Методологічний бюлетень

Серійний номер: МінФін-AML-2025-32

Серпень 2025

“Маленька дія часто спричиняє великий поштовх”

Ноа Скалін

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

АУДІОПЕРЕКАЗ

Керівні принципи щодо критеріїв оцінки знань та компетентності відповідно до MiCA [1]

Документ є Фінальним звітом Європейського управління з цінних паперів та ринків (ESMA). Метою публікації цих керівних принципів є зміцнення захисту інвесторів та забезпечення відповідного рівня знань і компетентності персоналу, який надає інформацію або консультації щодо криптоактивів чи послуг, пов'язаних з криптоактивами. Це досягається шляхом забезпечення мінімального рівня знань і компетентності такого персоналу та врахування специфічних особливостей та ризиків ринків криптоактивів. Керівні принципи допомагають постачальникам послуг з криптоактивів (CASP) виконувати свої зобов'язання діяти в найкращих інтересах своїх клієнтів і підтримують компетентні органи в адекватній оцінці того, як CASP виконують ці зобов'язання. Очікується, що ці керівні

[1] https://www.esma.europa.eu/sites/default/files/2025-07/ESMA35-1872330276-2380_Final_Report_on_MiCA_Guidelines_on_knowledge_and_competence.pdf

принципи сприятимуть більшій конвергенції критеріїв оцінки знань та компетентності персоналу, що надає консультації або інформацію про криптоактиви чи послуги, пов'язані з криптоактивами, та їх застосуванню. Положення MiCA щодо надання послуг з криптоактивів набули чинності 30 грудня 2024 року.

ESMA було уповноважено видати ці керівні принципи згідно зі статтею 81(15) MiCA. Стаття 81(7) MiCA вимагає, щоб CASP, які надають консультації щодо криптоактивів, гарантували, що фізичні особи, які надають консультації або інформацію про криптоактиви чи послуги, пов'язані з криптоактивами, від їх імені, володіють необхідними знаннями та компетентністю для виконання своїх зобов'язань. Крім того, ESMA вважає, що всі CASP, а не лише ті, що надають консультації, повинні забезпечувати, щоб фізичні особи, які надають інформацію про криптоактиви чи послуги, пов'язані з криптоактивами, володіли необхідними знаннями та компетентністю для виконання своїх зобов'язань, відповідно до статті 68(5) MiCA. Керівні принципи застосовуються до компетентних органів та CASP і набудуть чинності через шість місяців після їх публікації на веб-сайті ESMA усіма офіційними мовами ЄС.

Ринок криптоактивів характеризується високою доступністю для роздрібних інвесторів через онлайн-платформи, низькі мінімальні інвестиції та цілодобову роботу. Однак знання учасників ринку, особливо роздрібних інвесторів, про криптоактиви та пов'язані послуги залишаються обмеженими. Крім того, ринки криптоактивів відзначаються швидким створенням нових активів та високою волатильністю, що перевищує традиційні фінансові інструменти. Оскільки MiCA не пропонує такого ж рівня захисту інвесторів, як MiFID II (наприклад, відсутність вимог до управління продуктами чи тестів на відповідність), зростає ризик потенційної шкоди, особливо для роздрібних інвесторів. Тому вкрай важливо, щоб персонал CASP, який надає консультації або інформацію, володів та підтримував відповідний рівень знань та компетентності.

У відповідь на консультаційний документ, більшість респондентів, включаючи Групу зацікавлених сторін ринків цінних паперів (SMSG), погодилися з підходом ESMA щодо мінімальних порогів кваліфікації, досвіду та безперервного професійного розвитку (CPD) для персоналу. Для персоналу, що надає інформацію, ESMA запропонувала мінімум 80 годин професійної кваліфікації та 6 місяців досвіду під наглядом. ESMA підкреслила, що 80 годин є доречним і пропорційним мінімумом, що дозволяє персоналу розуміти ключові аспекти ринків криптоактивів, таких як структура ринку та кібербезпекові ризики. Для персоналу, що надає консультації, ESMA запропонувала мінімум 160 годин професійної освіти, або інші варіанти, такі як вища освіта з досвідом, або професійний досвід за MiFID II чи IDD. ESMA аргументувала, що 160 годин є необхідним для забезпечення високої якості консультаційних послуг, враховуючи волатильність криптоактивів та специфічні ризики. CASP можуть застосовувати вищі стандарти залежно від спектру пропонованих послуг.

Щодо тематичних знань, ESMA уточнила, що персонал, який надає інформацію, повинен розуміти ключові характеристики, ризики та особливості лише тих криптоактивів та послуг, які пропонуються конкретним CASP. ESMA також виключила вимогу щодо розуміння загальних податкових наслідків для персоналу, що лише надає інформацію, вважаючи це непропорційним. Для оцінки вартості вимагається лише базове розуміння механізмів оцінки. Основними ризиками, які необхідно враховувати, є волатильність, кібербезпекові ризики (зломи, крадіжки), ризики неправильного зберігання приватних ключів, ризики IT-програм та ризики передачі криптоактивів. Крім того, персонал повинен мати базове розуміння механізмів консенсусу, правил валідації транзакцій, масштабованості, рівня децентралізації, структури управління, заходів захисту мережі, інтероперабельності, варіантів використання та економічної моделі протоколів.

Для існуючого персоналу, який вже надає інформацію або консультації на дату набрання чинності керівними принципами, ESMA дозволяє вважати їх компетентними, якщо вони успішно

надавали такі послуги на повну ставку, під наглядом або без нього, протягом мінімум 1 року до набрання чинності. CASP мають гнучкість у методах демонстрації цієї компетентності, наприклад, через щорічні оцінки або внутрішні/зовнішні іспити. ESMA встановила мінімальну кількість годин безперервного професійного розвитку (CPD) на рік: 10 годин для персоналу, що надає інформацію про менш складні криптоактиви, та 20 годин для персоналу, що надає консультації. Зміст CPD повинен охоплювати регуляторні зміни, ключові ринкові розробки та нові технології, включаючи потенційні ризики для інвесторів. CPD також має включати перевірку набутих знань та компетентності.

Щодо автоматизованого або напівавтоматизованого надання інформації чи консультацій, ESMA уточнила, що керівні принципи поширюються на персонал, відповідальний за визначення змісту інформації або консультацій, а також на персонал, що встановлює параметри та налаштування для її надання, щоб забезпечити точність та доречність. Група зацікавлених сторін ринків цінних паперів (SMSG) загалом підтримала керівні принципи, але висловилася за суворішу перевірку компетентності, пропонуючи проведення її зовнішніми сторонами, а не самими CASP. SMSG також закликала до розробки затверджених програм професійної кваліфікації та публікації списків затверджених освітніх провайдерів.

