коштів, отримуючи невеликий відсоток. Грошові мули розмивають грошовий слід через численні транзакції, кошти конвертуються в криптовалюту для ускладнення відстеження, а близько 70% прибутку надсилається на сервери в Бразилії. Процес від викрадення коштів до їхньої передачі займає приблизно 20 хвилин.

Після зараження комп'ютера Grandoreiro працює у фоновому режимі, збираючи інформацію про жертву, встановлені антивіруси та банківські програми, активується під час відвідування банківських сайтів, імітуючи легітимні сторінки для викрадення даних, а зловмисники можуть використовувати вкрадені дані для входу в акаунт жертви або керування її пристроєм.

Попри зусилля правоохоронців, Grandoreiro залишається активним. У січні 2024 року в Бразилії заарештували п'ятьох підозрюваних, які викрали 3,9 млн доларів, у травні 2024 року в Аргентині ліквідували місцевий осередок, заарештувавши 16 осіб, які викрали 1,6 млн доларів, а в 2025 році аргентинська влада провела додаткові арешти. Не зважаючи на це, основні розробники залишаються на свободі, а шкідливе ПЗ еволюціонує, розгалужуючись на дві окремі версії, ймовірно, розроблені різними групами.

Grandoreiro демонструє високу стійкість завдяки децентралізованій структурі, де осередки діють незалежно, спілкуючись через приватні форуми та зашифровані месенджери. Стаття підкреслює зростання зв'язків між кіберзлочинністю та традиційними злочинними мережами, такими як наркоторгівля, що ускладнює боротьбу з подібними групами.

Тіньова флотилія: Як російський бізнесмен обходить санкції через Данію [7]

Публікація від Danwatch є частиною масштабного журналістського розслідування, проведеного спільно з норвезьким мовником NRK. Вона викриває складну шахрайську схему, яка дозволяє російській «тіньовій флотилії» нафтових танкерів обходити західні санкції, використовуючи фіктивну страхову компанію в Данії.

У центрі історії — російський бізнесмен, який створив у Данії компанію Ingosstrakh (не пов'язану з російською страховою компанією «Ингосстрах»), що видає підроблені страхові сертифікати для суден, які перевозять російську нафту, зокрема через данські територіальні води. Розслідування підкреслює системні вразливості в роботі данської влади, екологічні та економічні ризики, а також політичні наслідки недостатньої пильності в умовах геополітичної кризи.

Після початку повномасштабного вторгнення Росії в Україну в лютому 2022 року країни G7, Європейський Союз і Австралія запровадили санкції, спрямовані на обмеження експорту російської нафти. Одним із ключових елементів цих санкцій стала вимога, щоб судна, які перевозять російську нафту, мали страховку від компаній, визнаних цими країнами. Це значно ускладнило логістику для Росії, оскільки провідні міжнародні страховики, такі як члени Міжнародної групи клубів взаємного страхування (International Group of P&I Clubs), припинили співпрацю з російськими суднами. У відповідь Росія сформувала так звану «тіньову флотилію» — мережу старих, часто технічно несправних танкерів, які регулярно змінюють назви, прапори, власників і порти приписки, щоб уникнути ідентифікації та санкцій. Ці судна перевозять нафту до країн, які не приєдналися до санкцій, зокрема до Китаю, Індії та Туреччини, забезпечуючи Росії мільярдні доходи, що фінансують її військову агресію.

Данія відіграє особливу роль у цьому процесі через своє географічне розташування. Більшість танкерів, що транспортують російську нафту з Балтійського моря до світових ринків, проходять через данські протоки, зокрема Великий Бельт і Малий Бельт. Данське морське управління (Danish Maritime Authority) зобов'язане перевіряти страхові документи цих суден, щоб переконатися, що вони відповідають міжнародним стандартам і санкційним вимогам. Однак розслідування Danwatch і NRK виявило, що ці перевірки є поверховими, що дозволяє тіньовим танкерам безперешкодно використовувати фальшиві страхові сертифікати, видані фіктивною компанією Ingosstrakh. Журналісти з'ясували, що ця компанія не має ліцензії на страхову діяльність, не входить до списку визнаних страховиків G7/ЄС, не володіє фінансовими резервами для покриття страхових зобов'язань і фактично існує лише на папері. Її документи містять численні помилки, неточності та явні ознаки підробки, але данські органи влади не проводять достатньо ретельних перевірок, щоб виявити ці порушення.

Розслідування детально описує механізм шахрайства. Російський бізнесмен, ім'я якого не розкривається в статті через триваюче слідство, зареєстрував Ingosstrakh у Данії, використовуючи її як інструмент для видачі фальшивих страхових сертифікатів. Ці документи надають тіньовим танкерам видимість законності, дозволяючи їм проходити через данські води без затримок. Норвезька поліція, яка також розслідує цю схему, висунула звинувачення чотирьом особам у підробці документів і незаконній видачі страхових паперів. Журналісти наводять приклади конкретних суден, які використовували ці фальшиві сертифікати для

[7] https://danwatch.dk/en/forged-papers-and-a-fake-company-how-russian-businessman-cheats-danish-authorities/

транспортування російської нафти через данські протоки до азійських ринків. Наприклад, згадуються танкери, які завантажували нафту в російських портах, таких як Усть-Луга чи Приморськ, і прямували до портів у Китаї чи Індії, використовуючи підроблені документи Ingosstrakh.

Стаття акцентує на кількох ключових ризиках, пов'язаних із цією схемою. По-перше, екологічний ризик: багато танкерів тіньової флотилії є старими, зношеними суднами з низьким рівнем технічного обслуговування. У разі аварії, наприклад, розливу нафти в данських протоках, наслідки для морського середовища Балтійського моря можуть бути катастрофічними. Балтійське море вже є екологічно вразливим регіоном, і будь-який значний інцидент може завдати шкоди екосистемам Данії, Швеції та інших прибережних країн. По-друге, економічний ризик: шахрайська схема дозволяє Росії продовжувати експортувати нафту, обходячи санкції, що послаблює їх ефективність. За оцінками експертів, Росія заробляє мільярди доларів щороку на цьому експорті, що фінансує її військові операції в Україні. По-третє, політичний ризик: недостатня пильність данської влади підриває репутацію Данії як країни, що підтримує міжнародні санкції, і може викликати критику з боку союзників по ЄС і НАТО.

Розслідування також висвітлює реакцію на проблему та перспективи її вирішення. Норвезька поліція активно співпрацює з міжнародними партнерами, щоб притягнути до відповідальності причетних до схеми. У Данії розпочато перевірки діяльності Ingosstrakh, але на момент публікації статті конкретних заходів проти компанії не було вжито. Експерти, опитані Danwatch, наголошують на необхідності посилення перевірок страхових документів, створення міжнародної бази даних для відстеження суден тіньової флотилії та їхніх страхових сертифікатів, а також покращення координації між країнами Балтійського регіону. Стаття зазначає, що танкери проходять не лише через данські, а й через шведські, фінські та інші територіальні води, що робить проблему регіональною. Окрім того, журналісти звертають увагу на потребу вдосконалення технічних перевірок суден, щоб мінімізувати екологічні ризики.

