Методологічний бюлетень

Серійний номер: МінФін-AML-2025-38

Вересень 2025

“Любіть те, що робите — тоді робитимете це якнайкраще”

Кетрін Джонсон

Мета

Методологічний Бюлетень видається Міністерством Фінансів України на регулярній основі 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.

Містить 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

Секторальний підхід до бенефіціарної власності у сфері закупівель та нерухомості [1]

Цей робочий документ МВФ детально розглядає важливість ідентифікації фізичної особи, яка є кінцевим власником або контролером активу (кінцевим бенефіціарним власником, КБВ), як ключового заходу прозорості, необхідного для запобігання використанню активів у злочинних чи неетичних цілях, включаючи протидію ВК/ФТ та корупції. У ньому зазначається, що хоча багато країн створюють централізовані реєстри КБВ, часто пов'язані з комерційними реєстрами для дотримання стандартів ПВК/ФТ, ці централізовані системи можуть бути недостатніми для задоволення специфічних потреб секторального нагляду, оскільки органи, як-от закупівельні відомства або земельні реєстри, можуть вимагати більш

[1] https://www.imf.org/en/Publications/WP/Issues/2025/09/12/Targeted-Transparency-Sectoral-Approach-to-Beneficial-Ownership-in-Procurement-and-Real-570051

деталізованих або спеціалізованих даних про КБВ, наприклад, інформації про іноземних суб'єктів або застосування нижчих порогових значень для політично значущих осіб (PEP).

Секторальний підхід до прозорості КБВ є цільовою та гнучкою рамковою основою, яка має на меті усунути ці прогалини шляхом узгодження збору, доступу та використання даних КБВ відповідно до унікальних ризиків та операційних реалій кожного сектору, при цьому доповнюючи національні рамкові основи КБВ. Важливо зазначити, що, на відміну від централізованих реєстрів ПВК/ФТ, кінцевою метою секторального підходу не є забезпечення повної відповідності міжнародним стандартам, таким як стандарти FATF, а зосередження на пом'якшенні конкретних ризиків, пов'язаних із корупцією, шахрайством, податковими злочинами або національною безпекою у межах конкретного сектору. Документ ґрунтується на досвіді, отриманому під час пандемії COVID-19, коли зобов'язання щодо прозорості КБВ у сфері державних закупівель, пов'язаних з надзвичайним фінансуванням МВФ, були реалізовані на рівні 90% (повністю або суттєво), попри те, що багато країн, які впроваджували ці заходи, мали низькі рейтинги ефективності FATF щодо прозорості КБВ. Це підтвердило, що цільові секторальні заходи можуть бути швидко впроваджені навіть за обмежених ресурсів.

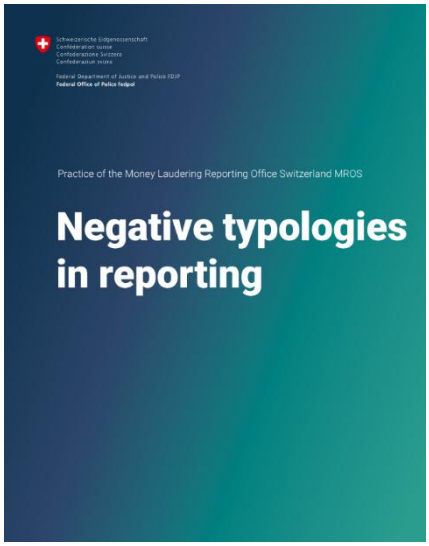
У сфері державних закупівель непрозорість КБВ дозволяє корумпованим суб'єктам маніпулювати процесами та приховувати конфлікти інтересів, тоді як розкриття інформації про КБВ сприяє підзвітності та виявленню схем змови. У секторі нерухомості, який є високоризиковим і часто використовується для відмивання коштів через низький рівень ефективного впровадження превентивних заходів ПВК/ФТ серед визначених нефінансових установ та професій (ВНУП), прозорість КБВ може суттєво доповнити існуючі рамки зниження ризиків. Мінімальний секторальний захід для нерухомості може включати збір інформації про КБВ покупця (якщо це юридична особа/правове утворення) земельним або нерухомим органом під час передачі майна.

Висновки:

- **Впроваджувати цільові заходи незалежно від національного реєстру:** Країнам слід негайно впроваджувати секторальні вимоги до прозорості КБВ у високоризикових сферах (закупівлі, нерухомість) на основі оцінки ризиків, оскільки це є ефективним і швидким способом пом'якшення корупційних ризиків, навіть якщо централізований реєстр КБВ ще не функціонує або має низьку ефективність.
- **Максимізувати верифікацію через посередників та публічність:** Для забезпечення точності даних про КБВ необхідно використовувати механізми верифікації, що включають публічний доступ до інформації для виявлення розбіжностей та/або покладення обов'язку збору і верифікації інформації на регульованих посередників (наприклад, нотаріусів чи рієлторів) під час транзакцій, особливо у сфері нерухомості.
- **Застосовувати санкції безпосередньо до КБВ та запобігати обходу:** Необхідно розробити законодавчі механізми, які запобігають використанню лазівок, таких як поділ великих контрактів для уникнення порогових значень розкриття КБВ, і які забезпечують застосування ефективних, пропорційних санкцій, включаючи відсторонення від тендерів, що стосуються безпосередньо КБВ, а не лише юридичної особи.
- **Забезпечити обізнаність та синергію:** Оскільки секторальні органи часто недостатньо обізнані з концепцією КБВ, необхідно проводити достатнє навчання для всіх зацікавлених сторін, включаючи посадових осіб, приватний сектор, ЗМІ та громадські організації, а також забезпечити координацію між секторальними органами та органами ПВК/ФТ для обміну інформацією та виявлення загроз.

Ефективна реалізація секторального підходу вимагає ретельного проектування, включаючи пристосування вимог до ризиків (наприклад, застосування нижчих порогів або розширення сфери охоплення PEP), а також забезпечення верифікації інформації. Оскільки секторальні органи часто не мають ресурсів для повної верифікації, ключовим механізмом є краудсорсинг (публічний доступ для виявлення невідповідностей громадськістю та журналістами) або покладання обов'язку верифікації на регульованих посередників (нотаріусів, юристів) під час транзакцій з нерухомістю. Крім того, при впровадженні секторальних заходів необхідно балансувати прозорість із законними занепокоєннями щодо конфіденційності, використовуючи багаторівневі механізми доступу, обмежуючи публікацію чутливих даних (наприклад, повну дату народження) та надаючи можливість вимагати винятків у випадках серйозного ризику насильства. Для забезпечення дотримання правил необхідне застосування переконливих і пропорційних санкцій, включаючи штрафи та відсторонення від участі у закупівлях, які повинні поширюватися як на компанії, так і на самих бенефіціарних власників, щоб уникнути обходу правил шляхом створення нових компаній.

Негативні типології у звітності [2]



Основна мета документу, виданого Офісом звітування про відмивання коштів Швейцарії (MROS) - підвищити якість вхідних повідомлень про підозрілу діяльність (SAR) та сприяти їх ефективній обробці, висвітлюючи поширені помилки та неадекватні практики, виявлені MROS. Швейцарська система ПВК/ФТ базується на принципі якісного звітування, і Парламент відмовився від звітування, заснованого на кількісних порогах. Фінансові посередники (ФП) покладаються на систему каскадних обов'язків належної перевірки: від верифікації клієнта та бенефіціарного власника (статті 3–5 Закону про боротьбу з відмиванням коштів, AMLA) до спеціальних обов’язків з належної перевірки (стаття 6 AMLA), які вимагають ретельного дослідження будь-яких підозр. Подання SAR до MROS відповідно до статті 9 AMLA є результатом кваліфікованої оцінки, а не просто припущенням, заснованим на ризику. Проте, MROS виявив чітку тенденцію до так званого захисного звітування, коли ФП подають SAR не через обґрунтовану підозру у відмиванні коштів, а для мінімізації власних кримінальних чи регуляторних ризиків. Така практика призводить до навмисного заниження порогу звітування, встановленого законом, і заповнення звітів малоцінною або нерелевантною інформацією, яка не додає вартості кримінальному розслідуванню. MROS може ефективно опрацьовувати лише ті SAR, які ґрунтуються на адекватній початковій підозрі та містять обґрунтоване, добре структуроване та задокументоване викладення фактів.

Наведені негативні типології базуються на практичному досвіді MROS і демонструють випадки, коли факти були недостатньо з'ясовані або коли відсутні адекватні ознаки відмивання коштів, предикатних злочинів, організованої злочинності чи фінансування тероризму згідно зі статтею 9 AMLA. Зокрема, документ виділяє вісім основних категорій:

1. Невдала спроба відкриття рахунку (Типологія 1): Звітування про спроби відкриття онлайн-рахунків, які були перервані до встановлення ділових відносин або руху коштів. Такі випадки часто не містять повної ідентифікації клієнта чи ознак предикатного злочину. Технічні перебої

[2] https://www.fedpol.admin.ch/dam/fedpol/en/data/kriminalitaet/geldwaescherei/mros-negativtypologien-2025.pdf.download.pdf/mros-negativtypologien-2025-e.pdf

або зміна рішення клієнтом самі по собі не є об'єктивними підставами для обґрунтованої підозри.

2. Підозрілі клієнти без явного зв'язку зі злочинними активами (Типологія 2): Звітування на основі нечітких невідповідностей або суб'єктивних факторів ризику, як-от "неправдоподібна бізнес-модель" чи надмірно складні юридичні структури, без надання відчутних доказів злочинного походження активів. Обґрунтована підозра вимагає об’єктивно підтверджуваних доказів того, що активи отримані внаслідок злочинної діяльності.

3. Інформація від третіх сторін (Типологія 3): Сюди належить звітування, засноване виключно на наказах про розкриття інформації/арешт, загальних посиланнях на участь TWINT-рахунку в поліцейському розслідуванні або повідомленнях ЗМІ. ФП повинен встановити зв'язок між цією зовнішньою інформацією та власними діловими відносинами шляхом проведення належних розслідувань (стаття 6 AMLA), а не просто пересилати отриману інформацію.