Керівні принципи передбачають, що CASP повинні щорічно оцінювати та переглядати ефективність своїх політик та процедур щодо знань та компетентності персоналу. Персонал, який не набув необхідних знань та компетентності, не може надавати відповідні послуги, якщо тільки він не працює під наглядом, при цьому період нагляду не може перевищувати 4 років. Керівники повинні бути компетентними та брати на себе відповідальність за послуги, надані персоналом під їхнім наглядом.

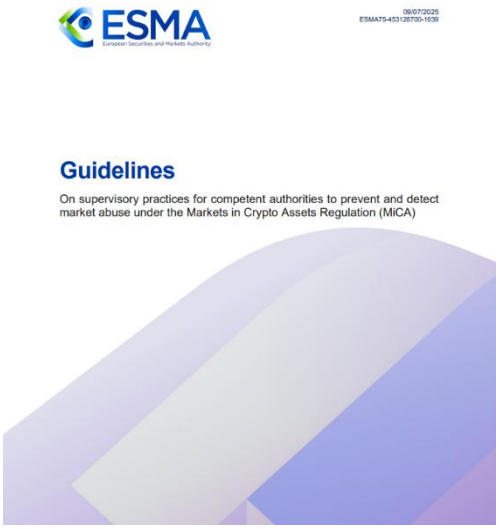
Очікується, що ці керівні принципи призведуть до обмежених витрат для CASP та національних компетентних органів, але принесуть значні переваги. Основні витрати для CASP пов'язані з одноразовими витратами на впровадження організаційних заходів та навчання персоналу, а також поточними витратами на CPD. Для компетентних органів це будуть обмежені поточні витрати на імплементацію та нагляд. Переваги для CASP включають підвищення якості послуг, зниження ризику неправомірного продажу, зростання довіри інвесторів та підвищення ефективності. Клієнти отримають вигоду від підвищеної якості інформації та консультацій,

Висновки:

- **Обов'язкова кваліфікація персоналу:** CASP повинні забезпечити, щоб їхній персонал, який надає інформацію або консультації щодо криптоактивів, відповідав встановленим ESMA мінімальним стандартам знань і компетентності, що включає обов'язкові години професійної кваліфікації (наприклад, 80 годин для надання інформації та 160 годин для надання консультацій) та регулярний безперервний професійний розвиток з обов'язковою перевіркою знань.
- **Диференційований підхід до компетентності:** CASP повинні застосовувати вищі стандарти знань та компетентності для персоналу, який надає консультації, ніж для того, що надає лише інформацію, враховуючи складність послуг та потенційні ризики для інвесторів; при цьому необхідно щорічно переглядати та оновлювати політики та процедури для забезпечення відповідності цим вимогам.
- **Пріоритет захисту інвесторів та прозорість:** З огляду на високу волатильність криптоактивів та обмежений захист інвесторів порівняно з традиційними фінансовими ринками, CASP зобов'язані забезпечити, щоб персонал надавав клієнтам точну, повну та зрозумілу інформацію про ризики, характеристики та витрати, а також вести відповідну документацію для перевірки компетентними органами.

посиленого захисту інвесторів та зменшення ризику шкоди. ESMA вважає, що переваги від цих керівних принципів переважать пов'язані з ними витрати.

Керівні принципи щодо наглядової практики для компетентних органів для запобігання та виявлення зловживань на ринку криптоактивів [2]



Документ Європейського управління з цінних паперів та ринків (ESMA), стосується наглядових практик для компетентних органів з метою запобігання та виявлення зловживань на ринку криптоактивів відповідно до MiCA. Ці настанови, які застосовуються до компетентних органів , мають на меті забезпечити послідовність наглядових практик для запобігання та виявлення інсайдерської торгівлі, незаконного розголошення інсайдерської інформації та маніпулювання ринком, а також забезпечити єдине, послідовне та ефективне застосування Розділу VI MiCA (статті 86-92).

Керівні принципи ESMA закликають компетентні органи застосовувати пропорційний і ризик-орієнтований підхід до нагляду за ринком криптоактивів. Це означає, що вони повинні адаптувати свої дії залежно від релевантності ризиків, які становлять послуги та діяльність підконтрольних установ. Вони повинні розуміти ризики, що створюються постачальниками послуг з криптоактивів (CASP), емітентами, а також трейдерами, майнерами, валідаторами або особами, активними в соціальних мережах, дії яких можуть призвести до зловживань на ринку, таких як маніпуляції з ордерами або поширення оманливої інформації. Компетентні органи також повинні бути уважними до нових форм зловживань через швидку еволюцію ринків криптоактивів і діяти завчасно, враховуючи потенційні ризики.

Керівні принципи також наголошують на інтеграції нових заходів у існуючі практики. Органи повинні оцінювати, наскільки практики, що використовуються для традиційних фінансових інструментів, можуть застосовуватися до криптоактивів, і адаптувати їх. Важливо моніторити практики, специфічні для технології криптоактивів (наприклад, маніпулятивні стратегії MEV). Окремо виділено необхідність моніторингу соціальних мереж , оскільки вони несуть вищий ризик поширення оманливої інформації, ніж традиційні ринки. Такий моніторинг повинен бути заснованим на даних і включати публічно доступну інформацію, регуляторні дані про транзакції, а також, наскільки це можливо, звірки ончейн та офчейн даних. У рамках моніторингу соціальних мереж компетентні органи можуть використовувати автоматизовані інструменти для виявлення закономірностей, ключових слів та тенденцій, доповнені аналізом людини.

Крім того, документ заохочує компетентні органи до формування спільної наглядової культури в ЄС. Вони повинні обмінюватися інформацією щодо ризиків, заходів та найкращих практик для забезпечення цілісності ринку. ESMA закликає до надежного використання ресурсів , що включає наявність спеціалізованого персоналу з необхідними знаннями про криптоактиви та технології , а також належних інструментів для нагляду. Також наголошується на важливості відкритого діалогу зі стейкхолдерами, включаючи експертів та академіків, для кращого розуміння технологічних розробок та нових ризиків. Компетентні органи мають розробляти

[2] https://www.esma.europa.eu/sites/default/files/2025-07/ESMA75-453128700-1039_Guidelines_on_supervisory_practices_to_prevent_and_detect_market_abuse_MiCA_.pdf

освітні ініціативи для підвищення обізнаності учасників ринку про зловживання, використовуючи різні канали, такі як веб-сайти, блоги, подкасти та тренінги.