Оцінка ризиків протидії відмиванню коштів для платіжного сектору [8]

Документ, підготовлений аналітиками компанії ComplyAdvantage, є всебічним керівництвом з оцінки ризиків, пов'язаних із ВК/ФТ та обходом санкцій у секторі платіжних послуг (PSPs). Зважаючи на вибухове зростання цифрових платіжних сервісів — за прогнозами, до $2,9 трлн до 2030 року — автори акцентують на тому, що водночас пропорційно зростають і ризики фінансових злочинів, зокрема використання PSPs для структурування (smurfing), змішування коштів, залучення офшорних рахунків, використання складних схем володіння активами.

Платіжний сектор не є однорідним: різні бізнес-моделі, продукти, юрисдикції та канали створюють неоднакові профілі ризику. Основні фактори притаманного ризику включають: тип клієнта (наприклад, нерезиденти, PEPи, клієнти з ігрового чи криптовалютного секторів), географічне охоплення (особливо транскордонні операції з юрисдикціями високого ризику), обсяги та частота

[8] https://get.complyadvantage.com/insights/payment-red-flag-guide

транзакцій, використання інновацій (включно з анонімними криптогаманцями), а також участь посередників (агентів).

У розділі "Risk Snapshot" надано візуальне зіставлення продуктів і каналів відповідно до рівня їхнього притаманного ризику у контексті санкцій, ВК, ФТ та шахрайства. Найбільші ризики зосереджені в таких продуктах, як криптовалютні гаманці, валютообмінні операції, перекази готівкою, та e-commerce з високим ступенем анонімності й сегментації.

Документ приділяє особливу увагу новим та еволюціонуючим загрозам. Зокрема, окреслено шляхи зловживань через money muling (мулінг), transaction laundering (відмивання коштів через e-commerce), third-party merchant acquiring (залучення третіх сторін до обслуговування торговців), white labeling (використання ліцензії PSP третіми сторонами), та віртуальні IBANи, які маскують справжню юрисдикцію рахунку.

Контрольна рамка, запропонована авторами, базується на пропорційному та ризик-орієнтованому підході. Сюди входять гнучкі процедури KYC та CDD, зокрема адаптивний скринінг клієнтів на підставі юрисдикції, сектору та професії, скринінг транзакцій (включаючи криптогаманці до і після транзакції), використання алгоритмів нечіткого пошуку (fuzzy matching), а також поведінкової аналітики для ідентифікації підозрілих шаблонів у режимі реального часу.

Додатки деталізують критерії оцінки ризиків, такі як транскордонний характер, швидкість руху коштів, анонімність, участь третіх сторін, складність структури, прозорість, способи доставки послуг та використання нових технологій.

Висновки:

- **Криптовалютні продукти та віртуальні IBANи становлять високий ризик ВК/ФТ та обходу санкцій** через анонімність, децентралізовану структуру, складність відстеження та обмежений регуляторний контроль. Необхідне впровадження попереднього скринінгу гаманців і транзакцій для підвищення прозорості.
- **Сектор e-commerce, зокрема платформи з низькими вимогами до входу, є вразливим до transaction laundering**, тому PSP мають впроваджувати посилені KYC- та onboarding-процедури для торговців.
- **Для ефективного зниження ризиків PSP мають переходити від ізольованих до інтегрованих контрольних систем**, поєднуючи транзакційний моніторинг, скринінг клієнтів і оцінку поведінки в режимі реального часу з урахуванням типологій фінансових злочинів.

MiCAR: Інституційний посібник для європейського ринку цифрових активів [9]

Звіт присвячено глибокому аналізу трансформації цифрового фінансового ринку Європейського Союзу під впливом повного впровадження Регламенту про ринки криптоактивів (MiCAR). Він окреслює ключові тренди, які формують новий регуляторний і ринковий ландшафт, з особливим фокусом на розширення використання євро у цифрових активах, стрімке зростання інституційної участі, посилення ролі кастодіальних послуг і регуляторну конкуренцію з боку США, Сінгапуру, Гонконгу та ОАЕ.

Одним із головних векторів трансформації є стрімке зростання обсягів торгівлі в парах з євро — обсяг торгівлі EUR-фіатними парами зріс на 74,3% за рік, перевищивши €300 млрд, що стало можливим завдяки вдосконаленій банківській інфраструктурі, розвитку EUR-стейблкоїнів, а також розширенню присутності європейських бірж. Хоча USD і далі домінує глобально, доля

[9] https://data.coindesk.com/reports/micar-the-institutional-playbook-for-europes-digital-asset-market

EUR-фіатних пар у світовому обсязі торгівлі досягла 6,66%. Найліквідніша пара — EUR/USDT — невдовзі зазнає втрат через виключення USDT з європейських платформ відповідно до вимог MiCAR, що спричиняє перерозподіл ліквідності на користь MiCAR-сумісних стейблкоїнів (USDC, EURC, EURCV).

Звіт наголошує на важливості регульованої кастодіальної інфраструктури для забезпечення довіри до цифрових активів в інституційному середовищі. Після краху FTX, саме регульовані кастодіани стали критичними гравцями в забезпеченні збереження активів, запобіганні контрагентським ризикам та виконанні вимог до капіталу, управління ризиками і безпеки. MiCAR вводить чітку відповідальність за втрату активів і надає кастодіальним послугам статус основного виду діяльності, на відміну від попереднього трактування як допоміжної послуги.

Окремий розділ присвячено розвитку EUR-стейблкоїнів, які залишаються у зародковому стані, займаючи лише 2,2% обсягів торгівлі в парах з євро. Втім, регуляторна визначеність і поступова відмова від несумісних токенів, таких як EURT від Tether, формує основу для зростання ринку сумісних токенів (наприклад, EURC, EURCV, EURQ, EURD). Очікується, що такі активи надалі використовуватимуться не стільки як засіб котирування, скільки як інструмент збереження євро on-chain.

Розвиток біржової інфраструктури у ЄС демонструє зростання довіри ринку до MiCAR: з 11 бірж із підтримкою EUR-пар у 2016 році до майже 60 у 2024-му. Найбільші гравці — Bitvavo, Kraken, Coinbase, Binance і Bitstamp — контролюють майже 90% ринку EUR-фіатних транзакцій. Водночас європейські біржі стикаються з жорсткою конкуренцією з боку США, де запуск біржових біткоїн-ETF призвів до зростання обсягу активів під управлінням на 2207%, у порівнянні зі 104% у Європі.

Висновки:

- **MiCAR повністю змінив правила гри для європейського ринку цифрових активів**, зробивши його найбільшою гармонізованою регульованою юрисдикцією, що приваблює інституційних гравців завдяки прозорості, відповідальності кастодіанів та спрощенню виходу на ринок.
- **Виключення USDT з європейських бірж** через невідповідність MiCAR відкрив шлях для зростання ролі стейблкоїнів сумісних з євро (EURC, EURCV), що вимагає від платформ і кастодіанів адаптації до нового середовища ліквідності.
- **Регульовані кастодіальні послуги стали критично важливими** для інституційного прийняття цифрових активів, зобов'язуючи провайдерів відповідати підвищеним вимогам до безпеки, звітності та розподілу ризиків.
- **Інновації на зразок Off-Exchange Settlement і Off-Venue Settlement дозволяють інституційним інвесторам торгувати, не передаючи активи біржам**, що значно знижує контрагентський ризик та сприяє інтеграції цифрових активів у традиційну фінансову систему.