4. Використання криптовалютних бірж (Типологія 4): Звіти, засновані виключно на обміні фіатних грошей на криптовалюти або використанні криптоплатформ. Використання криптовалют є фактором ризику, але не є підозрілим само по собі і не відповідає правовому порогу обґрунтованої підозри.

Висновки:

- **Посилення внутрішнього розслідування (Ст. 6 AMLA):** Фінансові посередники зобов'язані припинити "захисне звітування" та забезпечити, щоб кожний SAR був результатом вичерпного внутрішнього розслідування (спеціальної належної перевірки згідно зі статтею 6 AMLA). Звіт має містити обґрунтовану підозру, засновану на фактичних доказах, а не на загальних припущеннях чи суб'єктивних факторах ризику.
- **Фокус на злочинному походженні активів:** Критерій для подання SAR (стаття 9 AMLA) вимагає об'єктивно верифікованих доказів того, що активи були отримані внаслідок предикатної злочинної діяльності. Необхідно відкидати звітування щодо випадків, де кошти мають законне походження, навіть якщо вони є частиною шахрайських схем, жертвою яких став клієнт чи сам ФП ("рахунки жертв" та Типологія 6).
- **Критичне опрацювання зовнішньої інформації:** Заборонити автоматичне пересилання до MROS інформації, отриманої від третіх сторін (медіа-повідомлення, накази про розкриття), без належного розслідування та встановлення прямого зв'язку з власними діловими відносинами та підозрою у відмиванні коштів.

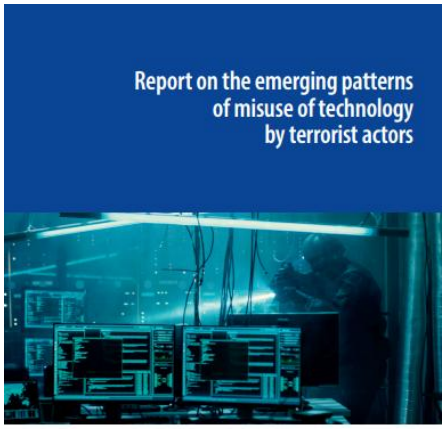
5. "Рахунки жертв" (Типологія 5): Випадки, коли клієнти з законно набутими коштами стають жертвами шахрайства (наприклад, романтичного чи інвестиційного) або втрачають платіжні інструменти (викрадення карток). Оскільки обов'язок звітування за статтею 9 AMLA спрямований на запобігання відмиванню злочинно отриманих активів, а не на інформування про втрату законних коштів чи карток, ці ситуації, як правило, не вимагають подання SAR, якщо відсутні додаткові ознаки відмивання.

6. ФП стає жертвою шахрайства (Типологія 6): Коли сам ФП стає жертвою кібератаки чи шахрайства і переказує власні законні кошти злочинцям. Оскільки активи походять з легітимних джерел самої установи, зобов'язання звітувати про предикатний злочин відмивання коштів не виникає.

7. "Чорна каса" (Slush funds, Типологія 7): Підозри, що законні кошти, отримані в ході звичайної ділової діяльності, можуть бути використані для майбутніх хабарів. Припущення про можливе майбутнє неправомірне використання не є достатнім. Зобов’язання подавати SAR виникає лише тоді, коли відбувся сам акт підкупу і були набуті активи злочинного походження.

8. Біржовий злочин без акцій, лістингованих у Швейцарії (Типологія 8): Повідомлення про інсайдерську торгівлю або маніпулювання ринком. Ці дії є предикатними злочинами лише за умови, що фінансова вигода перевищує один мільйон швейцарських франків та вони стосуються цінних паперів, допущених до торгів на торговому майданчику, зареєстрованому у Швейцарії.

Нові технології у руках терористів: виклики для Європи та світу [3]



Рада Європи у своєму звіті проаналізувала, як новітні технології трансформують характер і масштаби терористичних загроз. Якщо у 2000-х роках головними інструментами терористів залишалися традиційні методи — вибухівка, стрілецька зброя, атаки на інфраструктуру, — то вже у 2020-х технологічний вимір став невід'ємним компонентом. Тепер мова йде не лише про тактичні інновації, а й про системні зміни: від фінансування до пропаганди, від комунікації до застосування штучного інтелекту. Звіт показує, що терористи активно «освоюють» цивільні технології, пристосовуючи їх до власних цілей, і це створює асиметричний виклик для держав, які змушені реагувати значно швидше, ніж це відбувалося у минулому.

Документ наголошує, що процес використання нових технологій терористичними групами залежить від кількох факторів. Внутрішні — це стратегія самої організації, рівень централізації та компетенції її учасників. Наприклад, групи з ієрархічною структурою легше інтегрують складні технологічні рішення, тоді як мережеві чи осередкові структури більше схильні використовувати простіші та доступніші інструменти. Зовнішні фактори включають доступ до фінансування, якість контртерористичної діяльності з боку держав і навіть міжнародний контекст. Таким чином, нові технології для терористів — не самоціль, а інструмент, який вони адаптують залежно від можливостей та середовища.

Одним із найбільш показових прикладів є використання безпілотників. У Сирії та Іраку Ісламська держава вже демонструвала можливості застосування дронів як розвідувальних, так і ударних платформ, створюючи імпровізовані системи доставки вибухівки. У Європі такі випадки поки поодинокі, але потенціал є очевидним: масове поширення цивільних дронів і розвиток комерційних технологій відкривають шлях до нової генерації атак. Проблема ускладнюється тим, що держави відстають у виробленні регуляцій і систем протидії — технології антидронового захисту дорогі, а правила використання часто носять декларативний характер.

Другий ключовий напрям — фінансування через криптовалюти. Екстремістські угруповання експериментують із біткойном та іншими віртуальними активами для збору коштів, особливо у міжнародних кампаніях. Проте у звіті зазначається, що цей інструмент досі не став масовим: волатильність курсів, а також посилення систем моніторингу роблять його не надто зручним. Водночас відзначається зростання ролі криптовалют поза межами Європи — у країнах Близького Сходу чи Африки, де банківська система слабша, а контроль з боку держави мінімальний. Там цифрові активи можуть стати основним каналом фінансування терористичних структур.

Не менш важливим є питання комунікацій і радикалізації. Соціальні мережі залишаються одним із головних каналів для поширення екстремістської ідеології. Великі платформи, такі як Facebook

[3] https://rm.coe.int/report-on-the-emerging-patterns-of-misuse-of-technology-by-terrorist-a/4880281a94

чи YouTube, посилили модерацію й видалення контенту, але терористи швидко знаходять альтернативні простори: менші соцмережі, закриті чати у Telegram, форуми у даркнеті, а навіть онлайн-ігри. Там вони вербують нових прихильників, поширюють пропаганду, а подекуди й інструкції з виготовлення вибухових пристроїв чи 3D-друкованої зброї. У звіті зазначається, що цифрова радикалізація може відбуватися приховано і поступово, що ускладнює роботу спецслужб і підвищує ризики появи так званих «самотніх вовків».

Ще одним новим виміром загроз є розвиток технологій штучного інтелекту. Генеративний AI дозволяє створювати багатомовні пропагандистські матеріали у величезних масштабах, генерувати фейкові новини чи маніпулятивний контент, який важко відрізнити від легітимних повідомлень. Більш того, використання чат-ботів і автоматизованих систем дає можливість вести персоналізовану комунікацію з потенційними рекрутами, фактично аутсорсячи процес радикалізації. Це новий рівень виклику, адже масштаби впливу та швидкість поширення такого контенту значно перевищують можливості традиційних контрзаходів.

Звіт Ради Європи робить акцент на тому, що держави часто реагують на нові загрози із запізненням. Між появою нової технології у цивільному використанні та її адаптацією терористами проходить від кількох місяців до кількох років, але відповіді держав відстають ще більше. У результаті виникає «часовий розрив», яким активно користуються екстремісти. Щоб його скоротити, рекомендується розвивати системи горизонт-сканування — механізми регулярного аналізу технологічних трендів і прогнозування можливих ризиків.

Особливий акцент робиться на міжнародній співпраці. Терористичні загрози не визнають кордонів, і тому лише національних зусиль недостатньо. Потрібен швидший обмін інформацією між країнами, координація правоохоронних структур, а також залучення приватного сектору — адже саме технологічні компанії володіють ключовими інструментами моніторингу та протидії. Проте все це має поєднуватися з дотриманням прав людини: баланс між безпекою та свободою слова є критичним, щоб уникнути зловживань.

Таким чином, звіт Ради Європи демонструє, що майбутнє тероризму дедалі більше залежатиме від технологій. Дрони, криптовалюти, соціальні мережі, 3D-друк і штучний інтелект уже сьогодні формують середовище, у якому діють терористи. Якщо держави не навчаться випереджати, а не наздоганяти ці тенденції, вони ризикують зіткнутися з новою хвилею загроз, які будуть складнішими, невидимими й потенційно більш руйнівними, ніж ті, що ми знали раніше.

Висновки:

- **Терористи швидко адаптують нові технології**, тому державам потрібно впроваджувати системи прогнозування ризиків і оперативного оновлення законодавства.
- **Соціальні мережі та онлайн-платформи стали ключовими каналами радикалізації**, що вимагає тісної співпраці держав із технологічними компаніями для раннього виявлення загроз.
- **Криптовалюти дедалі активніше використовуються для фінансування терористів**, і це потребує посиленого міжнародного контролю та прозорості фінансових операцій.
- **Штучний інтелект відкриває нові можливості для пропаганди та радикалізації**, тож необхідно розвивати інструменти «захисного ШІ» та етичні стандарти для AI-розробників.

Стейблкоїни та фінансовий моніторинг: як Wolfsberg Group окреслює рамки для глобальних інституцій [4]

Документ, підготовлений Wolfsberg Group, присвячений одній з найгарячіших тем сучасних фінансів: ролі стейблкоїнів у глобальній економіці та тих ризиках, які вони несуть для системи AML/CFT.