У документі також описано, що компетентні органи повинні наглядати за системами та процедурами PPAETs (осіб, які професійно організовують або здійснюють операції) , а також реагувати на отримані повідомлення про підозрілі операції, використовуючи чіткі, пропорційні процедури. Важливою є координація ESMA у транскордонних випадках. Компетентні органи повинні також інформувати ESMA та інші відповідні органи про перешкоди, створені третіми країнами, які можуть заважати ефективному нагляду, наприклад, коли CASP направляє значну кількість транзакцій на платформи за межами ЄС.

Висновки:

- **Компетентні органи повинні застосовувати ризик-орієнтований підхід**, що виходить за рамки традиційних фінансових ринків, і адаптувати свої наглядові практики, враховуючи технологічні особливості криптоактивів та нові форми зловживань на ринку, такі як стратегії MEV.
- Для ефективного запобігання та виявлення зловживань на ринку криптоактивів необхідно **активно моніторити різні комунікаційні канали**, включаючи соціальні мережі, блоги та подкасти, використовуючи як автоматизовані, так і людські аналітичні інструменти.
- **Важливою є взаємодія та обмін інформацією** між компетентними органами в ЄС та з іншими стейкхолдерами для створення спільної наглядової культури, а також для виявлення нових ризиків та розробки ефективних рішень.
- **Компетентні органи повинні мати адекватні ресурси**, включаючи спеціалізований персонал з відповідними знаннями та інструменти для моніторингу, а також активно співпрацювати з іншими органами для подолання транскордонних перешкод, що ускладнюють ефективний нагляд.

Пріоритетні напрями досліджень у сфері економічної злочинності [3]

Документ є стратегічним орієнтиром, розробленим Національним центром з питань економічної злочинності (NECC) у співпраці з Міністерством внутрішніх справ Великої Британії, що визначає пріоритетні напрями наукових досліджень у сфері економічної злочинності на найближчі три роки. Він охоплює ключові сфери, де існують суттєві прогалини в доказовій базі, та закликає академічну спільноту, дослідницькі організації та донорів зосередити свої ресурси на цих напрямках для формування більш ефективної політики та практики правоохоронних органів. Основний акцент зроблено на трьох головних категоріях злочинів — відмиванні коштів, шахрайстві та корупції, які розглядаються як серйозні загрози національній безпеці, економічному зростанню та міжнародній репутації країни.

Документ структурований за десятьма тематичними напрямами досліджень: розуміння загроз (включаючи оцінку масштабів, вразливостей, профілю правопорушників і наслідків), заходи

[3] https://www.nationalcrimeagency.gov.uk/who-we-are/publications/755-economic-crime-areas-of-research-interest-ari-report-july-2025/file

протидії (попередження, правозастосування, оцінка ефективності втручань) та міжгалузеві теми (технології, методи дослідження, горизонтальне сканування). Для кожного напряму подано узагальнений опис поточних знань і прогалин, а також перелік конкретних запитань, відповіді на які допоможуть підвищити ефективність протидії економічній злочинності.

У частині оцінки масштабів злочинів наголошується на складності точного вимірювання через латентність, міжнародний характер та недостатню звітність, особливо у відмиванні коштів і корупції. Пропонуються дослідження, які б визначили масштаби відмивання коштів з-за кордону, роль окремих секторів, методи трансферу вартості, обсяг використання криптовалют у незаконних операціях, а також вплив міжнародної корупції на внутрішню ситуацію у Великій Британії.

Розділ про вразливості закликає до глибшого вивчення факторів, що полегшують вчинення злочинів, зокрема у неврегульованих секторах, а також у контексті використання нових технологій, включаючи штучний інтелект і віртуальні активи. Аналіз профілю правопорушників передбачає вивчення мотивацій, шляхів залучення, ролі професійних посередників та міжзлочинної взаємодії організованих злочинних груп.

Важливим елементом є дослідження шкоди від економічних злочинів — як фінансової, так і нефінансової, зокрема впливу на вразливі групи населення, бізнес-клімат, економічне зростання та репутацію країни. Пропонується розробка підходів до кількісного вимірювання цих впливів.

У блоці «Our response» визначено пріоритети превентивних заходів, серед яких — ефективні заходи для секторів, що підпадають під регулювання з ПВК/ФТ, етичні стандарти, поведінкові інсайти та зменшення вразливості громадян і бізнесу. У сфері правозастосування акцент зроблено на інноваційних методах виявлення та конфіскації активів, підвищенні якості звітності про корупцію, міжнародній співпраці та усуненні бар'єрів для ефективного переслідування злочинців. Окремо наголошується на необхідності системної оцінки ефективності заходів, включаючи вплив санкцій, відновлення активів та відповідність нормативно-правової бази сучасним викликам.

Перехресні теми підкреслюють необхідність гнучкого реагування на технологічні зміни, виявлення нових каналів відмивання коштів та шахрайства у цифрових середовищах (зокрема в метавсесвіті), удосконалення методологій досліджень та проведення горизонтального сканування для прогнозування майбутніх ризиків.

Висновки:

- Необхідно розширити дослідження масштабів, вразливостей та методів відмивання коштів, шахрайства і корупції з особливим акцентом на міжнародний вимір та нові технології (включаючи криптовалюти й ШІ).
- Слід розробити уніфіковані підходи до кількісного вимірювання шкоди від економічних злочинів, щоб забезпечити більш точне оцінювання їхнього впливу на економіку, суспільство та вразливі групи.
- Потрібно впроваджувати інноваційні методи запобігання та правозастосування, зокрема у сфері конфіскації активів, міжнародної координації та підвищення якості звітності про злочини.
- Варто системно оцінювати ефективність існуючих заходів і адаптувати їх до швидких технологічних змін та еволюції злочинних моделей.

Таким чином, документ є дорожньою картою для синергії держави, науковців та приватного сектору з метою заповнення критичних прогалин у знаннях, підвищення результативності заходів і зміцнення захисту фінансової системи від економічної злочинності.

SARs Reporter Booklet Липень 2025 [4]

Збірка, підготовлена ПФР Великої Британії (UKFIU), є спеціалізованим продуктом, спрямованим на підзвітних суб'єктів які формують звіти про підозрілу діяльність (SARs), таких як фінансові установи, банки, юридичні фірми та інші організації, які відповідно до законодавства Великої Британії зобов'язані повідомляти про підозрілі фінансові операції. Цей документ створений з метою обміну інформацією про використання SARs правоохоронними органами, заохочення найкращих практик серед репортерів, а також надання зворотного зв'язку щодо функціонування системи SARs, що є ключовим елементом боротьби з фінансовими злочинами. Він відображає зобов'язання NCA ділитися перспективами щодо ефективності режиму SARs та підкреслює важливість співпраці між підзвітними суб'єктами, UKFIU та правоохоронними органами для протидії серйозним злочинам, таким як шахрайство, відмивання грошей, торгівля людьми, фінансування тероризму, виявлення сексуальних злочинів, шахрайських схем, вбивць та зниклих осіб.