Окрему увагу в документі приділено інноваційним підходам до зберігання та переміщення цифрових активів, зокрема Off-Exchange Settlement (OES) і Off-Venue Settlement (OVS) — двом технологіям, які суттєво змінюють взаємодію між інституційними інвесторами, біржами та торговими майданчиками. OES дозволяє зберігати активи у кастодіальному сховищі поза межами біржі, але водночас відображати їх на біржовій платформі як доступні до торгівлі. Завдяки цьому активи залишаються в безпечному

сховищі, а сам процес купівлі-продажу відбувається без їх фізичного переміщення, що мінімізує контрагентські ризики, пришвидшує виконання операцій та знижує витрати на перекази. OVS є розширенням цієї моделі — воно забезпечує можливість здійснення розрахунків за операціями не лише на централізованих біржах, але й поза ними, зокрема з OTC-деськами та маркет-мейкерами. Таким чином, OVS дозволяє інвесторам взаємодіяти з ширшим колом контрагентів та ліквідності без необхідності передоплати чи переведення активів на сторонні рахунки. Прикладом такої моделі є рішення Zodia Interchange, що дозволяє інституційним гравцям зберігати активи у кастодіальному середовищі, а розрахунки здійснювати з будь-якими контрагентами, які також відповідають вимогам MiCAR. Це сприяє підвищенню контролю, прозорості та безпеки у сфері цифрових фінансів.

Звіт завершується прогнозом щодо поступового зростання обсягів торгівлі в євро, збільшення кількості зареєстрованих VASPів у ЄС, зміцнення позицій ЄС як провідної юрисдикції для інституційних гравців та подальшої конвергенції традиційного і цифрового фінансових ринків.

ВНУП

Компалєнс з ПВК для CSP

Однією з пріоритетних вимог до осіб, які надають послуги щодо створення, забезпечення діяльності або управління юридичними особами, трастами та іншими утвореннями без статусу юридичної особи (CSP), є дотримання законодавства у сфері запобігання відмиванню коштів, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення. У контексті сучасних глобальних викликів та зростання зловживань корпоративними структурами, саме ці суб'єкти відіграють ключову роль у запобіганні використанню таких утворень для злочинних цілей.

Відповідно до вимог законодавства України, CSP визнаються суб'єктами первинного фінансового моніторингу та мають забезпечити впровадження повноцінної системи внутрішнього контролю на основі ризик-орієнтованого підходу. Для цього необхідно виконувати низку взаємопов'язаних дій — від офіційної реєстрації в Держфінмоніторингу до безперервного моніторингу ділових відносин і належного документування. Нижче представлено послідовну модель ПВК-процесу для CSP в Україні, яка охоплює ключові обов'язки, процедури та регуляторні орієнтири.

1. **Реєстрація як суб'єкта первинного фінансового моніторингу (СПФМ) та призначення відповідального працівника.** Першим обов'язковим кроком є офіційне набуття статусу СПФМ. Така особа повинна подати повідомлення про початок діяльності до Державної служби фінансового моніторингу України. Це дає підставу вважати CSP відповідальним за дотримання вимог у сфері ПВК/ФТ. Якщо цього не зробити, діяльність визнається такою, що ведеться з порушенням закону, і може призвести до санкцій. Юридична особа повинна офіційно призначити працівника, який відповідатиме за організацію і здійснення фінансового моніторингу. Такий фахівець зобов'язаний володіти відповідною кваліфікацією, проходити регулярне навчання та брати участь у всіх процесах виявлення ризиків, перевірки клієнтів і подання повідомлень до Держфінмоніторингу.
2. **Проведення внутрішньої оцінки ризиків ВК/ФТ.** CSP має розробити та впровадити систему оцінки ризиків відмивання коштів та фінансування тероризму, яка охоплює всю діяльність підприємства. Це передбачає врахування ризиків, пов'язаних із типом клієнтів, юрисдикціями, послугами, каналами їх надання та попереднім досвідом. Оцінка ризиків повинна бути задокументована, затверджена керівництвом та оновлюватися щонайменше раз на 3 роки або при істотних змінах.

3. **Розробка та оновлення внутрішніх політик, процедур і контролю.** Це один із ключових елементів комплаєнс-системи CSP. Внутрішні документи повинні, зокрема, визначати (не вичерпний перелік):
   - порядок ідентифікації та перевірки клієнтів;
   - критерії ризику;
   - дії у випадках підозри на ВК/ФТ;
   - процедури звітування;
   - вимоги до навчання персоналу;
   - збереження документації. Документи затверджуються керівництвом і підлягають регулярному оновленню.
4. **Проведення KYC та належної перевірки клієнтів.** Перед встановленням ділових відносин CSP повинен провести ідентифікацію та верифікацію клієнта — фізичної або юридичної особи. Це включає:
   - збір паспортних/реєстраційних даних;
   - виявлення кінцевих бенефіціарних власників;
   - визначення статусу публічної особи (PEP);
   - збір інформації щодо джерел походження коштів (за потреби). Перевірка проводиться з урахуванням результатів оцінки ризику; тощо
5. **Проведення скринінгу.** Клієнта і його КБВ перевіряються за:
   - списками терористів і осіб, пов'язаних з ФТ (національним переліком);
   - санкційними списками (у тому числі ООН, ЄС, США, Канади);
   - базами даних PEP;
   - іншими ризиковими реєстрами. У разі виявлення збігу CSP зобов'язаний зупинити операції та подати повідомлення до Держфінмоніторингу; тощо
6. **Профілювання ризику клієнта.** На основі попередніх етапів клієнт класифікується як такий, що має низький, середній або високий ризик. До уваги береться ряд даних:
   - тип клієнта (фізособа, юрособа, траст тощо);
   - юрисдикція реєстрації;
   - організаційно-правова форма;
   - тип послуги;
   - спосіб взаємодії (особисто чи дистанційно);
   - джерела походження коштів. Клієнти з високим ризиком обов'язково проходять поглиблену перевірку (EDD); тощо
7. **Поглиблена перевірка клієнта (EDD).** Для високоризикових клієнтів CSP повинен провести додаткові дії:
   - перевірити джерело походження коштів та статків;
   - зібрати додаткові документи та пояснення;
   - забезпечити, щоб оплати проводилися тільки з рахунків, що належать клієнту;
   - отримати письмовий дозвіл керівника підприємства на встановлення або продовження ділових відносин; тощо
8. **Постійний моніторинг ділових відносин.** Моніторинг не завершується після започаткування ділових відносин. CSP зобов'язаний:
   - відслідковувати транзакції клієнта;
   - оцінювати відповідність операцій очікуваному профілю;
   - проводити повторну перевірку клієнта у разі появи нових ризиків або інформації;
   - оновлювати документи за потреби; тощо
9. **Подання повідомлення про підозрілі фінансові операції (STR).** У разі виявлення ознак, що можуть свідчити про спробу відмивання коштів, фінансування тероризму або обхід санкцій, CSP зобов'язаний подати повідомлення до Держфінмоніторингу.