З одного боку, стейблкоїни — це інструменти, створені для стабільності та прозорості, які мають на меті забезпечити прості та дешеві транскордонні платежі, пришвидшити обіг коштів і розширити доступ до фінансових послуг. З іншого боку, їхня швидка інтеграція у фінансову систему відкриває нові вразливості: підвищений рівень анонімності користувачів, можливість обходити традиційні банківські канали, ризик втрати контролю через відсутність уніфікованого міжнародного регулювання та потенціал для використання злочинними чи терористичними мережами.

Wolfsberg Group у цьому документі намагається не просто зафіксувати ризики, а й створити дорожню карту для фінансових установ, які опиняються перед фактом: стейблкоїни вже є частиною фінансової реальності, і їх не можна ігнорувати. Головний акцент робиться на тому, що ефективний моніторинг повинен враховувати три базові фактори. По-перше, хто виступає емітентом стейблкоїна: централізована компанія з офісами, персоналом і ліцензіями, чи децентралізована організація без чіткої юридичної структури. По-друге, який саме механізм забезпечення використовується: класичні резерви у банках і державних цінних паперах або алгоритмічні рішення, які спираються на взаємодію кількох токенів і математичні формули. По-третє, які канали розповсюдження застосовуються: централізовані біржі та кастодіальні сервіси чи децентралізовані фінансові протоколи, де фактично відсутній контроль над тим, хто і як взаємодіє з активами. Кожен із цих елементів визначає рівень ризику і ступінь відповідальності фінансових установ.

Особливу увагу документ приділяє питанню прозорості резервів, оскільки довіра до стейблкоїнів напряму залежить від того, чи реально вони забезпечені активами, які декларує емітент. Якщо компанія заявляє, що токен забезпечений доларовими депозитами, банки та регулятори повинні вимагати незалежних аудиторських підтверджень, регулярних звітів і механізмів перевірки. Алгоритмічні стейблкоїни визнаються Wolfsberg Group як високоризикові інструменти, адже мають історію крахів і нестабільності (прикладом є колапс TerraUSD у 2022 році). Саме тому фінансовим установам радять застосовувати до них найжорсткіші процедури due diligence, аж до обмеження співпраці, якщо ризики переважають потенційні вигоди.

Не менш значимою є роль посередників: криптобірж, гаманців, платіжних провайдерів. Вони фактично стають точкою входу користувачів у систему стейблкоїнів, і саме на цьому рівні вирішується, чи буде застосована процедура ідентифікації клієнтів. Проблема полягає в тому, що децентралізовані сервіси часто не проводять жодного KYC, створюючи «сліпі зони» для злочинних угруповань. Wolfsberg Group пропонує фінансовим інституціям не обмежуватися формальною перевіркою клієнтів, а активно застосовувати технології моніторингу блокчейн-транзакцій, інвестувати у спеціалізовані інструменти для аналізу on-chain даних, співпрацювати з криптокомпаніями та правоохоронними органами для спільного відслідковування підозрілих схем. Важливою є також побудова глобальних каналів обміну інформацією між банками, адже

[4] https://db.wolfsberg-group.org/assets/b7d371b0-eec0-4383-ae0c-05510aabd47c/Wolfsberg_StablecoinGuidance%20(1).pdf

стейблкоїн-транзакції часто носять транснаціональний характер і не можуть бути ефективно контрольовані в межах однієї юрисдикції.

Автори документа наголошують на серйозному виклику — регуляторній фрагментації. У різних країнах стейблкоїни трактуються по-різному: від електронних грошей, що підлягають жорстким правилам моніторингу, до активів, які майже не регулюються. Така асиметрія створює умови для «регуляторного арбітражу»: емітенти обирають юрисдикції з найменшими вимогами, а користувачі користуються цим для обходу більш суворих правил. Wolfsberg Group прямо закликає до гармонізації міжнародних підходів і створення єдиних стандартів, без яких боротьба з відмиванням коштів і фінансуванням тероризму у сфері цифрових активів приречена на лише частковий успіх.

Висновки:

- **Стейблкоїни створюють нові ризики** відмивання коштів і фінансування тероризму, тому фінансові установи повинні адаптувати свої процедури KYC/AML і моніторингу, враховуючи специфіку емісії, резервів і каналів обігу.
- **Прозорість і незалежний аудит резервів** стейблкоїнів є критичними для довіри, тому банки мають вимагати регулярних підтверджень від емітентів та контролювати їхнє виконання.
- **Найбільший фінансовий злочинний ризик становлять клієнтські розрахункові рахунки** емітентів, тому фінансові установи мають встановлювати чіткі обмеження за типами клієнтів, географією і транзакційними потоками.
- **Моніторинг on-chain активності** повинен здійснюватися у пропорційний спосіб, з акцентом на високоризикових емітентах і юрисдикціях, із використанням аналітики блокчейну та регулярних перевірок узгодженості ризик-апетиту емітента з банком.

Ключовий меседж документа полягає у необхідності для фінансових установ діяти проактивно. Ідеться про інтеграцію аналізу стейблкоїнів у внутрішні системи управління ризиками, навчання персоналу щодо нових схем, посилення комунікації з регуляторами, а також впровадження технологій моніторингу, які здатні працювати у режимі реального часу. Ігнорування теми, як підкреслює Wolfsberg Group, призведе до появи «тіньової фінансової системи», де AML/CFT-вимоги фактично не діятимуть. Для глобальних банків і фінансових посередників це не лише репутаційний ризик, а й загроза санкцій, штрафів і втрати доступу до міжнародних ринків.

Таким чином, документ стає дороговказом для світових фінансових гравців: стейблкоїни слід розглядати як невід'ємну частину сучасної фінансової реальності, аналізувати їхню структуру та ризики залежно від моделі забезпечення та каналів обігу, впроваджувати механізми прозорості й контролю, і водночас працювати над міжнародною координацією. Wolfsberg Group наполягає: лише спільні стандарти, розроблені за участю держав, приватних банків і криптоіндустрії, дозволять зберегти баланс між інноваціями та безпекою, не допустивши використання стейблкоїнів як «сліпої зони» злочинцями та терористами.

Звіти окремих інституцій та експертів

Децентралізовані фінанси [5]

Децентралізовані фінанси (DeFi) є фінансовою екосистемою, що швидко розвивається, побудованою на криптовалютах і технології блокчейн, яка усуває централізованих посередників, таких як банки, замінюючи їх одноранговими (peer-to-peer) системами, що забезпечують автономію та безмежний доступ до фінансових послуг. Ідеологія DeFi виникла з маніфесту Bitcoin 2008 року, який закликав викорінити банки та уряди з грошової гри. Як зазначено у джерелах, DeFi працює на незмінних цифрових реєстрах (блокчейнах) і виконується за допомогою «смартконтрактів» — коду, який автоматично виконує транзакції, коли виконані заздалегідь визначені умови, керуючи всім: від позик до фармінгу прибутковості. Користувачі застосовують DeFi, щоб позичати, торгувати, заощаджувати або купувати деривативи, подібно до традиційних фінансів.

Основна проблема, висвітлена у документі, полягає в тому, що тоді як DeFi стрімко розвивається, регулювання відстає. Досі відсутня єдина правова база, що визначає, як DeFi має функціонувати, що створює «сіру регуляторну зону». Це дозволяє DeFi-сервісам діяти поза межами, наприклад, регламенту ЄС щодо боротьби з відмиванням коштів (AML). Конфіденційність, швидкість та автономія, які є основними перевагами DeFi, водночас є його «ахіллесовою п’ятою». Джерела вказують, що ця екосистема стала місцем для хакерів, шахраїв та осіб, які відмивають гроші. Лише у 2024 році через порушення безпеки було викрадено близько 1,5 мільярда доларів, і ці кошти зникають без можливості повернення, оскільки немає механізмів на кшталт FDIC (Федеральної корпорації зі страхування вкладів).

Злочинці активно експлуатують відкритий характер DeFi, використовуючи його як інструмент для відмивання коштів. У документі перелічено такі ключові механізми: ліквідні пули, які дозволяють миттєвий обмін токенів P2P; крос-чейн мости, що приховують транзакції шляхом переміщення активів між блокчейнами; а також міксери (тумблери), які змішують криптовалюти багатьох користувачів, обриваючи ланцюжок відстеження. Міксери, такі як Tornado Cash, використовують для того, щоб перервати сліди руху коштів, ускладнюючи відстеження, при цьому багато з них працюють без KYC у юрисдикціях із м'яким регулюванням. Змішування коштів у одному пулі ускладнює слідчим відокремлення «забруднених» монет від легітимних.

Усі основні послуги DeFi пов’язані з ризиками відмивання коштів:

- Децентралізовані біржі (DEX): Часто не вимагають перевірок ідентифікації клієнта (KYC), що робить їх привабливими для злочинців. DEX дозволяють обмінювати активи, які недоступні на регульованих біржах (наприклад, Monero).
- Кредитування та запозичення: Незаконні активи можуть бути депоновані як застава для запозичення «чистих» активів, при цьому швидкий та автоматизований потік коштів через численні гаманці ускладнює відстеження.
- Фармінг прибутковості та стейкінг: Незаконні кошти можуть заробляти винагороди, які виглядають законними і можуть бути виведені на інші гаманці чи платформи, маскуючи початкове джерело.

5 https://www.canva.com/design/DAGrpWYqyjI/hgqF9NAPWGZtZ5koh5FEPA/view?utm_content=DAGrpWYqyjI&utm_campaign=designshare&utm_medium=link2&utm_source=uniquelinks&utlId=h8cf735abb5

- Синтетичні активи: Дозволяють імітувати реальні торги (наприклад, акціями або товарами) без фінансового нагляду, а прибутки, виведені у криптовалютах, ускладнюють регуляторам відстеження походження коштів.