UKFIU, як національний орган, відповідає за прийом, аналіз і поширення фінансової розвідувальної інформації, отриманої через SARs, які надають критично важливу інформацію, включаючи телефонні номери, адреси, банківські рахунки, деталі компаній, інвестиційну активність та інші активи. Ці дані дозволяють правоохоронним органам ініціювати нові розслідування або підтримувати вже існуючі. Документ містить практичну інформацію для підзвітних суб'єктів, зокрема контактні дані для подання SARs. Особливо наголошується на перевагах використання онлайн-порталу SAR Portal, який значно прискорює обробку звітів порівняно з поштовою відправкою, що не передбачає підтвердження отримання. UKFIU також активно комунікує з громадськістю через соціальні мережі, такі як LinkedIn та X (офіційні акаунти NCA та UKFIU), а також через подкасти, доступні на платформах Spotify, Apple Podcasts, Amazon Music та Audible.

Основна частина видання присвячена анонімізованим кейс-стаді, зібраним на основі звітів правоохоронних органів за жовтень 2024 року, які демонструють практичне застосування SARs у боротьбі з серйозними та організованими злочинами, визначеними у Національній стратегічній оцінці серйозної та організованої злочинності (NSAI). У сфері шахрайства один із прикладів описує випадок, коли підзвітний суб'єкт подав запит DAML SAR через підозри, що бізнес не веде справжньої діяльності, а отримані кошти є результатом шахрайства шляхом перенаправлення коштів через рахунки. UKFIU відхилила запит, швидко передала інформацію до Служби з боротьби з серйозним шахрайством (SFO) та інших правоохоронних органів, що призвело до кримінального розслідування, отримання ордеру на замороження рахунку (AFO) на суму понад £30,000 та повернення коштів жертві в іншій юрисдикції.

В іншому випадку жертва шахрайства з передоплатою повідомила правоохоронний орган про переказ коштів підозрюваному, який вимагав додаткові платежі та погрожував жертві. Завдяки SARs від кількох підзвітних суб'єктів, включаючи прискорену передачу даних UKFIU, правоохоронці виявили додаткові рахунки, спільників та інших жертв, що завершилося арештом і засудженням підозрюваного за кількома шахрайськими статтями. Ще один приклад стосується кількох компаній, пов'язаних із особою, раніше засудженою за відмивання грошей. Підзвітні суб'єкти виявили підозрілу фінансову активність, пов'язану з інвестиційним шахрайством, і подали численні SARs, включаючи DAML SAR для повернення залишку на рахунку (£10,000).

[4] https://www.nationalcrimeagency.gov.uk/who-we-are/publications/758-sars-reporter-booklet-july-2025/file

UKFIU відхилила запит, передала інформацію правоохоронцям, що призвело до арешту головного підозрюваного та виявлення численних жертв.

У сфері відмивання грошей документ наводить приклад підозри на відмивання грошей у сфері торгівлі (TBML), де підзвітний суб'єкт помітив невідповідність між бізнес-моделлю компанії та обсягом отриманих коштів, підозри в шахрайстві з виплатами, зміну власників пов'язаних компаній та низьку якість вебсайту компанії. Підзвітний суб'єкт подав DAML SAR для виплати залишку (£60,000) і виходу з відносин із клієнтом, але UKFIU відхилила запит, а кошти були заморожені для ліквідації компанії. В іншому випадку бізнес, який виявився прикриттям для відмивання грошей, отримував кошти, значно перевищуючі очікуваний оборот, і переказував їх на численні індивідуальні рахунки. UKFIU відхилила DAML SAR, передала інформацію правоохоронцям, які заморозили рахунок на суму £100,000 та вилучили кошти. У ще одному випадку SARs виявили великі перекази з іноземних юрисдикцій на рахунок у Великій Британії з подальшим переведенням за кордон. UKFIU відхилила два пов'язані DAML SARs від різних підзвітних суб'єктів, що дозволило правоохоронцям заморозити рахунки на £150,000 та £280,000, виявити зв'язки з міжнародною організованою злочинною групою (OCG) та продовжити розслідування.

UKFIU відіграє ключову роль у швидкому реагуванні на SARs через відхилення запитів DAML у випадках підозр щодо злочинного походження коштів і прискорену передачу інформації ("fast-tracking") до правоохоронних органів. SARs надають детальну інформацію, яка допомагає виявляти злочинців, жертв і пов'язані злочинні мережі, включаючи міжнародні операції.

Висновки:

- **Подавайте SARs через SAR Portal** для швидшого опрацювання та підвищення ефективності розслідувань, оскільки поштова відправка значно уповільнює процес.
- **Надавайте детальну** інформацію про пов'язаних суб'єктів і підозрілу активність у SARs, щоб прискорити передачу інформації до правоохоронних органів і підвищити шанси на успішне розслідування.
- **Активно співпрацюйте з UKFIU**, надаючи відгуки та використовуючи ресурси, такі як подкасти та журнал "SARs in Action", для покращення якості звітів.
- **Будьте готові до відхилення запитів** DAML у разі підозр щодо злочинного походження коштів, що може призвести до замороження рахунків і подальших розслідувань.

Документ підкреслює важливість детального заповнення SARs, зокрема інформації про пов'язаних суб'єктів, що підвищує ефективність розслідувань. Підзвітним суб'єктам рекомендують використовувати SAR Portal для швидшої обробки звітів та звертатися до додаткових ресурсів, таких як журнал "SARs in Action" і подкасти UKFIU, доступні на сайті NCA та стрімінгових платформах. Документ наголошує на ефективності SARs у поверненні активів жертвам, виявленні міжнародних злочинних мереж і оперативному реагуванні на підозрілу активність, закликаючи репортерів до тісної співпраці з UKFIU для підвищення якості звітності та боротьби зі злочинністю.