10. **Повторення процесу у разі змін.** У випадку зміни бенефіціарного власника, структури власності, географії, ризикового профілю клієнта чи появи нових обставин, CSP повинен повторно провести етапи перевірки: від скринінгу до переоцінки ризиків. Це дозволяє постійно підтримувати актуальність профілю клієнта.
11. **Зберігання документації.** Всі зібрані дані щодо ідентифікації, верифікації, оцінки ризику, моніторингу, повідомлень та рішень мають зберігатися не менше 5 років після завершення ділових відносин або проведення одноразової операції. Дані повинні бути доступні для перевірки регуляторами.

Запровадження системного комплаєнс-процесу, відповідного до національних та міжнародних стандартів, дає змогу CSP не лише виконувати нормативні зобов'язання, але й ефективно управляти ризиками, захищати власну діяльність від репутаційних втрат та сприяти зміцненню фінансової системи держави.

Забезпечення своєчасної перевірки клієнтів, проведення профілювання ризиків, запровадження процедур моніторингу, а також готовність і здатність виявляти та повідомляти про підозрілі дії — це не просто вимога законодавства, а ознака зрілого та відповідального провайдера корпоративних послуг. Комплексне виконання кожного з наведених етапів процесу забезпечує належний рівень комплаєнсу та сприяє загальному зміцненню прозорості бізнес-середовища в Україні.

Рекомендовані матеріали та заходи

Китайський фантом: Розкриваючи таємниці фінансової секретності [10]

Епізод #152 подкасту "The Taxcast" від Tax Justice Network має назву "The Chinese Phantom". Подкаст зосереджується на розслідуванні діяльності китайського торговця зброєю Лі Фан Вея, відомого як Карл Лі, проблемах фінансової секретності, неефективності санкцій, а також поточних подіях у сфері податкової справедливості у США та Великобританії.

Центральною темою є історія Лі Фан Вея, якого ФБР розшукує з винагородою у 5 мільйонів доларів, але він два десятиліття уникає арешту. Журналіст Фредерік Обермаєр, співавтор книги "The Chinese Phantom: The Hunt for the World's Most Dangerous Arms Dealer", разом із колегами з International Consortium of Investigative Journalists та Paper Trail Media розкриває, як Лі, звинувачений у допомозі Ірану в ракетній програмі та постачанні зброї Росії для війни в Україні, використовує непрозорі фінансові структури. Він змінює назви компаній, наприклад, перейменувавши Wealthy Ocean Enterprise Ltd. на ABC Metallurgy, щоб обійти санкції США. Обермаєр підкреслює, що навіть ФБР і ЦРУ не можуть його затримати через брак прозорості та пособництво банків і юрисдикцій, таких як Сейшели.

Цікаво, що в Китаї, попри автократичний режим, реєстри компаній і судові документи є більш доступними, ніж у багатьох західних країнах, таких як, наприклад, Німеччина, завдяки унікальним ID-номерам, які містять дані про регіон народження, дату народження та стать. Водночас Китай, ймовірно, захищає Лі, адже офіційних звинувачень проти нього немає, хоча дипломатичний тиск зростає.

Епізод також аналізує неефективність санкцій через фінансову секретність. Юрисдикції з високим рівнем секретності дозволяють обходити санкції, а Обермаєр закликає до публічних

[10] https://podcasts.taxjustice.net/episode/152-the-chinese-phantom/

реєстрів кінцевих бенефіціарних власників (КБВ), критикуючи США за непублічний Закон про корпоративну прозорість і Німеччину за невиконання обіцянок щодо КБВ-реєстру. У США через судові позови та політичний тиск Закон про корпоративну прозорість не застосовуватимуть до американських компаній, що зменшує його ефективність: лише 12,000 іноземних компаній звітуватимуть замість 32 мільйонів загалом.

Подкаст підкреслює, що фінансова секретність сприяє війнам, корупції та нерівності, закликаючи до тиску на юрисдикції з такою секретністю, публічності КБВ-реєстрів і відповідальності посередників.

Саміт про майбутнє платежів [11]

Future of Payments Summit 2025 — це масштабна подія, організована компанією Comply Advantage, яка відбудеться 25 червня 2025 року з 16:00 до 20:00 за київським часом (2:00 PM – 6:00 PM BST). Цей саміт обіцяє стати наймасштабнішим в історії компанії, зібравши понад тисячу учасників для обговорення ключових тенденцій у сфері платежів, фінансових технологій та регуляторного комплаєнсу.

Основні теми саміту:

- Роль RegTech у розвитку бізнесу з використанням миттєвих платежів (RTPs): Обговорення того, як технології регуляторного комплаєнсу можуть сприяти зростанню бізнесу в умовах стрімкого розвитку миттєвих платежів.
- Трансформаційний вплив Agentic AI на боротьбу з фінансовими злочинами: Дослідження можливостей штучного інтелекту в адаптації до ризиків, пріоритизації загроз та покращенні виявлення фінансових злочинів.
- Навігація по кривій зрілості комплаєнсу: Аналіз стадій розвитку комплаєнс-функцій в організаціях та шляхів їх удосконалення.
- Огляд нових продуктів Comply Advantage: Презентація майбутніх оновлень та інновацій у продуктах компанії.

Формат заходу:

Саміт проходитиме у віртуальному форматі, що дозволяє учасникам з усього світу приєднатися до події. Учасники матимуть можливість вибирати сесії за інтересами, а також переглядати демонстрації продуктів у реальному часі. Цей саміт буде особливо корисним для фахівців у сферах фінансових технологій, комплаєнсу, управління ризиками та регуляторного середовища.

Участь у Future of Payments Summit 2025 надає можливість отримати актуальні знання, обмінятися досвідом з колегами та ознайомитися з передовими рішеннями у сфері фінансових технологій та комплаєнсу. Реєстрація на захід вже відкрита.

[11] https://get.complyadvantage.com/insights/future-of-payments-summit-2025?_gl=1*1mbwtqj*_gcl_aw*R0NMLjE3Mzg2NjQ0MTcuQ2p3S0NBaUE5SUM2QmhBM0Vpd0FzYmx0T0dwYm9VcTVuS2xIaTQ5NURldU9Rcmdfb003QkVEMFV3emtodlNVY0NMUzFscURXYkFxMjN4b0NmeFFRQXZEX0J3RQ..*_gcl_au*MTg2NTAwOTg3OS4xNzM2MjQ5NjIyLjc2OTc5OTIzMy4xNzQzNTA2MTM4LjE3NDM1MDYxNTE.*_ga*MTEzNjcyMTU0NC4xNzIwNTE0NzQy*_ga_SP15H3TF04*MTc0MzU4NTE5MS4xODUuMS4xNzQzNTk3MDEzLjU3LjAuMTAxMjYxNjkz

RUSI Land Warfare Conference 2025 [12]

У червні 2025 року Лондон стане центром військово-аналітичної думки, де зустрінуться генерали, дослідники, технологи та оборонні аналітики з усього світу, щоб визначити, як має виглядати сухопутна війна у XXI столітті. RUSI Land Warfare Conference 2025, яка проходитиме 17–18 червня у Church House, Westminster, — це стратегічний компас для демократичних держав, які шукають відповіді на виклики нової глобальної архітектури безпеки.