Документ наводить приклади експлуатації DeFi злочинними організаціями:

1. Primeiro Comando da Capital (PCC) у Бразилії: Відмивали мільярди доларів від наркотрафіку ($9,3 млрд і $5,5 млрд), використовуючи підставні компанії та посередників, які переводили кошти через великі міжнародні біржі у криптовалюти, щоб позбавити їх відстежуваності. Ключову роль відігравали фінтех-фірми, які на той час мали мінімальний нагляд через відсутність суворих AML-вимог, на відміну від банків.
2. Lazarus Group (Північна Корея): На початку 2025 року використовувала DeFi-біржі Chainflip і Thorchain для відмивання понад 1,4 мільярда доларів. Chainflip зміг тимчасово задіяти заходи блокування транзакцій, жертвуючи частиною децентралізації, тоді як Thorchain, через відсутність центрального органу, не зміг швидко впровадити подібні засоби захисту, дозволивши хакерам обходити обмеження, взаємодіючи безпосередньо з кодом протоколу.

Регулятори розглядають можливість поширення традиційних фінансових законів на DeFi через «підхід, заснований на діяльності» (activity-based approach), який має на меті регулювати DeFi на основі виконуваної функції, а не структури. Європейський Союз робить початкові кроки, включаючи оцінку DeFi у спільному звіті EBA та ESMA згідно зі статтею 142 Регламенту MiCAR (прийнятого у 2023 році). Втім, фрагментовані національні підходи є неефективними проти глобальних децентралізованих мереж. Для забезпечення майбутнього DeFi необхідно поєднати законодавчу чіткість, міжнародну координацію та технологічні рішення.

Висновки:

- **Розширення регулювання на основі діяльності:** Регулювання, засноване на діяльності, повинно бути поширене на DEX, платформи кредитування та ліквідні пули, вимагаючи введення обов’язкових перевірок KYC/AML, щоб усунути лазівки, які експлуатуються злочинцями.
- **Інвестиції в аналітичні інструменти:** Слідчі та правоохоронні органи мають бути забезпечені передовими інструментами блокчейн-аналітики, моніторингом транзакцій на основі AI та засобами відстеження незаконних потоків в реальному часі.
- **Вбудовування захисту на рівні коду протоколу:** DeFi-протоколи повинні інтегрувати захисні механізми, такі як конфігуровані списки блокування транзакцій, оракули ризикових оцінок та прозорі ради валідаторів, щоб запобігати відмиванню коштів, не руйнуючи децентралізації.
- **Координація та стандартизація контролю:** Необхідна співпраця між регуляторами та спільнотою DeFi для встановлення стандартизованих API для звітності та обміну розвідданими про загрози, а також міжнародна координація для посилення контролю в критичних точках входу та виходу (on- та off-ramps).

Імперія Алієвих: як президентська родина Азербайджану вибудувала приховану фінансову мережу [6]

Проєкт “Aliyev Empire” від аналітичної платформи Atlas (The Sentry) розкриває масштабну корпоративну та фінансову мережу, пов’язану з родиною президента Азербайджану Ільхама Алієва. Центральною фігурою розслідування є його доньки Лейла та Арзу Алієви, на яких, за даними дослідників, оформлено володіння численними компаніями та активами у різних юрисдикціях світу. Загалом йдеться про понад 148 компаній, що оцінюються у більш ніж 13 мільярдів доларів, і ця мережа вибудувана таким чином, щоб приховати справжнє бенефіціарне володіння та убезпечити фінансову імперію від викриття.

Особливістю цього проєкту є його методологія: Atlas поєднує відкриті дані, корпоративні реєстри, архівні документи, витоки на кшталт Panama Papers та судові матеріали. Завдяки такому багатошаровому підходу вдалося створити цілісну карту зв’язків між особами, компаніями, фінансовими структурами й навіть колишніми державними службовцями, які виконували роль фіктивних власників. Ключовим прикладом є AtaHolding, колишній великий холдинг в Азербайджані, який через низку компаній-посередників та участь чиновників із податкової сфери фактично став одним із прихованих інструментів президентської родини для управління активами. Додатковим вузлом у схемі виступала Triangle Investments & Development у Лондоні, яка допомагала конвертувати прибутки для покупки престижної нерухомості в столиці Великої Британії.

Контекст, у якому з’явився цей проєкт, має важливе значення. Азербайджан — країна з високим рівнем корупції, слабкими інституціями та фактичною концентрацією влади в руках президентської династії. За таких умов економічні ресурси та державні контракти системно перетікають у приватні активи правлячої еліти. Випадки, коли компанії, пов’язані з дочками Алієва, отримували державні замовлення без конкуренції чи доступ до кредитів на особливих умовах, демонструють, як державна система перетворюється на механізм приватного збагачення. Водночас значна частина капіталу виводиться за кордон і розміщується у Лондоні, Москві, Дубаї та на Мальті. Це не лише створює шляхи для відмивання коштів, а й слугує гарантією для родини на випадок політичних потрясінь у самій країні.

У цьому сенсі проєкт “Aliyev Empire” є не просто журналістським розслідуванням чи базою даних. Це демонстрація того, як формується модель «гібридної державної корупції», коли влада і кримінально-фінансові інтереси стають невіддільними. Президентська родина контролює доступ до ключових секторів — насамперед енергетичного, який є основою економіки Азербайджану, — і перетворює його на особистий фінансовий ресурс. Зміни в офіційній звітності компаній, різке зменшення активів у балансах або передача активів через мережу офшорів і підставних осіб підтверджують системність цих процесів.

Важливим є й міжнародний вимір. Виведення капіталів у західні юрисдикції ставить під сумнів ефективність контролю за відмиванням коштів у країнах ЄС та Великій Британії. Придбання розкішної нерухомості або інвестиції у великі будівельні проєкти на Заході стають частиною глобальної проблеми — як авторитарні еліти використовують міжнародні фінансові центри для легалізації незаконних доходів.

[6] https://atlas.thesentry.org/azerbaijan-aliyev-empire/

Проєкт Atlas має також прикладний ефект: він створює відкриту карту, яку можуть використовувати журналісти, дослідники, антикорупційні організації чи урядові інституції. Це спосіб зробити прозорими ті схеми, які зазвичай приховані за складними юридичними і корпоративними оболонками. Автори наголошують, що база не є вичерпною й регулярно доповнюється, адже масштаби прихованої імперії Алієвих значно ширші за те, що вдалося задокументувати на сьогодні.

Таким чином, проєкт “Aliyev Empire” стає важливим дзеркалом для розуміння того, як корупційні династії використовують державні ресурси для формування приватних фінансових імперій, ховаючи їх за офшорами, фіктивними власниками та іноземною нерухомістю. Це приклад того, що корупція у сучасному світі не обмежується межами однієї країни: вона глобалізована, розгалужена і функціонує як транснаціональна мережа.

Висновки:

- **Інституційний контроль над ресурсами перетворюється на приватні активи –** державні контракти та енергетичні доходи в Азербайджані системно спрямовуються у структури, підконтрольні родині Алієвих.
- **Масштабне використання офшорів та фіктивних власників унеможливлює прямий контроль –** приховане бенефіціарне володіння дозволяє уникати як внутрішнього, так і міжнародного моніторингу.
- **Виведення капіталів у західні юрисдикції легалізує корупційні доходи –** Лондон, Дубай та Мальта стають “тихою гаванню” для сімейних статків.
- **Прозорість та open data є ключем до викриття** – саме поєднання відкритих реєстрів, журналістських розслідувань і витоків даних дозволило скласти картину “імперії” Алієвих.

Паливна мафія: як крадіжка пального перетворилася на мільярдну кризу [7]

У Мексиці за останнє десятиліття відбулася трансформація злочинного бізнесу, який із побічного заробітку для невеликих груп став повноцінною кримінальною індустрією з мільярдними прибутками. Йдеться про крадіжку пального — явище, відоме в країні під назвою huachicol.

Те, що ще десять–п’ятнадцять років тому виглядало як локальна проблема — несанкціоновані врізки у трубопроводи чи дрібні схеми продажу бензину «з-під поли», сьогодні стало однією з головних нелегальних економік у країні, яка за обсягами і структурою зрівнялася з наркобізнесом.

Суть феномена полягає в тому, що організовані злочинні угруповання зрозуміли: паливо — це не менш вигідний, а часом і безпечніший товар, ніж наркотики. Його можна красти безпосередньо з нафтопроводів, організовуючи незаконні врізки, або завозити з-за кордону з фальсифікованими документами, мінімізуючи податки й митні збори. Участь у таких схемах потребує складної координації, але вона ж створює можливості для значних доходів. Витрати на організацію врізок чи корупційне прикриття митниці швидко окуповуються завдяки обігу на чорному ринку. В результаті, великі мексиканські картелі почали активно диверсифікувати свої доходи: кокаїн і метамфетамін лишаються базовим товаром, але паливо забезпечує стабільний

[7] https://insightcrime.org/news/mexico-multibillion-dollar-fuel-theft-crisis/

потік коштів і дозволяє фінансувати інші злочинні операції, включно з відмиванням грошей, купівлею зброї та підкупом посадовців.

Особливо тривожним є той факт, що ця економіка можлива лише за умов системної корупції. Врізки у трубопроводи, транспортування цистернами, перепродаж через фіктивні компанії чи незаконний імпорт — усі ці етапи вимагають покриття з боку державних інституцій. До процесу втягуються не лише місцеві поліцейські чи чиновники, а й військові підрозділи та митники, які дозволяють паливним схемам існувати практично безкарно. Таким чином, huachicol стає не лише кримінальною практикою, а й своєрідною симбіотичною системою, у якій злочинні угруповання та державні структури взаємодіють задля взаємної вигоди.

Уряд намагався реагувати на кризу, оголошуючи кампанії «нульової толерантності», проводячи спецоперації та арештовуючи організаторів врізок. Втім, ці дії радше мають ситуативний, ніж системний характер. На кожен перекритий канал з'являються нові, адже прибутковість залишається колосальною. Окрім того, розслідування, які доходять до високопосадових чиновників чи впливових фігур, рідко доводяться до завершення. Це свідчить про те, що сама державна машина значною мірою уражена корупцією і нездатна самостійно ліквідувати кризу.