Корупційні ризики під час будівництва, реконструкції, капітального ремонту цивільних об'єктів для відновлення України [5]

[5] https://nazk.gov.ua/pdfjs/?file=/wp-content/uploads/Pages/a6/84/a684c9bcc3dd2ba5e6135be3f225c688759f81ac32d035fb14ef47fad29dddbf2744054.pdf

Дослідження, підготовлене Національним агентством з питань запобігання корупції у 2025 році, є комплексним стратегічним аналізом системних корупційних вразливостей у сфері цивільного будівництва, які становлять загрозу для ефективності, прозорості та доброчесності процесів повоєнного відновлення країни. У фокусі дослідження — виявлення практичних проблем нормативного, адміністративного та організаційного характеру, що сприяють зловживанням у сфері будівництва соціальної інфраструктури та використанню публічних коштів.

На тлі широкомасштабних руйнувань, спричинених російською агресією, потреба у відбудові об'єктів критичної та соціальної інфраструктури набуває пріоритетного значення, однак саме ця сфера демонструє найвищу концентрацію корупційних ризиків. У дослідженні наголошено, що ключовим джерелом таких ризиків є відсутність чіткої стратегії відновлення, загальнонаціонального плану та формалізованих процедур відбору і пріоритезації проєктів, що дозволяє суб'єктам владних повноважень зловживати дискреційними повноваженнями при розподілі державного фінансування. Аналіз використання коштів Фонду ліквідації наслідків збройної агресії свідчить про безсистемність фінансування, нецільове використання ресурсів, затягування строків реалізації проєктів, а також включення до фінансування об'єктів, які не мають безпосереднього відношення до ліквідації наслідків агресії. Виявлено, що значна частина коштів фонду витрачалась без урахування затверджених пріоритетів, без належного обґрунтування та за відсутності прозорих критеріїв, а формальна процедура пріоритезації була впроваджена лише після фактичного здійснення розподілу бюджетних ресурсів.

Окрему увагу у звіті приділено ризикам, пов'язаним із застосуванням механізмів «експериментальних проєктів», які реалізуються поза межами загального регулювання та без уніфікованого підходу до оцінки ефективності. Автори вказують на тенденцію підміни повноцінного нормативного врегулювання постійним розширенням дії експериментів, що суперечить їхній тимчасовій природі та створює умови для зловживань. Наявність можливості реалізовувати будівельні ініціативи в обхід прозорих процедур відбору та контролю підриває цілісність державної політики відновлення та посилює суб'єктивність прийняття рішень.

Серед технічних ризиків чітко окреслено слабкість системи контролю за проєктною документацією, відсутність обов'язкової верифікації вартості матеріалів, використання застарілих або неточних цінових орієнтирів при складанні кошторисів. Це сприяє завищенню очікуваної вартості проєктів, зниженню конкуренції та відкриває можливості для змов між замовниками, проєктантами та підрядниками. Недостатній контроль за супутніми послугами — технічним наглядом, інженерним супроводом — призводить до формального підходу до приймання робіт та включення до кошторисів надмірних чи фіктивних витрат. Значну небезпеку становить практика закупівель без використання електронної системи, зокрема укладання прямих договорів без обґрунтованої потреби, що надає замовникам надмірну свободу у виборі постачальників та створює передумови для фаворитизму.

Ще однією системною проблемою визначено обмеження доступу до інформації про тендери, застосування завищених кваліфікаційних вимог, що ускладнює участь нових або доброчесних компаній у закупівлях. Такі бар'єри перешкоджають розвитку ринку, знижують рівень конкуренції та сприяють корупційній концентрації ринку будівельних підрядів. Дослідження також висвітлює ризики, пов'язані з процедурою зміни істотних умов договорів підряду: відсутність єдиних правил зміни цін, складу робіт і строків, відсутність моніторингу ринкової відповідності створюють підґрунтя для маніпуляцій на етапі виконання договорів. Підрядники

можуть ініціювати невмотивоване зростання вартості без відповідної перевірки чи погодження, що призводить до нераціонального використання бюджетних коштів.

Особливу стурбованість викликає відсутність державного архітектурно-будівельного контролю в умовах воєнного стану, що унеможливлює перевірку дотримання проєктних рішень, будівельних норм і стандартів, ставить під сумнів якість виконаних робіт та підвищує ризик самочинного будівництва або неналежного використання міжнародної допомоги. Відсутність електронної інтегрованої системи обліку виконаних робіт і розрахунків сприяє дублюванню платежів, фіктивному включенню ПДВ, штучному пріоритету окремих підрядників, що порушує принципи доброчесності та рівного доступу до фінансування.

Висновки:

- **Відсутність затверджених на рівні закону критеріїв пріоритезації проєктів спричиняє дискреційний розподіл коштів і підвищує ризики корупції.**

  Рекомендація: ухвалити обов'язкові нормативні критерії пріоритетності, засновані на публічних, вимірюваних показниках.

- **Механізм «експериментальних проєктів» використовується поза правовими межами, фактично як спосіб уникнення контролю та законодавчих процедур.**

  Рекомендація: чітко обмежити правовий режим експериментів у часі та змісті, а їхні результати — піддавати обов'язковій оцінці ефективності.

- **Відсутність централізованої електронної системи обліку та контролю оплати робіт дозволяє завищувати обсяги, додавати фіктивні ПДВ і маніпулювати платежами.**

  Рекомендація: впровадити національну систему цифрового обліку виконаних робіт і бюджетних розрахунків із верифікацією даних.

- **Недостатній контроль за змінами до підрядних договорів дозволяє підрядникам необґрунтовано збільшувати вартість проєктів без підтвердження ринкової відповідності.**

  Рекомендація: запровадити обов'язковий аудит змін до істотних умов договорів з використанням даних про середні ринкові ціни та історію реалізованих проєктів.

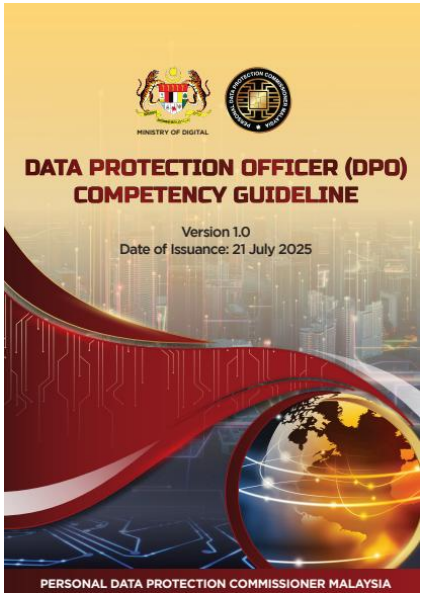
Завершується звіт блоком рекомендацій, які мають на меті системно реформувати підходи до управління відбудовою: впровадити єдиний загальнонаціональний план, нормативно унормувати критерії пріоритезації, удосконалити законодавство щодо закупівель, створити незалежну систему моніторингу змін до договорів, запровадити централізовану електронну систему обліку будівельних робіт і відновити ризик-орієнтований державний контроль. Запропоновані заходи спрямовані на зменшення дискрецій, підвищення прозорості, цифровізацію процесів і повернення довіри до системи відновлення, що є критично важливим для ефективного використання міжнародної фінансової допомоги та національних ресурсів.