Цьогорічна подія є надзвичайно актуальною, враховуючи не лише триваючу агресію росії проти України, але й активізацію регіональних загроз на Близькому Сході та стратегічне зближення росії з Іраном і Північною Кореєю. Конференція ставить за мету розібратися, як ці фактори трансформують сучасну війну, і яким чином західні армії мають реагувати.

Обговорення будуть присвячені як фундаментальним стратегічним викликам, так і прикладним аспектам — від оперативного управління й організації сил до новітніх технологій, які змінюють правила гри. Перша сесія відкриється виступом генерала Патріка Сандерса, Головнокомандувача британської армії, а надалі відбудуться панелі з участю високопоставлених командувачів з Литви, Польщі, США, Німеччини, Австралії, Канади, Швеції. Учасники обговорюватимуть, як зробити війська більш маневреними, живучими та летальними, адаптованими до сучасного бойового простору, де майже немає прикриття і все визначається швидкістю та здатністю до цифрової інтеграції.

День другий відкриється виступом генерала Крістофера Донахью (США), а подальші сесії будуть присвячені тактичним інноваціям, досвіду з України та Близького Сходу, а також оцінкам готовності європейських армій. Особливо очікуваними є доповіді Олександри Азархіної (We Build Ukraine) про український досвід, професора Ейтана Шаміра (Ізраїль), Емми Білс (European Institute of Peace), а також виступ Адмірала Тоні Радакіна, Начальника штабу оборони Великобританії, який завершить конференцію.

На конференції відбудеться презентація практичних кейсів, у тому числі від представників Palantir, Defence Science and Technology Laboratory, CNAS, IISS, а також дослідників з Німеччини, Великобританії та Австралії. Комерційні технології подвійного призначення та інноваційні рішення від таких компаній, як Babcock, Lockheed Martin, Leonardo, MBDA, Moog та Janes, стануть важливою частиною діалогу про майбутнє бойових систем.

Цей захід буде корисним для офіцерів високої та середньої ланки, фахівців з військового планування, оборонних аналітиків, представників промисловості, науковців, а також для країн-союзників і партнерів, що прагнуть адаптуватися до нового рельєфу глобальної безпеки. RUSI забезпечує платформу, де точаться не лише дискусії про сучасне поле бою, але й про те, якою має бути стратегічна культура нової доби.

Темні гроші та дезінформація: битва за чесність виборів [13]

Це одна з найактуальніших подій у сфері захисту демократії, яка відбудеться 29 квітня 2025 року у центральному офісі RUSI (61 Whitehall, Лондон). У той час, коли Велика Британія готується до місцевих та муніципальних виборів, тема виборчої доброчесності набуває особливої ваги. Подія

[12] https://my.rusi.org/events/rusi-land-warfare-conference-2025/tickets-and-venue.html
[13] https://my.rusi.org/events/dark-money-disinformation-the-battle-for-electoral-integrity.html?utm_campaign=e-shot-2025&utm_medium=email

організована Центром фінансів і безпеки (Centre for Finance and Security) при RUSI у партнерстві з громадською організацією Democratys, яка спеціалізується на інформуванні суспільства про демократичні процеси через освітні події, подкасти та медіа-розслідування.

У фокусі дискусії — вплив "темних" грошей, дезінформації, великих технологічних платформ і зовнішнього втручання на прозорість та легітимність виборчих процесів. Спікери та учасники обговорять, яким чином ці фактори руйнують суспільну довіру до політичних інституцій, як фінансова і цифрова непрозорість уможливлюють втручання у вибори, та які механізми потрібно посилювати для підвищення стійкості демократій.

Модераторами дискусії стануть Оуен Беннетт-Джонс (журналіст BBC) та Ніна дос Сантос (екс-ведуча CNN), які також є ведучими подкасту Ctrl Alt Deceit: Democracy in Danger від Democratys. Серед основних спікерів — Том Кітінг (директор Центру фінансів і безпеки, RUSI), Даррен Г'юз (керівник Electoral Reform Society) та професорка Джина Нефф (директорка Minderoo Centre for Technology & Democracy при Кембриджському університеті та професорка в галузі ШІ у Queen Mary University). Також анонсовано участь інших експертів, які будуть оголошені найближчим часом.

Цей захід — не лише аналітична подія, а й стратегічний форум, що поєднує експертизу у сфері регулювання фінансування політичних кампаній, технологічного нагляду, штучного інтелекту та цифрової безпеки. Він буде корисним для:

- фахівців з виборчого законодавства та доброчесності;
- політиків і державних службовців, відповідальних за захист виборів;
- журналістів-розслідувачів;
- аналітиків у сфері боротьби з дезінформацією;
- представників громадянського суспільства, які прагнуть захистити демократичні процеси від маніпуляцій.

Обговорення відбудеться у відкритому форматі, а його результати, з урахуванням актуальності виборчого циклу, можуть мати прямий вплив на регуляторні рішення не лише у Великій Британії, а й у ширшому трансатлантичному просторі. Це важлива нагода не просто дізнатись більше про ризики, а й долучитися до формування стійких механізмів захисту демократії в цифрову епоху.

Інші новини

Прозорість бенефіціарного володіння: чому боротьба ще не завершена [14]

Стаття Флоренсії Лоренцо, опублікована Tax Justice Network, ґрунтовно досліджує триваючу глобальну боротьбу за прозорість бенефіціарної власності, підкреслюючи стійкі виклики та фрагментарний прогрес у цій ключовій сфері. Бенефіціарна власність стосується ідентифікації реальних фізичних осіб, які остаточно володіють, контролюють або отримують вигоду від юридичних осіб, таких як

[14] https://taxjustice.net/2025/04/07/new-article-explores-why-the-fight-for-beneficial-ownership-transparency-isnt-over/

компанії, трасти чи партнерства. Стаття акцентує на важливості цієї прозорості для боротьби з незаконними фінансовими потоками, ухиленням від податків, відмиванням грошей та іншими зловживаннями, які стають можливими через непрозорі структури володіння.

Автор розпочинає з опису нещодавніх перешкод у впровадженні реєстрації бенефіціарних власників. Гучні суперечки, такі як рішення Європейського суду щодо обмеження публічного доступу до реєстрів бенефіціарного володіння в ЄС та судові позови в Сполучених Штатах проти Закону про корпоративну прозорість, підірвали досягнуті успіхи. У США судові процеси фактично призупинили вимоги до юридичних осіб звітувати про своїх бенефіціарних власників до Мережі з протидії фінансовим злочинам (FinCEN), що погіршується через наявні прогалини в законодавстві, які вже обмежували обсяг зобов'язань щодо реєстрації. Ці події підкреслюють крихкість прогресу та невизначеність у глобальних зусиллях із забезпечення прозорості.

Лоренцо простежує історію проблеми непрозорості бенефіціарного володіння до кінця 1990-х років, коли міжнародні організації, зокрема Організація Об'єднаних Націй, Цільова група з фінансових заходів (FATF) та Рада з фінансової стабільності, почали визнавати її глобальним викликом. Витоки інформації, такі як Panama Papers, продемонстрували транскордонні наслідки секретності, показавши, як юрисдикції зі слабкими рамками прозорості створюють ефекти переливу, що ускладнюють правозастосування в усьому світі. У статті описуються історичні підходи до вирішення цієї проблеми, зокрема "підхід наявної інформації", який покладався на посередників, таких як банки та юристи, для зберігання даних про власників, та "корпоративний підхід", який вимагав від компаній знати своїх власників. Обидва підходи виявилися неефективними, що призвело до появи реєстраційного підходу, за якого юридичні особи зобов'язані повідомляти відомості про власність відповідним органам.