У підсумку крадіжка пального в Мексиці вже давно вийшла за межі злочину проти державної компанії Pemex чи бюджету. Це явище підриває макроекономічну стабільність, зменшує податкові надходження, створює паралельні ринки з власними «правилами гри» та посилює кримінальні організації, які завдяки цьому зміцнюють свій вплив і перетворюються на ключових гравців у регіональній політиці. Фактично паливна мафія стала новим елементом гібридної реальності Мексики: це водночас і кримінальна, і економічна, і політична проблема, яка формує середовище нестабільності й недовіри до держави.

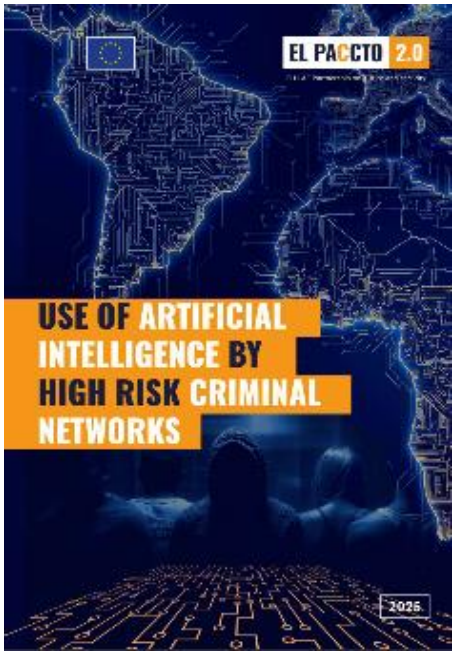
Висновки:

- **Крадіжка пального стала стратегічним джерелом доходів для картелів** – це вже не дрібний злочин, а індустрія з мільярдними оборотами.
- **Корупція є ключовим рушієм паливної мафії** – без участі митників, військових та чиновників ці схеми неможливі.
- **Спроби «гасити пожежу» арештами не вирішують проблему** – уряд має реформувати паливний сектор загалом, мінімізуючи монополію, впроваджуючи цифрові системи відстеження пального та прозорі канали імпорту.
- **Huachicol підриває державні фінанси і довіру до інституцій** – це створює паралельну тіньову економіку, де злочинці фактично замінюють державу.

Алгоритмічна злочинність: як штучний інтелект змінює екосистему кримінальних мереж [8]

Документ пропонує глибокий аналіз того, як штучний інтелект поступово інтегрується у діяльність злочинних мереж і стає не просто допоміжним інструментом, а ключовим елементом у їхньому функціонуванні. Якщо у попередні десятиліття організовані групи сприймали технології як інструменти підтримки — шифрування для зв'язку, анонімізація для онлайн-операцій, автоматизація для фінансових транзакцій, — то сьогодні вони будують цілісні злочинні екосистеми, в основі яких лежать алгоритми. Це не лише підвищує ефективність злочинної діяльності, а й змінює логіку її організації, створюючи умови для так званого «алгоритмічного врядування» у кримінальному світі.

[8] https://zenodo.org/records/16750778



Автори документа пропонують концептуальну матрицю, де поєднуються три виміри: мотивація злочинців (економічна, сексуальна, політична, терористична), технологічні інструменти (від генеративних моделей, deepfake та клонування голосу до адаптивного шкідливого ПЗ і автономних агентів) та організаційні структури (ієрархічні картелі, децентралізовані колективи, автономні кримінальні платформи). Такий підхід дозволяє побачити закономірності в адаптації штучного інтелекту до злочинних потреб і передбачити напрямки, у яких ця трансформація може розвиватися далі.

Традиційні ієрархічні структури — зокрема наркокартелі на кшталт Сіналоа чи CJNG (Халіско) — використовують штучний інтелект (AI) для оптимізації логістики, управління фінансовими потоками та контролю над своїми членами. Завдяки алгоритмам вони можуть точніше прогнозувати маршрути доставки наркотиків, уникати перехоплень, управляти ризиками та підтримувати дисципліну. Децентралізовані колективи, наприклад Yahoo Boys у Західній Африці чи хакерські групи на кшталт FunkSec, покладаються на AI у швидкому створенні контенту, генерації масових фішингових атак, автоматизації соціальної інженерії та поширенні викрадених даних.

Автономні кримінальні платформи — WormGPT, FraudGPT, Xanthorox AI, Storm-2139 — перетворюють штучний інтелект на ядро бізнес-моделі «злочину-як-послуги», пропонуючи будь-кому за підпискою доступ до інструментів злочинної діяльності. Нарешті, російські та іранські проксі-структури, інтегрують AI у гібридні операції: від маніпуляції виборами і масштабної дезінформації до кібератак на критичну інфраструктуру.

Документ наводить конкретні приклади: мексиканські картелі вже використовують алгоритми для шахрайства з емоційним забарвленням, коли створюються deepfake-дзвінки для вимагання викупу; хакерські спільноти тестують чат-боти для автоматизації атак на банки та урядові портали; африканські колективи, орієнтовані на масові онлайн-афери, застосовують AI для масштабування своїх схем до мільйонів одночасних контактів. Deepfake та voice cloning дозволяють створювати переконливі фальшиві «особистості» для шахрайських дзвінків, у тому числі від «родичів у біді» чи нібито урядових чиновників.

Найбільш тривожним трендом є формування автономних злочинних платформ, які функціонують фактично як новий «сервісний бізнес». Вони продають генерацію шкідливого коду, готові інструкції з обходу систем безпеки, автоматизовані набори для фішингових кампаній, а також інструменти відмивання коштів через криптовалюти. Такі платформи позбавлені географічної прив’язки та мають високий рівень автономності: їхні користувачі можуть навіть не знати одне одного, а злочини здійснюються алгоритмічно, без прямої людської координації. Це знаменує новий етап — перехід від злочинних груп до злочинних екосистем, які працюють за принципами SaaS-компаній.

Ще одна ключова тенденція — зникнення «людського обличчя» злочинності. Завдяки deepfake, синтетичним особистостям і генеративним моделям стає дедалі важче встановити, хто стоїть за злочином. Особистість більше не є статичною ознакою: її можна створити, змінити, приховати або масово відтворити. Це унеможливлює традиційні методи атрибуції і значно ускладнює роботу правоохоронних органів. У документі це описано як становлення «алгоритмічного врядування» у кримінальних мережах — системи, де рішення ухвалюються не конкретними людьми, а автоматизованими процесами, а правила встановлюються кодом.

Авторам вдалося зафіксувати і те, що зростає інтеграція AI у терористичні практики. Наприклад, ІДІЛ та афілійовані групи експериментують із застосуванням генеративного ШІ для пропаганди кількома мовами, що дозволяє поширювати ідеологію на нові аудиторії. Вони також тестують алгоритми для планування атак, пошуку слабких місць у захисті інфраструктури та анонімізації фінансових потоків. Терористи вбачають у штучному інтелекті інструмент, який можна використати для радикалізації, вербування і навіть персоналізованої пропаганди через чат-боти.

У документі наголошується, що цей зсув має глибокі наслідки для держав і міжнародної безпеки. Класичні підходи — кримінальні розслідування, судові процеси, екстрадиція — виявляються малоефективними проти мереж, які діють без центру та без конкретних «голів». Відповідальність розмивається: замість чітких організаторів є код, замість конкретних рішень — алгоритмічні процеси. У таких умовах надзвичайно складно встановити юридичну вину й забезпечити правосуддя.

Документ закликає до нових стратегічних рішень. Потрібне оновлення регуляторних рамок, зокрема створення правових категорій для злочинів, скоєних із використанням штучного інтелекту, а також відповідальності за розробку і поширення інструментів на кшталт WormGPT. Необхідно підвищувати інституційну спроможність держав — інвестувати у фахівців із кібербезпеки, створювати спеціалізовані підрозділи, налагоджувати співпрацю з приватним сектором. Ключову роль відіграє міжнародна кооперація: жодна країна не здатна самостійно боротися з транснаціональними алгоритмічними мережами. При цьому важливо зберегти баланс між безпекою і правами людини — нові регуляції не мають перетворюватися на інструмент тотального контролю.

Висновки:

- **Штучний інтелект уже став невід'ємною частиною злочинних мереж**, тому державам потрібні спеціалізовані підрозділи для моніторингу й протидії.
- **Автономні платформи «злочину-як-послуги»** роблять злочинність масово доступною, що потребує міжнародної криміналізації й глобального блокування таких сервісів.
- **Deepfake та генеративні моделі стирають особистість злочинців**, тому необхідно розвивати «захисний ШІ» та нові юридичні рамки для доказовості.
- **Терористичні та кримінальні групи застосовують ШІ для пропаганди й фінансування**, тож потрібна співпраця фінансових розвідок, технологічних компаній та інформаційні кампанії для суспільства.

У підсумку автори підкреслюють: штучний інтелект вже сьогодні створив нову парадигму злочинності, яку вони називають «алгоритмічною». Йдеться не просто про черговий інструмент у руках злочинців, а про фактор, що змінює саму суть організованої злочинності у XXI столітті. Традиційні групи, децентралізовані колективи, автономні платформи та державні проксі вже сьогодні взаємодіють на новому рівні, де алгоритми визначають темп, масштаб і форму злочинної діяльності. Якщо держави не почнуть діяти на випередження, світ може зіткнутися з феноменом кримінальних екосистем, які не лише важко зупинити, а й майже неможливо атрибутувати.

Рекомендовані та навчальні матеріали

Усередині ІДІЛ у Сомалі: як терористи ховаються, фінансуються й становлять глобальну загрозу [9]

У північній частині Сомалі, у регіоні Пунтленд, силові структури країни за підтримки союзників ведуть операції проти відроджених осередків Ісламської Держави, які укріпилися в гірських печерах та віддалених ущелинах. Журналісти Sky News мали доступ до деяких з цих печер — місць, де бойовики не просто переховувалися, а фактично управляли місцевими спільнотами, проводили побут, виробляли вибухівку й координували глобальні зв'язки. Печери слугують багатофункціональними базами: тут є спальні місця, кухні, навіть елементарні санітарні споруди, а на стінах лишилися сліди сажі від розпалів вогню, що свідчать про недавнє проживання.