Компетентність посадовця із захисту персональних даних: малайзійська модель [6]

Документ, підготовлений Комісаром із захисту персональних даних Малайзії, є офіційним керівництвом, що визначає стандартизований підхід до формування та оцінки професійної компетентності посадовців із захисту персональних даних — DPO. Він спрямований на забезпечення ефективного та цілісного впровадження положень Закону Малайзії про захист

[6] https://www.pdp.gov.my/ppdpv1/en/data-protection-officer-dpo-competency-guideline-2/

персональних даних (PDPA), підвищення рівня професіоналізму в цій сфері, а також створення умов для уніфікованого підходу до підготовки, сертифікації та функціонального навантаження DPO на національному рівні.



У вступній частині документа викладено обґрунтування необхідності його розроблення: зростаюча роль DPO у контексті забезпечення цифрової безпеки, підзвітності та довіри до цифрових послуг вимагає створення чітких орієнтирів щодо знань, навичок і здібностей, якими повинен володіти такий фахівець. Визначається, що існує нагальна потреба у формуванні єдиної професійної рамки для DPO, яка охоплює як технічні, так і управлінські аспекти діяльності. Метою керівництва є надати орієнтири щодо мінімального обсягу знань, практичних навичок та особистісних характеристик, необхідних для ефективного виконання функцій DPO, а також запропонувати систему рівнів професійної підготовки для забезпечення поступового розвитку фахівця — від базового до просунутого рівня.

Основна частина документа присвячена деталізації функцій DPO та визначенню відповідних компетентностей через модель KSA (знання, навички, здібності). Ця модель структурує очікування до DPO за трьома ключовими векторами: знання законодавства, технологій і практик захисту даних (знання); здатність застосовувати ці знання в операційній діяльності, виконанні аналізу ризиків, моніторингу відповідності та комунікації з органами регулювання (навички); а також здатність до стратегічного мислення, лідерства, прийняття етичних рішень та впровадження інституційної культури захисту даних (здібності).

Висновки:

- **Визначено єдину модель компетентності для DPO,** яка структурує очікування щодо знань, навичок та здібностей через модель KSA з двома рівнями (базовий / поглиблений). Це створює підґрунтя для стандартизації професії DPO на національному рівні.
- **Модель дозволяє здійснювати оцінку та розвиток DPO через навчання, сертифікацію та моніторинг виконання функцій,** що може бути використано як на внутрішньому рівні організацій, так і на рівні регуляторного контролю.
- Базовий рівень орієнтований на забезпечення відповідності PDPA, а поглиблений рівень — на управління ризиками, стратегію захисту даних та корпоративну інтеграцію, що робить цю модель релевантною для різних типів організацій (МСП / великі корпорації).
- **Документ може бути використаний як методологічна основа для розробки національних стандартів навчання і сертифікації DPO в інших країнах,** зокрема в Україні, особливо в контексті наближення до GDPR, оскільки модель KSA сумісна з європейською практикою.

Компетенції структуровано за двома рівнями — базовим і поглибленим. Базовий рівень передбачає базове розуміння PDPA, вміння ідентифікувати ризики обробки персональних даних, забезпечувати документальне оформлення політик та процедур, надавати первинні консультації працівникам і здійснювати внутрішній контроль за відповідністю. У цьому контексті DPO діє переважно реактивно, тобто забезпечує відповідність установленим вимогам без глибокої інтеграції в бізнес-процеси. Натомість поглиблений рівень орієнтований на проактивне управління ризиками та впровадження стратегічних

ініціатив у сфері захисту даних. DPO на цьому рівні володіє глибокими знаннями національного й міжнародного законодавства, здатен будувати комплексні програми захисту даних, здійснювати вплив на корпоративне управління, оцінювати ефективність заходів безпеки, аналізувати інциденти й формувати культуру дотримання правил серед персоналу.

Окрему увагу приділено структурі підвищення рівня компетенцій та механізмам оцінки. У документі наголошується, що модель є гнучкою і може бути адаптована до типу організації, її розміру, галузі діяльності та ризик-профілю. Пропонується використовувати керівництво як основу для розробки навчальних програм, розробки посадових інструкцій, проведення внутрішніх аудитів відповідності та оцінки ефективності виконання функцій DPO. Водночас документ має нормативно-дорадчий характер, що дозволяє організаціям інтегрувати його елементи відповідно до своїх конкретних потреб і рівня зрілості системи захисту даних.

Таким чином, дане керівництво виконує функцію структурного стандарту, який спрямований на посилення професійного рівня посадовців із захисту персональних даних у Малайзії та водночас може бути використаний як методологічна база для адаптації подібних підходів в інших юрисдикціях, зокрема тих, що наближають своє законодавство до вимог GDPR. У глобальному контексті документ є прикладом державної політики щодо інституціоналізації функції DPO, що базується на компетентнісному підході, ризик-орієнтованому управлінні та стратегічній інтеграції захисту даних у всі процеси організації.

Регуляторна еволюція: нові технічні стандарти EBA щодо управління операційними збитками [7]

Фінальний звіт Європейського банківського органу (EBA/RTS/2025/03) спрямований на врегулювання технічних аспектів обліку операційного ризику відповідно до оновленого регламенту ЄС № 575/2013 (CRR3). Документ є відповіддю на три окремі регуляторні мандати, які передбачають: по-перше, розробку нової, уніфікованої таксономії ризиків операційного характеру та методології класифікації збитків; по-друге, визначення обставин, за яких обчислення щорічного операційного збитку є надмірно обтяжливим для фінансової установи; і по-третє, встановлення правил коригування набору даних про збитки у разі злиття чи придбання активів або суб'єктів. Запропоновані норми мають на меті гармонізувати підходи до побудови наборів даних про операційні збитки, підвищити якість звітності та забезпечити кращу порівнюваність даних як усередині інституції, так і між різними установами фінансового сектору ЄС.