Спираючись на концепцію транснаціональних правових порядків, розроблену академіками Грегорі Шаффером і Терренсом Галлідеєм, стаття аналізує інституціоналізацію реєстрації бенефіціарного володіння через два виміри: нормативне врегулювання (як норми стабілізуються через визначення, правові тлумачення та практики) та відповідність норм проблемі (наскільки норми відповідають проблемі, яку вони мають вирішувати). Автори зазначають, що хоча кількість юрисдикцій, які прийняли закони про реєстрацію бенефіціарного володіння, значно зросла — з 34 у 2018 році до 97 у 2022 році, згідно з Індексом фінансової секретності, — глобальна правова система залишається фрагментованою та слабко узгодженою з цілями.

Ключові проблеми включають невідповідність визначень бенефіціарного володіння в різних юрисдикціях. Наприклад, рекомендації FATF, які пропонують поріг у 25% володіння або прав голосу як індикатор бенефіціарного володіння, були широко прийняті, але є недосконалими. На практиці цей високий поріг дозволяє багатьом компаніям, наприклад половині зареєстрованих у Люксембурзі, повідомляти про вищих менеджерів замість справжніх власників, що підриває прозорість. Відмінності в обсязі реєстрації, критеріях, доступі до даних та відповідальних органах ще більше

Висновки:

- **Необхідно уточнити визначення бенефіціарного власника:** Скасувати високі пороги володіння (наприклад, 25% за FATF) і запровадити чіткі критерії, щоб компанії повідомляли справжніх власників, а не менеджерів.
- **Розширити охоплення реєстрації:** Зобов'язати всі юридичні особи, включно з трастами та партнерствами, реєструвати бенефіціарних власників, усуваючи прогалини в законодавстві.
- **Забезпечити публічний доступ до реєстрів:** Відкрити дані про бенефіціарне володіння для громадськості, щоб посилити контроль і протидіяти обмеженням.
- **Гармонізувати глобальні стандарти:** FATF та ЄС мають узгодити вимоги до реєстрації, щоб зменшити розбіжності між юрисдикціями та підвищити ефективність.

послаблюють систему. Стаття також зазначає, що прогрес не був одностороннім; ініціативи на національному та регіональному рівнях, такі як директиви ЄС щодо боротьби з відмиванням грошей, іноді визначали глобальні стандарти, а не лише їх приймали.

Покращення інституціоналізації прозорості бенефіціарного володіння потребує усунення цих невідповідностей. Вони виступають за уточнення визначень бенефіціарних власників, розширення обсягу реєстрації для охоплення всіх відповідних юридичних осіб та забезпечення публічного доступу до даних про власність для підвищення підзвітності. Ці рекомендації відповідають "Дорожній карті ефективної прозорості бенефіціарного володіння" від Tax Justice Network.

Стаття завершується висновком, що без таких реформ транснаціональний правовий порядок, який регулює бенефіціарне володіння, продовжуватиме бути неефективним, дозволяючи секретності зберігатися та сприяючи зловживанню юридичними особами.

Інформаційний бюлетень EBA з ПВК/ФТ [15]

Цей випуск інформаційного бюлетеня Європейського банківського органу (EBA) містить актуальні оновлення щодо законодавчого та інституційного розвитку системи протидії відмиванню коштів і фінансуванню тероризму (ПВК/ФТ) в Європейському Союзі, з особливим фокусом на сектор криптоактивів, впровадження наглядових технологій (SupTech), управління податковою доброчесністю, узгодження санкційних механізмів та процес дерискінгу (відмови в обслуговуванні клієнтів). Публікація демонструє прогрес у реалізації європейського пакету ПВК/ФТ та відображає зусилля EBA щодо плавної передачі повноважень майбутньому Європейському органу з протидії відмиванню коштів (AMLA).

Головним зрушенням є повне набрання чинності нового правового режиму у сфері криптоактивів: Регламентів MiCAR (ЄС 2023/1114), TFR для криптоактивів (ЄС 2023/1113), а також змін до Директиви (ЄС) 2015/849. Повідомляється про нові зобов'язання для постачальників послуг, пов'язаних із криптоактивами (CASPs), які мають забезпечити наявність дієвих механізмів контролю, аби уникнути використання їх інфраструктури у незаконних цілях. У спільному звіті EBA та ESMA здійснено ґрунтовний аналіз ризиків у децентралізованих фінансах (DeFi) і ринках криптокредитування, стейкінгу та позик, де виявлено високі вразливості, інформаційні асиметрії, потенціал для системного ризику та використання з метою ВК/ФТ.

Питання авторизації CASPs, відповідно до MiCAR, розглянуто у брифінгу ESMA для національних органів, де наголошено на необхідності врахування ПВК/ФТ ризиків з урахуванням складності, трансграничності та масштабу діяльності заявника. У цьому контексті регуляторам рекомендовано співпрацювати з національними органами ПВК/ФТ. Одночасно EBA завершила консультації щодо розробки критеріїв для призначення центральної контактної особи CASPs у країнах-членах, відповідальної за дотримання місцевого законодавства у сфері ПВК/ФТ.

У частині застосування технологій для нагляду, EBA провела воркшоп із SupTech/AI для ПВК/ФТ-наглядачів з усіх країн ЄС. Зазначено, що 35% органів лише розробляють свої перші інструменти

[15] https://ec.europa.eu/newsroom/eba/newsletter-archives/62249

SupTech, тому наголошено на потребі у тісній міждисциплінарній співпраці (IT, ПВК/ФТ, захист даних) та координації для створення інноваційних рішень.

У лютому 2025 року EBA опублікувала результати оцінювання заходів у відповідь на схеми податкового арбітражу (Cum-Ex/Cum-Cum). Попри наявність позитивних практик, виявлено суттєві недоліки в діях наглядових органів та сформульовано низку рекомендацій щодо підвищення ефективності заходів з податкової доброчесності.

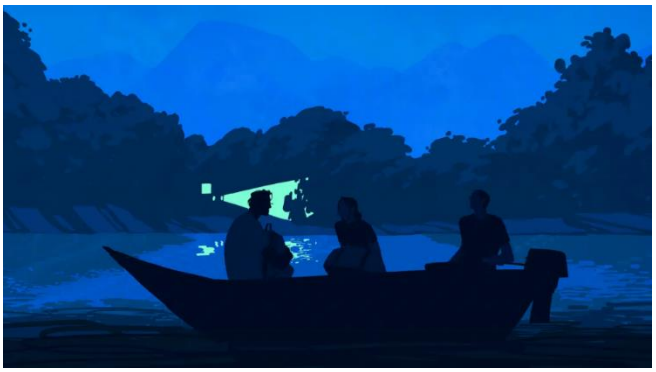
У сфері санкційної політики зазначено, що рекомендації EBA з внутрішніх політик і процедур щодо імплементації обмежувальних заходів ЄС тепер перекладені всіма офіційними мовами Союзу. Також оголошено про відкриту консультацію щодо чотирьох регуляторних технічних стандартів (RTS), які стануть основою майбутнього режиму ПВК/ФТ в ЄС: щодо санкцій, належної перевірки клієнтів (CDD), оцінювання ризиків ВК/ФТ та критеріїв для визначення установ, що підлягатимуть прямому нагляду AMLA.