Зі знайдених телефонів, SIM-карт, носіїв даних вдається реконструювати спосіб життя бойовиків: у відеозаписах видно сцени сімейного побуту, дітей, які збирають дрова, моменти розмов у машинах, сміх, заклики до джихаду. Такі записи вказують, що ці угруповання існують не лише як прихисток, а як повноцінні "спільноти", із спробами легітимізації в очах місцевих людей.

Ці укриття не є випадковими — вони стратегічно розташовані в складному гірському рельєфі, важкодоступному для наземного пересування, з мінімальною інфраструктурою й контрольованими шляхами. Дороги до входів часто брудні, віддалені, що змушує армію рухатися пішки чи використовувати допоміжний транспорт, а піщані основи часто приховують закладені вибухові пастки й саморобні міни.

Наземні колони часто супроводжуються групами саперів, що йдуть попереду, розміновують шлях і перевіряють рослинність на вибухівку.

Однією з ключових знахідок у знешкоджених об'єктах були майстерні з виготовлення бомб і ракет, компоненти саморобних засобів ураження, залишки дронів, що могли нести вибухові заряди, а також інструменти електропостачання — генератори та акумулятори, що дозволяли бойовикам використовувати електричні прилади.

Було виявлено навіть медичне обладнання, нове та запаковане, що свідчить про спробу створити елементарні медичні або госпітальні модулі.

Ці райони не тільки прихисток, але й хаби організаційного характеру: через телефонні мережі й криптовалютні гаманці бойовики переказують великі суми готівки, використовують глобальні грошові ланцюги, щоб фінансувати операції ІДІЛ у інших країнах. У одного з конфіскованих телефонів зафіксовано 80 000 доларів на цифровому гаманці. Радіодані та документи вказують на те, що ІДІЛ у Сомалі підтримує фінансові та організаційні контакти з групами у Демократичній Республіці Конго, Мозамбіку, Уганді і навіть Південно-Африканському регіоні.

Стаття також показує, що частина фінансування походить не лише з криптовалют, але й через вимагання, тиск на місцевих підприємців у портових містах і сплату «податків» або «тарифів» з

[9] https://news.sky.com/story/hunting-for-isis-inside-the-caves-at-heart-of-expanding-terror-network-13414040

бізнесів. У місті Босасо, портовому центрі, місцевим бізнесам часто нав'язували такі виплати грошима під загрозами вибухів чи репресій.

За даними інтерв'ю військових та представників армії, з моменту початку операцій ліквідовано щонайменше 600 бойовиків ІДІЛ, але питання залишається відкритим: чи достатньо цього, щоб знищити мережу, чи лише перемістити її активи в інші регіони?

У статті також порушено питання кооперації екстремістів: знайдено листування, яке вказує на співпрацю ІДІЛ у Сомалі з Хуситами в Ємені — особливо в контексті перевезення зброї, логістики та маршрутів морського транспорту.

Морські шляхи між Сомалі і Аравійським морем використовуються як канали для переміщення зброї, людей, фінансових ресурсів і добрив.

Таким чином, стаття демонструє, що ІДІЛ не просто переховується в печерах, але активно консолідує ресурси, розвиває глобальні мережі й адаптується до тиску держав, використовуючи віддалені території як лабораторію для стратегічного відродження — з можливістю розширення на інші регіони світу.

Висновки:

- **ІДІЛ у Сомалі використовує гірські печери** як довгострокові бази, що вимагає постійного моніторингу дронами й супутниками для запобігання їх відновленню.
- **Основні джерела фінансування бойовиків** — криптовалюти, вимагання та "податки" з бізнесу, тому необхідний суворий контроль за цифровими активами й портовою економікою.
- **Мережа ІДІЛ активно використовує морські шляхи** для глобальних операцій, що потребує міжнародного морського патрулювання й координації флотів.
- **Ліквідація бойовиків не знищує мережу**, яка адаптується й переміщується, тож акцент має бути на стримуванні й роботі з місцевими громадами.

Інші новини

Європейський регуляторний розкол: Боротьба за централізований нагляд над криптоактивами та виклики моделі "мультиемітента" стейблкоїнів» [10] [11] [12]

Наразі в Європейському Союзі точиться запекла суперечка щодо централізації нагляду за великими криптофірмами, яка безпосередньо стосується ефективного впровадження нового Регламенту ЄС про ринки криптоактивів (MiCA). Три країни-члени — Франція, Австрія та Італія — спільно виступають за розширення повноважень Європейського управління з цінних паперів та ринків (ESMA), яке базується в Парижі, щоб воно взяло на себе пряму наглядову роль над основними гравцями крипторинку. Цей заклик зумовлений глибокою стурбованістю, що

[10] https://www.reuters.com/sustainability/boards-policy-regulation/france-threatens-block-crypto-licence-passporting-eu-regulatory-fight-2025-09-15/
[11] https://www.reuters.com/sustainability/boards-policy-regulation/maltas-financial-regulator-opposes-push-centralise-eu-crypto-supervision-2025-09-16/
[12] https://www.reuters.com/business/finance/bank-italy-urges-clarity-rules-multi-issuance-stablecoins-2025-09-18/

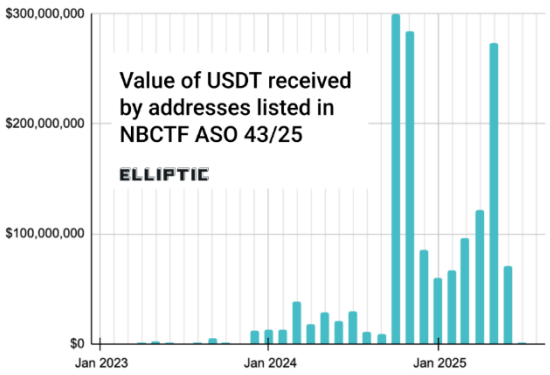
національні регулятори можуть непослідовно тлумачити положення MiCA, що створює ризик нерівномірного застосування правил по всьому блоку.

Основне побоювання, висловлене регуляторами, включно з Управлінням фінансових ринків Франції (AMF), зосереджене на моделі "паспортування" (passporting), передбаченій MiCA. Ця модель дозволяє криптофірмам, які отримали ліцензію в одній країні ЄС, безперешкодно працювати у всіх 27 державах-членах. Французькі регулятори побоюються, що така система стимулюватиме компанії шукати отримання ліцензії в юрисдикціях із більш поблажливим наглядом, підриваючи тим самим довіру до всього єдиного крипторинку ЄС. Через це Франція виступила із попередженням, не виключаючи можливості використати «крайні заходи» – оскаржити паспортування ліцензії, виданої іншою державою-членом, щоб запобігти експлуатації регуляторних лазівок. Регулятори Франції (AMF), Австрії (FMA) та Італії (CONSOB) у своїй спільній позиції підкреслили, що досвід перших місяців застосування MiCA вже показав, що "наглядова конвергенція між національними органами швидко досягає своїх меж і є недостатньою для гарантування єдиного застосування стандартів у межах ЄС".

З іншого боку, Мальта виступила категорично проти передачі нагляду ESMA. Управління фінансових послуг Мальти (MFSA) підтримує посилення координації між національними регуляторами, але виступає проти централізованого контролю, застерігаючи, що така централізація на цьому етапі лише "запровадить додатковий шар бюрократії, що може перешкоджати ефективності". Ця напруга розгортається на тлі того, що сама Мальта вже потрапила під пильну увагу ESMA: у липні Управління опублікувало експертний висновок щодо ліцензування криптофірм MFSA, де було встановлено, що Мальта лише "частково відповідає очікуванням" при авторизації постачальників послуг криптоактивів (CASP), залишивши низку істотних питань невирішеними. ESMA наголосило, що послідовність між державами-членами ЄС має важливе значення для стандартизації ліцензування та нагляду, передбаченого MiCA.

Окрім нагляду за криптоактивами загалом, Італія через свій центральний банк підняла окреме, але пов'язане питання, щодо необхідності єдиних правил ЄС для стейблкоїнів, особливо для їх транскордонного випуску, з метою захисту прав користувачів. Центральний банк Італії висловив занепокоєння щодо моделі "мультиемітента", коли стейблкоїни, випущені ліцензованими установами ЄС, можуть вважатися взаємозамінними з токенами, випущеними неєвропейськими структурами тієї ж компанії. Це створює значні ризики для фінансової стабільності, включаючи можливість того, що емітенти з третіх країн можуть обійти вимоги MiCA щодо захисту споживачів, прозорості та розкриття інформації. Такий підхід також може призвести до невідповідності резервів під час погашення, оскільки емітенти ЄС можуть отримувати запити на погашення від нерезидентів ЄС. Для запобігання цим регуляторним прогалинам пропонується обмежити випуск стейблкоїнів юрисдикціями, які дотримуються еквівалентних регуляторних стандартів, гарантують погашення за номінальною вартістю та запроваджують транскордонні угоди про реагування на кризи. Таким чином, дискусія в ЄС обертається навколо ключового питання: як забезпечити єдиний, надійний та захищений регуляторний ландшафт, уникаючи як бюрократичної централізації, так і ризиків нерівномірного застосування національних правил, особливо в умовах, коли ESMA вказує на недостатнє виконання вимог деякими країнами.