У рамках першого мандату запропоновано деталізовану таксономію операційного ризику, побудовану за дворівневою структурою: рівень 1 охоплює 7 основних типів подій (наприклад, внутрішнє шахрайство, зовнішнє шахрайство, порушення трудових норм, пошкодження фізичних активів тощо), що відповідає міжнародним стандартам Basel II, а рівень 2 включає 26 категорій, які деталізують характер збитків. Рівні 1 і 2 є взаємовиключними та колективно вичерпними. Унікальною особливістю є впровадження так званих «атрибутів» або «прапорців», які використовуються для подальшого маркування збитків за додатковими характеристиками, такими як наявність ESG-ризиків, участь третіх сторін, пов'язаність з бізнес-лініями, ІКТ-ризиками, юридичними аспектами або процесами неперервності бізнесу. Особливу увагу приділено ESG-факторам, де виділено окремі атрибути для ESG-ризику в цілому та грінвошингу як окремого виду ризику, пов'язаного безпосередньо з діяльністю установи. Це нововведення

[7] https://www.eba.europa.eu/sites/default/files/2025-08/1f9809f8-13bf-4365-aadc-4e7a8cdf89f1/Final%20Report%20on%20RTS%20Operational%20risk%20losses%20mandates.pdf

пов'язане з вимогами CRR3 та регуляторною увагою до впливу кліматичних, соціальних та управлінських факторів на фінансову стабільність. Установи мають не лише ідентифікувати такі фактори в структурі операційного ризику, а й забезпечити надійні процеси управління, моніторингу та звітності.

Крім ESG-факторів, значну частину документа присвячено узгодженню таксономії з вимогами Регламенту DORA (EU) 2022/2554 щодо цифрової операційної стійкості. Документ описує нові атрибути для подій, пов'язаних з ІКТ-ризиками, включаючи кібератаки, з урахуванням необхідності відповідності звітності щодо ІКТ-інцидентів, передбаченої іншими підзаконними актами ЄС. Зокрема, уточнено, що окремі інциденти мають відображатися одночасно через декілька атрибутів, якщо вони стосуються і третіх сторін, і кіберподій, і неперервності бізнесу.

У другій частині документа розглядаються ситуації, за яких обчислення щорічного операційного збитку може вважатися надмірно обтяжливим. Визначено чіткі критерії, за яких установи можуть звертатися до компетентного органу з проханням про звільнення від обчислення: це стосується установ із BI (бізнес-індикатор) між 750 млн і 1 млрд євро у випадках злиття та поглинання, тимчасового перевищення порогу BI або створення перехідних установ у рамках процедури вирішення. Передбачено максимальний строк надання звільнення — до трьох років, а також умови, коли звільнення не допускається (наприклад, якщо обидві сторони злиття вже проводили облік операційних збитків).

У третій частині регламенту конкретизовано, як слід адаптувати набір даних про збитки у разі приєднання нових суб'єктів або активів. Установи мають включати історичні збитки (за останні 10 років) придбаних або злитих організацій у свої дані, з урахуванням курсової переоцінки на момент кожного року звітності. Якщо неможливо миттєво інтегрувати дані у відповідності до нової таксономії, допускається використання проксі-методів з обов'язковим завершенням процесу інтеграції протягом одного року. Якщо джерельні дані не відповідають новій структурі ризиків, установи мають перерозподілити збитки пропорційно до власного внутрішнього розподілу збитків.

Загалом документ представляє комплексне, методологічно обґрунтоване бачення управління операційними ризиками в умовах нової регуляторної архітектури ЄС. Він покликаний сприяти підвищенню прозорості, порівнюваності та надійності даних про операційні збитки, а також враховує сучасні виклики, пов'язані з ESG, кіберризиками та складністю трансакційного середовища. Після громадського обговорення, у якому взяли участь 19 учасників, у фінальний текст були внесені суттєві зміни з урахуванням отриманого зворотного зв'язку. Надалі документ

Висновки:

- **Установи з BI > 750 млн євро зобов'язані збирати й класифікувати дані про операційні збитки за дворівневою таксономією відповідно до міжнародних стандартів.** Це створює основу для уніфікованого підходу в обрахунку капіталу та забезпечує контроль наглядових органів.
- **EBA інтегрує ESG-ризики та ризик грінвошингу в операційну таксономію - установи мають ідентифікувати, коли такі фактори були тригерами збитків.** Це сприяє посиленню ESG-нагляду і зменшенню репутаційних та юридичних ризиків.
- **Можливість отримати звільнення від розрахунку щорічного операційного збитку запроваджується лише для обмежених випадків - M&A, перехідні установи або тимчасове перевищення порогу BI.** Встановлено чіткі часові межі та умови для таких звільнень.
- **У разі злиття або придбання активів, установи мають адаптувати набір даних про збитки за новою таксономією впродовж одного року.** У разі неможливості - дозволено використовувати проксі-методи тимчасово, щоб уникнути заниження капітальних вимог.

буде передано до Європейської Комісії для офіційного затвердження та подальшого розгляду Європарламентом і Радою ЄС.

Санкції

Велика Британія запроваджує перший у світі санкційний режим проти контрабанди людей [8]

У липні 2025 року уряд Великої Британії здійснив безпрецедентний крок у сфері міжнародної безпеки та протидії нелегальній міграції, запровадивши перший у світі санкційний режим, спрямований виключно проти організованої злочинності, що займається контрабандою людей. У межах цього нового режиму, створеного на основі положень Закону про санкції та боротьбу з відмиванням коштів (Sanctions and Anti-Money Laundering Act), були запроваджені санкції проти 25 осіб та організацій, які безпосередньо причетні до формування глобальної інфраструктури нелегального переміщення мігрантів до Великої Британії.

Санкції охоплюють широкий географічний спектр — від постачальників маломірних суден у Китаї до грошових посередників у країнах Близького Сходу, від балканських кримінальних угруповань до ватажків банд у Північній Африці. Серед осіб, проти яких вжито заходи, — організатори перевезень через Ла-Манш, зокрема лідер бельгійського крила албанської контрабандної мережі Бледар Лала, а також колишній поліцейський перекладач із Сербії Ален Басіл, який очолював одну з найбільш жорстоких мереж у регіоні. Також під санкції потрапив Мохаммед Тетвані — самопроголошений «Король Хоргоша», який керував табором біженців на сербському кордоні, де мігрантів катували й утримували в заручниках.

Окрему увагу приділено ролі хавала-банкінгу — неформальних систем переказу грошей, які використовуються для розрахунків між мігрантами та контрабандистами. У списку фігурують ключові фігури, які забезпечували фінансову інфраструктуру цих схем, контролюючи платежі з Іраку до Туреччини, а звідти — до Європи.

Санкції також поширюються на компанії, зокрема на китайську Weihai Yamar Outdoors Product, яка рекламувала на онлайн-платформах човни, спеціально пристосовані для перевезення мігрантів. Ці човни використовувались для небезпечних переправ через Ла-Манш, де регулярно гинуть люди.