EBA також звертає увагу на процес передачі повноважень новостворюваному AMLA, зокрема підготовку до передачі бази даних EuReCA, укладення угод про співпрацю з іншими європейськими наглядовими органами (ESMA, EIOPA), щоб забезпечити інтегровану та ефективну протидію фінансовим злочинам.

Нарешті, згідно зі звітом про споживчі тенденції (CTR), явище дерайзингу залишається значущою проблемою: відмова у фінансовому обслуговуванні може бути як обґрунтованою, так і дискримінаційною, тому EBA нагадує про наявні рекомендації щодо балансування ризиків та доступу до фінансових послуг як публічного блага.

Для загального розвитку

За лаштунками «романтичного шахрайства»: Як злочинні синдикати використовують технології для обману та експлуатації [16]



Стаття від MIT Technology Review, розкриває механізми «романтичних шахрайств» (pig butchering scams), які організовують злочинні синдикати в Південно-Східній Азії, переважно в М'янмі. Автори Пітер Гест та Емілі Фішбейн, спираючись на свідчення жертв, експертів із боротьби з торгівлею людьми та кіберзлочинністю, детально описують методику злочинів, структуру шахрайської індустрії та виклики, з якими стикаються правоохоронні органи в боротьбі з цими схемами.

Стаття зосереджується на історії Гавеша (псевдонім), молодого чоловіка з Південної Азії, якого обманом залучили до роботи в шахрайському комплексі KK Park у М'янмі через фальшиве оголошення про роботу на Facebook. Замість обіцяної посади в сфері обслуговування клієнтів із зарплатою $1500 на місяць, його змусили брати участь у шахрайстві, де зловмисники вибудовують довірливі, часто романтичні стосунки з жертвами онлайн, щоб виманити їхні гроші. Ця історія слугує прикладом для аналізу ширшої індустрії, яка експлуатує тисячі людей і завдає мільярдних збитків.

[16] https://www.technologyreview.com/2025/03/27/1113782/scam-compound-meta-facebook-pig-butchering-wechat/

Шахрайство типу «pig butchering» (термін, якого Interpol уникає через стигматизацію) базується на обмані, що починається з розміщення фальшивих оголошень про роботу на платформах, таких як Facebook, із привабливими умовами: високі зарплати, безкоштовне проживання, візи. Гавеш пройшов співбесіду через Telegram, демонструючи навички англійської, щоб виглядати професійно. Після прибуття до Таїланду його перевезли через кордон до М'янми вночі, використовуючи човен через річку Моей.

У таборі KK Park, укріпленому стінами, колючим дротом і озброєною охороною, йому видали iPhone 8, SIM-карти та програми для підробки геолокації, щоб створювати фальшиві профілі на Facebook, Instagram, WhatsApp, Telegram і дейтинг-додатках, таких як Tinder. Гавеш копіював фото привабливих людей, імітуючи заможне життя, додаючи деталі з Google, щоб видавати себе за жителя, наприклад, Маямі-Біч. Його завдання полягало в пошуку цілей, часто заможних чоловіків середнього віку із Заходу, через масові повідомлення чи прямі підходи, такі як «помилковий номер» у WhatsApp.

Після контакту він будував емоційний, часто романтичний зв'язок, уникаючи відеодзвінків або використовуючи записані відео. Останнім часом синдикати застосовують штучний інтелект для підробки голосу чи обличчя, роблячи обман переконливішим. На фінальному етапі жертв переконували інвестувати в фальшиві криптовалютні платформи через легальні біржі, як Binance, показуючи фальшиві графіки прибутку та повертаючи дрібні суми для довіри, після чого виманювали великі кошти. Гроші переміщали через Tether (USDT), використовуючи «міксери» для відмивання, а потім конвертували у фіатну валюту. Дослідники оцінюють, що з 2020 року синдикати вкрали близько $75 мільярдів.

Шахрайська індустрія функціонує як ієрархічна організація, подібна до аутсорсингової компанії, але з активним використанням насильства і експлуатації. За оцінками ООН, у 2023 році в М'янмі утримували 120 000 людей для примусової роботи в шахрайстві. На чолі стоять не ідентифіковані китайські «боси». Під ними — менеджери з «чорними» чи «сірими» тегами, що керують операціями, і «червоні теги» — лідери команд, які стежать за квотами. «Жовті теги» виконують функції HR чи перекладачів, контролюючи «синіх» — нанижчий рівень, як Гавеш, що створюють профілі та спілкуються з жертвами. Ці працівники працюють 12+ годин без вихідних, зазнаючи покарань за невиконання завдань: від побиттів до ізоляції у «водяній в'язниці», де жертв б'ють до втрати свідомості.

Успішні шахраї отримують привілеї, такі як доступ до ресторанів, невдахи продаються іншим «роботодавцям» або платять викуп за звільнення. Табори побудовані з 2019 року, оснащені iPhone, Starlink і системами безпеки, включаючи металошукачі. Розташовані в прикордонних зонах М'янми, де корупція та збройні групи, пов'язані з військовим урядом, забезпечують безкарність.

З правоохоронної точки зору, боротьба з синдикатами ускладнена транснаціональним характером, технологіями та геополітикою. Жертви шахраїв рідко отримують правосуддя через юрисдикційні бар'єри: синдикати діють у кількох країнах, залучаючи людей із 60+ країн, а гроші ховаються в криптовалютних гаманцях у юрисдикціях із слабким контролем. WhatsApp і Telegram шифрують повідомлення, ускладнюючи моніторинг, а фальшиві профілі обходять верифікацію через маніпуляції. Tether забезпечує анонімність транзакцій, і хоча відстеження можливе, воно вимагає ресурсів, яких бракує багатьом правоохоронним агенціям. Технологічні компанії, як Meta чи Tinder, видаляють акаунти, але нові з'являються швидше; Tether рідко заморожує гаманці, щоб зберегти привабливість валюти.

Табори в М'янмі діють у «сірій зоні», де місцева влада отримує прибуток від злочинів. Таїланд відключає інтернет до таборів, але синдикати використовують Starlink. Китай співпрацює з М'янмою проти шахрайств із їхніми громадянами, але західні країни уникають контактів із військовим урядом М'янми. У США законодавство зосереджене на банках, а не на платформах, а політика дерегуляції, підкріплена адміністрацією Трампа, послаблює тиск на компанії. Скасування санкцій проти криптоміксера Tornado Cash і припинення фінансування програм боротьби з торгівлею людьми у 2025 році ускладнюють зусилля.