Ізраїль пов'язує криптогаманці, які отримали 1,5 мільярда доларів, з Корпусом вартових ісламської революції Ірану [13] [14]



Міністр оборони Ізраїлю випустив адміністративний наказ, що є офіційним правовим інструментом, який ґрунтується на Законі Ізраїлю про боротьбу з тероризмом 5776-2016. Основний зміст наказу полягає в арешті конкретних криптовалютних гаманців та віртуальних активів, що в них містяться. В основі цього рішення лежить тверде переконання, що ці цифрові активи є власністю визнаної терористичної організації «Корпус вартових ісламської революції» або використовувалися для скоєння «тяжкого терористичного злочину». Наказ містить перелік адрес гаманців USDT, які підпадають під цей наказ про арешт, та зобов'язує будь-яку особу, що має справу з цим майном, негайно повідомити про це ізраїльську поліцію та Національне бюро з питань фінансування боротьби з тероризмом у Міністерстві оборони. Наказ набуває чинності терміном на два роки або до підписання наказу про остаточну конфіскацію. Додатковий аналіз від Elliptic посилює та деталізує висновки, викладені в наказі. Згідно з аналітичним звітом, Наказ про арешт, виданий ізраїльською владою, включає 187 адрес криптовалютних гаманців. Цей аналіз надає значний фінансовий контекст, показуючи, що ці гаманці сукупно отримали близько 1,5 мільярда доларів у стейблкоіні Tether (USDT). Як наслідок, Tether вжив заходів, заблокувавши 39 із цих адрес, що призвело до ефективного замороження 1,5 мільйона доларів у USDT. Загалом, ці обставини свідчать про скоординовані зусилля з боку уряду та приватної аналітичної компанії для використання аналізу блокчейну та правових механізмів з метою протидії фінансуванню тероризму в сфері цифрових активів. Це демонструє не лише активну державну позицію в боротьбі з незаконними фінансовими потоками, але й еволюцію методів, що використовуються для санкціонування та конфіскації активів, пов'язаних з терористичною діяльністю у фінансовому просторі, що стрімко розвивається.

Венесуела, «картелі» та ракетний удар США: що криється за гучними заявами [15]

2 вересня 2025 року відбувся інцидент, який багато експертів уже називають «зсувом парадигми» у війні США з наркотиками у Південній Америці. Американські військові завдали ракетного удару по швидкісному катеру біля узбережжя Венесуели. На борту перебувало 11 осіб, більшість з яких були жителями невеликого прибережного міста Сан-Хуан-де-Унаре у штаті Сукре. Цей регіон давно відомий як транзитний хаб для контрабанди та нелегальної міграції, а катер, за наявними даними, ймовірно прямував до Тринідаду і Тобаго, що за 180 кілометрів від узбережжя.

Вашингтон подав цей удар як масштабний крок у боротьбі з міжнародною наркоторгівлею. Президент Дональд Трамп заявив, що екіпаж катера був «позитивно ідентифікований як наркотерористи Tren de Aragua», організації, яку США нещодавно офіційно визнали

[13] https://www.elliptic.co/blog/israel-links-crypto-wallets-handling-billions-to-irans-revolutionary-guard
[14] https://nbctf.mod.gov.il/he/Announcements/Documents/%d7%a6%d7%aa%2043-25.pdf
[15] https://insightcrime.org/news/behind-the-curtain-venezuelas-cartels-and-the-us-missile-strike-explained/

терористичною. У риториці американської адміністрації цей крок подано як доказ того, що режим Ніколаса Мадуро контролює та координує діяльність кримінальних структур, використовуючи їх для поширення наркотиків, торгівлі людьми та організованого насильства у Західній півкулі. Державний секретар Марко Рубіо навіть наголосив: «Замість того щоб перехопити, ми його підірвали. І це повториться». Тим самим було анонсовано зміну всієї логіки американської стратегії протидії наркотрафіку: від перехоплення до превентивного знищення.

Однак дані, зібрані з різних джерел, малюють значно складнішу картину. По-перше, наявність 11 людей на борту виглядає нелогічною для класичного наркокур'єрського рейсу. Зазвичай подібні човни обмежуються екіпажем у 2–3 особи, максимум чотирьох, якщо є ризик піратських нападів. Така кількість людей радше свідчить про перевезення мігрантів чи контрабандистів, а не лише наркотиків. По-друге, напрямок на Тринідад і Тобаго не належить до стандартних маршрутів, якими постачають кокаїн до США. Типовий шлях із північного узбережжя Венесуели та Колумбії веде до Домініканської Республіки чи інших карибських точок із подальшим транзитом у США. Натомість рейси на Тринідад частіше пов'язані з перевалкою у напрямку Європи через численні французькі, голландські та британські території у Карибському морі, що мають зручні легальні транспортні канали для контрабанди.

Сумнів викликає й офіційна версія про участь Tren de Aragua. Хоча ця венесуельська організація справді є найпотужнішим злочинним угрупованням країни, її ядро спеціалізується на рекеті, торгівлі людьми, мікротрафіку та контролі локальних чорних ринків. У минулому Tren de Aragua намагався закріпитися у штаті Сукре, проте був витіснений місцевими бандами, які традиційно контролюють східнокарибські контрабандні маршрути. Доказів того, що ця структура активно задіяна у міжнародному наркобізнесі, немає; максимум — поодинокі випадки роботи як «субпідрядників» для великих картелів. Тому твердження, що катер був безпосередньо операцією TDA, виглядає політично мотивованим перебільшенням.

Ще більш суперечливими є звинувачення на адресу самого Ніколаса Мадуро. Американські офіційні особи називають його одним із найбільших наркоторговців світу, опираючись на звинувачення 2020 року, коли Мадуро та його соратника Діосдадо Кабельйо інкримінували керівництво так званим «Картелем сонць» (Cártel de los Soles). Та дослідження InSight Crime показують: йдеться не про класичний картель, а радше про «гібридну кримінальну систему управління», у якій венесуельський режим створює альянси з кримінальними групами, регулює нелегальні економіки та використовує їхні прибутки для виживання режиму та винагороди лояльних силовиків і політиків. Інакше кажучи, Мадуро очолює систему державної корупції, тісно переплетену з криміналом, але некоректно зображати його як «світового наркобарона» у класичному розумінні.

Що ж дає цей удар у практичному сенсі? На короткій дистанції — серйозний стримувальний ефект. Венесуельські контрабандисти ймовірно утримаються від використання швидкісних катерів, поки у водах присутні американські кораблі. Сам режим також відреагував показовими антинаркотичними операціями, намагаючись продемонструвати контроль над ситуацією. Але в довгостроковій перспективі глобальні потоки кокаїну не зникнуть, а лише переорієнтуються. Уже зараз очевидно, що трафік знову посилюватиметься через південні маршрути: Гайану, Суринам, північ Бразилії, які більше орієнтовані на Європу, або ж через Колумбію та Центральну Америку, що веде до США.

Отже, ракетний удар США мав радше політичний та символічний характер, ніж стратегічно вирішальний. Він демонструє жорсткішу лінію Вашингтона, створює атмосферу тиску на Мадуро та його оточення, але реального зменшення масштабів міжнародного наркотрафіку очікувати не варто. У кращому випадку, удар тимчасово порушив звичні схеми перевезень і змусив кримінальні мережі адаптуватися. Як показує досвід останніх десятиліть, глобальний наркоринок завжди знаходить нові шляхи, і ця ситуація навряд чи стане винятком.

«Криза шахрайства на Booking.com»: як платформа стає знаряддям обману [16]

Стаття, опублікована на платформі Which?, досліджує феномен поширення шахрайських схем на популярній платформі бронювання житла Booking.com, акцентуючи увагу на повідомленнях користувачів, які вважають, що отримували шахрайські повідомлення через офіційні канали платформи, а також на випадках підробленого або фіктивного розміщення об'яв про житло.

Журналісти провели опитування серед користувачів, і приблизно 9 % з 237 опитаних заявили, що за останні два роки отримували повідомлення, які, на їхню думку, були шахрайськими, але виглядали так, ніби надіслані через систему повідомлень Booking.com. Ці повідомлення часто вимагали підтвердити бронювання шляхом переказу коштів на сторонні рахунки — класична фішингова схема, але небезпечна через те, що видається як "офіційна" комунікація.

Крім того, стаття розкриває інший аспект проблеми: фіктивні розміщення об'яв про житло. Приклади включають кілька випадків, коли шахраї створювали об'яви з фото, які належать реальним об'єктам (наприклад, знімки, зроблені професійним фотографом), але без згоди власників. У одному з кейсів господар будинку, який ніколи не вносив своє майно в Booking.com, виявив, що його маєток самостійно додали до платформи. Він намагався звернутися до служби підтримки, але без ідентифікатора об'яви це виявилось безрезультатним. Пост пробув активним на сайті майже місяць перед видаленням — лише після втручання журналістів і звернення через окрему форму "report illegal content".

Стаття також наводить інший винахідливий шахрайський сценарій: користувач отримує підтвердження бронювання, яке він ніколи не здійснював, із повідомленням, що кошти вже сплатили. У такому випадку Booking.com підтвердив, що можливо зловмисники отримали доступ до облікового запису користувача для створення бронювання без його відома. У відповідь компанія погодилась повернути кошти після підтвердження з боку клієнта, стверджуючи, що не виявила порушення власних систем безпеки.

Журналісти закликають британського регулятора із онлайн-безпеки — Ofcom — розслідувати, чи достатньо Booking.com зробив для видалення незаконного контенту й захисту користувачів у рамках нового Online Safety Act. У статті міститься низка рекомендацій до платформи: вимагати верифікацію особи від орендодавців, обмежувати можливість надсилання повідомлень із платформи з проханням про оплату, активніше відслідковувати і видаляти підозрілі пости, зробити функцію скарги на шахрайство більш помітною і оперативною, впровадити службу підтримки для термінових випадків, а також змінити систему відгуків, щоб якщо багато користувачів попереджають про шахрайство, це було видно на першій сторінці.

Booking.com відповів, що питання кібербезпеки є пріоритетом, і що він використовує AI/машинне навчання для виявлення аномалій. Компанія каже, що має процедури верифікації орендодавців і перевірки об'яв, а також спирається на понад 339 мільйонів перевірених відгуків. Водночас вони радять користувачам не надсилати платіжні дані електронною поштою або повідомленнями, а у випадку сумніву — звертатися до служби підтримки чи перевіряти даність повідомлення безпосередньо через портал платформи.

Загалом, стаття демонструє, що Booking.com, як платформа з великою кількістю користувачів і транзакцій, стала привабливою мішенню для шахраїв, і що існуючі заходи з безпеки не завжди спрацьовують. Вона підкреслює, що шахрайство може відбуватися на межі технічного обману

[16] https://www.which.co.uk/news/article/the-scam-crisis-on-booking.com-aAj2P4i2c06f

та експлуатації слабких місць у системі підтримки та модерації, і що багато випадків лишаються непоміченими або не розслідуваними оперативно. Для повноцінного захисту користувачів необхідні більш жорсткі превентивні заходи, прозорі процедури реагування, а також чіткий баланс між зручністю користування та безпекою.

Для загального розвитку

Моніторинг транзакцій 2025 – як зробити його ефективним для вашого бізнесу [17]

Стаття від AMLCube присвячена трансформації традиційних систем моніторингу транзакцій, які в умовах 2025 року більше не відповідають потребам бізнесу та вимогам регуляторів. Автор наголошує, що підходи, побудовані на простих правилах і порогах, вже не забезпечують ефективності, оскільки злочинні схеми постійно ускладнюються, а регуляторні органи дедалі більше орієнтуються не на кількість сигналів чи повідомлень SAR, а на якість, релевантність і практичну користь для розслідувань. У цьому контексті ключовим стає перехід від класичного Transaction Monitoring до ширшої концепції Monitoring for Suspicious Activity (MSA), що передбачає поєднання транзакційних даних із поведінковими індикаторами, ризиковими факторами, історією клієнта та інформацією з попередніх розслідувань. Ефективність тепер визначається тим, наскільки система охоплює пріоритетні типології, наскільки точно виявляє релевантні ризики і наскільки цінною є інформація, передана правоохоронцям.

У статті виокремлено п’ять головних практик, які забезпечують ефективність у новій парадигмі:

- **Переосмислення того, що означає “добре”.** Замість метрик обсягу (кількість сигналів, кількість SAR, % оброблених акаунтів) — зрушення до якості та релевантності: чи покриваються пріоритетні ризики, чи використовуються поведінкові та контекстуальні дані, наскільки часто спрацювання приводять до адекватних розслідувань, чи повідомлення до правоохоронців дають потрібну інформацію.
- **Проєктування для інтеграції, а не ізоляції.** Моніторинг має бути інтегрований із іншими елементами програми фінансового моніторингу: дані з розслідувань і типології мають впливати на дизайн моделей, відгуки front-office та внутрішні звіти мають коригувати ризикові індикатори, моніторинг має бути тісно пов’язаний із ризиковим рейтингом клієнтів, із даними, отриманими при онбордингу. Доступ до контексту для аналітиків має бути легким.
- **Сприймати перехід як стратегічну бізнес-зміну.** Не порівнювати нові моделі просто з тими, що були, якщо цілі змінилися. Визначення нових цілей (наприклад, покращення виявлення високопріоритетних загроз, відповідність типологіям) має бути пріоритетом.

[17] https://www.amlcube.com/post/transaction-monitoring-2025-how-to-make-it-effective-for-your-business

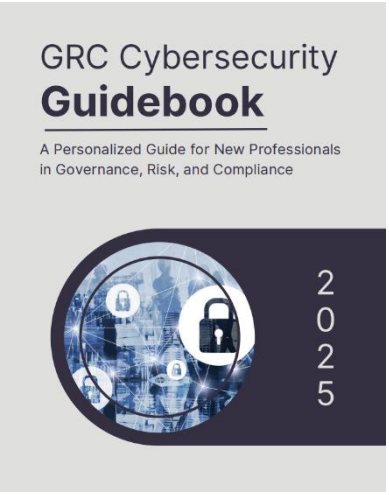
Використовувати proof-of-concept тестування на історичних даних, вводити покращення поступово — не обов'язково замінити все одразу.

- **Надати належний рівень нагляду.** Моделі фінансових злочинів не обов'язково мають йти через ті ж самі процеси управління модельним ризиком, що, скажімо, моделі кредитного ризику. Треба адаптувати рівень нагляду залежно від важливості моделі для бізнесу, уникати зайвих дублювань перевірок, скорочувати затримки. Якщо зміни моделі тривають місяцями — це ознака, що управління є неефективним.
- **Пріоритет пояснюваності, як усередині організації, так і перед регуляторами.** Моделі мають бути зрозумілими: які ризики вони націлені виявляти, як обрані типології, які індикатори входять, як формується вихід, як інтерпретувати спрацювання. Якщо аналітик не може пояснити, чому спрацював alert — розслідування затримується, система втрачає довіру. Підтримка технологій візуалізації або інструментів, що допомагають підсумовувати й пояснювати.

Автор також наголошує на практичних наслідках для бізнесу, який ігнорує ці зміни. Серед основних ризиків — високий рівень хибних спрацювань, що веде до значних витрат на перевірки при низькій якості результатів; недостатня інтеграція з іншими процесами, яка робить систему негнучкою перед новими типологіями; затримки через громіздке управління змінами моделей, що паралізує здатність адаптуватися; а також загроза регуляторних санкцій, якщо підходи компанії не відповідатимуть сучасним очікуванням, закріпленим у міжнародних стандартах, таких як рекомендації Вольфсберзької Групи.

Основна ідея статті полягає в тому, що моніторинг транзакцій має еволюціонувати з інструмента "спрацювань" у ключовий елемент системи боротьби з фінансовими злочинами, інтегрований із даними, процесами і типологіями. Лише такий підхід дає змогу бізнесу забезпечити високу якість результатів, відповідність регуляторним вимогам і довіру з боку наглядових і правоохоронних органів.

Посібник з кібербезпеки. Персоналізований посібник для нових фахівців у сфері управління, ризиків та відповідності [18]



Даний документ є посібником з кібербезпеки в сфері GRC, тобто Governance (управління), Risk Management (управління ризиками) і Compliance (дотримання нормативів). GRC у кібербезпеці — це три ключові складові, які допомагають організаціям управляти процесами кібербезпеки, щоб відповідати нормативним вимогам, знижувати ризики та узгоджувати ініціативи з безпеки з бізнес-цілями. Цей підхід стає дедалі важливішим, оскільки кіберзагрози стають все більш витонченими.

Основні компоненти GRC:

- Управління: Це політики, процедури та процеси, що визначають, як керується та контролюється кібербезпека в організації. Воно включає залучення керівництва, узгодження стратегій та розподіл ресурсів.

[18] https://media.licdn.com/dms/document/media/v2/D4D1FAQHLHiWYjPKxHg/feedshare-document-pdf-analyzed/B4DZlSwEM3H0AY-/0/1758029969049?e=1759363200&v=beta&t=MKfHc6xxXCtFTdGynpOHYsDNsxTITbMVEGAfEVyESzQ

- Управління ризиками: Цей процес охоплює ідентифікацію, оцінку та пом'якшення ризиків для активів, даних та систем організації. Це безперервний цикл, що включає виявлення вразливостей, оцінку їх впливу та розробку планів пом'якшення, а також постійний моніторинг.
- Дотримання нормативів: Це забезпечення того, що організація відповідає всім відповідним правовим, нормативним та внутрішнім вимогам щодо кібербезпеки. Воно включає регулярні аудити та взаємодію з регуляторними органами.

Документ також визначає ролі та обов'язки GRC-фахівців з кібербезпеки, які включають розробку політик, проведення оцінок ризиків, розробку планів пом'якшення, забезпечення дотримання галузевих стандартів та підготовку звітів про дотримання. Серед необхідних навичок для таких фахівців виділяються знання кібербезпеки (протоколи, шифрування), вміння аналізувати ризики, знання нормативної бази та сильні навички комунікації.

У посібнику згадуються поширені регуляторні рамки, з якими мають бути знайомі GRC-фахівці, а саме:

- GDPR (General Data Protection Regulation): Регламент ЄС, що фокусується на захисті персональних даних та конфіденційності.
- PCI DSS (Payment Card Industry Data Security Standard): Стандарти безпеки для операцій з платіжними картками.
- NIST Cybersecurity Framework: Добровільна структура, розроблена Національним інститутом стандартів і технологій США (NIST) для управління та зменшення ризиків кібербезпеки.

Для реалізації GRC-процесів у кібербезпеці використовуються різні інструменти та технології, включаючи програмне забезпечення для управління ризиками, платформи для управління дотриманням нормативів та інструменти для моніторингу безпеки.

Посібник також надає ключові рекомендації для GRC-фахівців, такі як створення культури усвідомлення ризиків, використання ризикорієнтованого підходу, впровадження постійного моніторингу, регулярне проведення аудитів та активна міжвідомча співпраця з юридичними, комплаєнс- та бізнес-командами.

На завершення, документ підкреслює, що GRC-фахівець відіграє вирішальну роль у формуванні безпекової культури організації. Подальші кроки для таких спеціалістів включають нарощування знань у сфері регуляторних рамок, використання стратегій управління ризиками та постійну співпрацю з іншими підрозділами.

Ваша думка важлива!

1. Як, на вашу думку, можна забезпечити ефективну перевірку інформації про КБВ у високоризикових секторах, особливо в умовах обмежених ресурсів держави?
2. Які практичні кроки, на вашу думку, можуть допомогти підвищити якість SAR та уникнути «захисного звітування» у вашій установі?
3. Чи можливе, на вашу думку, ефективне регулювання DeFi без руйнування його децентралізованої природи, і якщо так – яким чином?
4. Які додаткові заходи мають вживати європейські юрисдикції, щоб запобігти використанню їхніх фінансових ринків для легалізації корупційних доходів, подібних до кейсу «Імперії Алієвих»?
5. Наскільки, на вашу думку, правоохоронні органи готові протистояти «алгоритмічному врядуванню» у кримінальному світі, і які технологічні інструменти їм найбільше потрібні?
6. Яким чином українські інституції можуть посилити прозорість у паливно-енергетичному секторі, щоб запобігти «зрощенню» бізнесу з організованими кримінальними групами? Чи достатньо дієвою є система контролю за ліцензіями, акцизами та переміщенням палива?
7. Які кроки варто зробити для посилення співпраці з IT-компаніями та соціальними мережами, щоб запобігти використанню їхніх платформ для радикалізації, вербування та поширення пропаганди?

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-2025-38

Бюлетень є 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].