Розпізнавання шахрайства в інтернеті: Як виявити продукти, створені за допомогою штучного інтелекту [17]

Документ, опублікований Bellingcat у співпраці з Evident, є вичерпним посібником, спрямованим на захист споживачів від шахрайств в електронній комерції, де використовуються зображення, створені штучним інтелектом (ШІ). Цей посібник детально розкриває, як сучасні технології ШІ дозволяють створювати переконливі, але фіктивні зображення товарів, що вводять покупців в оману, і пропонує практичні методи для їх розпізнавання за допомогою критичного мислення та доступних інструментів, таких як зворотний пошук зображень.

На початку документ вводить читача в контекст проблеми через приклад шахрайства з так званими «кришталевими кавовими чашками», які рекламувалися як унікальні вироби з натуральних мінералів, таких як аметист чи рожевий кварц, і продавалися за привабливими цінами на платформах, включаючи Amazon та Facebook. Зображення цих чашок виглядали магічно привабливими, але покупці, які їх замовляли, отримували дешеві продукти, що не мали нічого спільного з рекламою. Цей приклад слугує відправною точкою для пояснення, як ШІ використовується для створення ілюзії якісних товарів, що ускладнює їх відрізнення від справжніх.

Далі документ заглиблюється в аналіз візуальних і практичних ознак, які можуть вказувати на ШІ-генерацію зображень. Наприклад, у зображеннях чашок помітні дефекти, такі як розриви ліній, розмиті плями чи навіть зникнення частин об'єкта, що є типовими помилками ШІ. Окремо розглядається питання функціональності продуктів: деякі зображення показують нереалістичні предмети, як-от чашку з «лавового каменю» з червоним світлом, але без згадки про джерело живлення, що викликає сумніви щодо їхньої автентичності. Крім того, справжні товари зазвичай демонструються з кількох ракурсів, тоді як ШІ-генеровані зображення часто обмежуються одним фото або містять невідповідності в деталях, якщо їх кілька.

Документ також звертає увагу на важливість ретельного аналізу описів продуктів. Шахраї можуть використовувати хитрощі, приховуючи правду в тексті, наприклад, називаючи продукт «кришталеподібним» замість справжнього кришталю. У прикладі з орнаментами на eBay зображення здавалися тривимірними, але в назві зазначалося, що вони плоскі, що могло залишитися непоміченим через імпульсивну покупку. Ще один приклад — в'язаний шаблон корови Highland на Etsy, де різні зображення показували невідповідні дизайни, а текстура пряжі не відповідала матеріалам для в'язання, що було підтверджено продавцем як ШІ-генерація після скарг клієнтів.

Для перевірки продуктів посібник рекомендує кілька методів. Зворотний пошук зображень допомагає виявити, чи використовувалося зображення в інших шахрайських оголошеннях або

[17] https://www.bellingcat.com/resources/2025/03/25/detecting-ai-products/

чи походить воно з сайтів із ШІ-контентом. Перегляд відгуків покупців, особливо тих, що містять фотографії, дозволяє порівняти реальний продукт із рекламою. Порівняння цін також є ключовим: наприклад, лампа у формі кота за $23 виглядала підозріло дешевою порівняно з аналогами за $100+, що вказувало на потенційне шахрайство.

Окремий акцент зроблено на перевірці продавців. Документ радить досліджувати їхню репутацію, перевіряти наявність веб-сайтів чи соціальних мереж, а також аналізувати профільні фото, які можуть бути ШІ-генерованими. У прикладі з книгою «Renal Diet Cookbook for Beginners» автор «Ethan Neulife» не мав жодної цифрової присутності в інтернеті, а його фото виявилося схожим на ШІ-генероване зображення зі стокового сайту FreePik. Це підкреслює важливість перевірки не лише продуктів, а й тих, хто стоїть за ними.

Ширший контекст документа охоплює не лише фізичні товари, але й інші сфери, як-от ШІ-генеровані книги, які з'являються навіть у бібліотеках без належного маркування. Це вказує на системну проблему в електронній комерції, де навіть платформи з репутацією не завжди ефективно борються з шахрайством. Посібник завершується закликом до пильності, наголошуючи, що уникнення імпульсивних покупок і ретельна перевірка можуть захистити від обману.

Висновки:

- **Ретельно аналізуйте зображення продуктів:** Перед покупкою уважно розглядайте зображення на наявність невідповідностей (розмитість, нереалістичні деталі, відсутність кількох ракурсів). Використовуйте зворотний пошук зображень, щоб перевірити, чи не є вони ШІ-генерованими або використаними в інших шахрайських оголошеннях.
- **Читайте описи та відгуки з фото:** Завжди перевіряйте описи продуктів на приховані застереження (наприклад, «кришталеподібний» замість «кришталевий»). Шукайте відгуки покупців із фотографіями, які показують реальний продукт, і порівнюйте їх із зображеннями в оголошенні.
- **Перевіряйте продавців і авторів:** Досліджуйте репутацію продавця, перевіряйте їхню присутність у мережі та аналізуйте профільні фото на предмет ШІ-генерації. Для книг перевіряйте існування автора та видавця, уникаючи самвидаву без додаткових перевірок.
- **Будьте обережні з надто привабливими цінами:** Порівнюйте ціни з аналогічними продуктами на ринку. Якщо ціна значно нижча (наприклад, $23 за лампу проти $100+ за простіші моделі), це може вказувати на шахрайство, особливо якщо зображення виглядає нереалістично.

Ваша думка важлива!

1. Чи здатні сьогоднішні механізми виявлення ПВК/ФТ ефективно розпізнати складні схеми із використанням криптоактивів, які пов'язані з децентралізованими групами типу ISIS-K? Яких нових індикаторів потребує аналітична практика?
2. Як має змінитися взаємодія між СПФМ, регуляторами та ПФР в умовах мультисекторальних схем ВК, де одночасно використовується TBML, криптовалюта та підставні особи?
3. Які наслідки для глобальної системи ПВК/ФТ може мати демонтаж американських антикорупційних та AML-законів? Чи здатна Європа чи інші регіони сформувати альтернативну лідерську позицію?
4. У контексті санкцій проти тіньового флоту: як регуляторам і СПФМ виявляти фіктивні елементи у документах щодо морського страхування або лізингу? Чи має сенс створити реєстр перевірених страховиків для використання у ПВК-аналізі?
5. Чи варто Україні запровадити жорстке регулювання технологічних платформ, таких як Meta чи Telegram, для протидії шахрайським схемам, і які ризики це може нести для свободи слова?
6. Яку роль можуть відіграти українські онлайн-платформи та маркетплейси у протидії шахрайству з ШІ-генерованими продуктами, і чи готові вони впроваджувати суворіші перевірки продавців?
7. Як Україна може співпрацювати з країнами Балтійського регіону, такими як Данія, для посилення моніторингу тіньової флотилії Росії та запобігання обходу санкцій?

Контактуйте щодо цього документу з Міністерством фінансів України:

- **Email:** aml_bulletin@minfin.gov.ua
- **Поштова адреса:** Міністерство фінансів України, Україна, 04071, м. Київ, вул. Межигірська, 11
- **Ідентифікація контакту:** стосовно Методологічного Бюлетеня № МінФін-AML-2025-16

Бюлетень є волонтерською розробкою методологічної команди Міністерства фінансів України відповідно до частини 8 статті 18 Закону України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення».

Щоб отримати доступ до інших Методологічних Бюлетенів – перейдіть за посиланням [офіційний веб-сайт Міністерства фінансів].