Новий режим передбачає заморожування активів осіб та компаній, заборону на надання їм фінансових або матеріальних ресурсів, а також заборону на в'їзд до Великої Британії. Крім того, певні санкції можуть включати заборону на участь у керівництві чи заснуванні компаній на території країни. Санкції мають глобальний характер і поширюються не лише на резидентів Великої Британії, а й на всіх громадян країни незалежно від місця їхнього перебування.

Ці заходи є частиною ширшої урядової стратегії «Disrupt, Deter, Return» — тобто зірвати злочинну діяльність, стримати нелегальну міграцію та повернути на батьківщину тих, хто не має законних підстав залишатися у Великій Британії. У рамках реалізації цієї стратегії за останній рік було повернуто понад 35 000 осіб, що на 13% більше, ніж у попередньому аналогічному періоді.

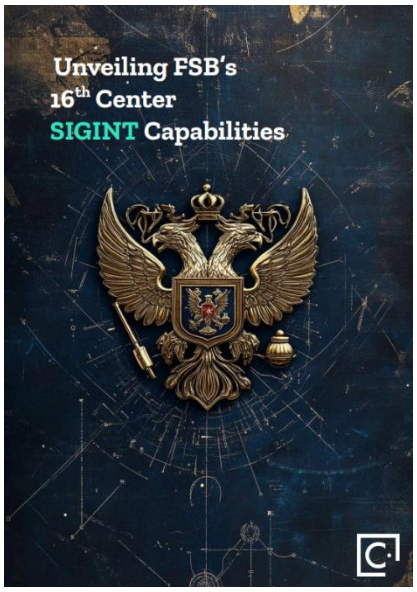
Загалом, запровадження цього санкційного режиму демонструє нову якість зовнішньої політики Великої Британії, що орієнтована на інноваційні механізми протидії транснаціональній

[8] https://www.gov.uk/government/news/uk-sanctions-notorious-people-smuggling-gangs-and-their-enablers-in-global-crackdown

злочинності, у тому числі через інструменти економічного та юридичного тиску. Уряд чітко сигналізує: всі ті, хто збагачується на стражданнях вразливих людей, будуть ідентифіковані та притягнуті до відповідальності, незалежно від країни, де вони перебувають чи здійснюють свою діяльність.

Звіти окремих інституцій та експертів

Розвідка через емблеми: як OSINT дозволив побачити невидиме [9]



Документ, підготовлений аналітичним центром CheckFirst у липні 2025 року, є ґрунтовним дослідженням структури, історії та функціонування одного з найзасекреченіших підрозділів ФСБ росії — 16-го Центру радіоелектронної розвідки. Упродовж року дослідницька команда здійснювала глибокий фалеристичний та OSINT-аналіз понад 200 одиниць військової символіки (знаків, емблем, медалей), пов'язаних із підрозділом, що дозволило відтворити значний обсяг раніше недоступної для громадськості інформації. Основу підходу склала ідея використання фалеристики як інструменту розвідки з відкритих джерел — через детальний аналіз графічних і текстових елементів на знаках: назв, абревіатур, картографічних об'єктів, символів, дат, архітектурних зображень та виробників. Ці дані були систематизовані за допомогою програмного забезпечення digiKam, що дозволило встановити структуру підрозділу, простежити його еволюцію, здійснити географічну прив'язку об'єктів і дати оцінку чисельності персоналу.

16-й Центр ФСБ формально виник у 2003 році в результаті розформування ФАПСІ (Федеральне агентство урядового зв'язку та інформації при Президентові рф), однак розглядається як прямий спадкоємець КДБ — зокрема, 16-ого Управління (відповідального за електронну розвідку, радіоперехоплення та криптоаналіз), утвореного ще у 1973 році. Центр, також відомий під умовною назвою «в/ч 71330», успадкував радянську систему перехоплення сигналів та криптоаналізу, доповнивши її новими функціями — зокрема, проведенням комп'ютерних мережевих операцій (CNO). Автори дослідження виявили щонайменше десять основних департаментів у структурі Центру: A, B, V, D, K, P, S, SP (спеціальні програми), ST і T, що підтверджується як через символіку, так і датування емблем. Деякі з департаментів функціонують ще з 1990-х або навіть радянських часів, і мають внутрішні підрозділи (наприклад, підрозділ №9 у департаменті T). Кожен з них виконує окремі функції: від захисту власних комунікацій до криптоаналітичної діяльності, технічної підтримки та операцій у кіберпросторі. Візуальні елементи емблем, зокрема символіка антени, блискавки, ключа та глобуса, чітко вказують на напрямки діяльності — SIGINT, криптоаналіз, супутниковий моніторинг та мережеві атаки.

Ключовим компонентом дослідження стало встановлення географічного розміщення десяти активних об'єктів системи перехоплення інформації, що підпорядковуються 16-му Центру. Це так звані «Центри спеціального зв'язку» (ЦСС), що також фігурують у російській літературі як «Центри прийому інформації». Автори детально проаналізували емблеми кожного з підрозділів, супутникові знімки та відкриті дані, що дозволило з високою точністю встановити координати об'єктів: від Адлера біля грузинського кордону до Калінінградської області, від

[9] https://checkfirst.network/wp-content/uploads/2025/07/OSINT_Phaleristics_Unveiling_FSB_16th_Center_SIGINT_Capabilities.pdf

Пскова до Владивостока. Усі станції оснащені антенами різного типу (CDAA, MBTA, параболічні тарілки) та призначені для перехоплення супутникових, високочастотних і радіочастотних сигналів. Частина об'єктів була побудована ще у 1940-х–1950-х роках і досі модернізується. Символи на емблемах часто містять натяки на конкретні локації, елементи архітектури об'єктів, а також згадки про радянських попередників, включно з НКВС та КДБ. Зібрані дані дозволяють дійти висновку, що ці центри працюють у комплексі та охоплюють перехоплення комунікацій по периметру державного кордону рф, а також з високою ймовірністю займаються розшифруванням перехоплених зашифрованих повідомлень.

Підсумком дослідження стала побудова цілісної картини щодо структури, функцій і просторової присутності 16-го Центру ФСБ. Автори доводять, що фалеристика — попри її зовнішню поверховість — є надзвичайно ефективним джерелом розвідки щодо навіть найбільш секретних військових і розвідувальних структур. Методика, застосована в дослідженні, може бути екстрапольована на вивчення інших силових структур рф і навіть інших держав. Автори визнають, що інформація, зафіксована на емблемах, завжди є результатом навмисної саморепрезентації структури й тому повинна інтерпретуватися обережно. Проте, у поєднанні з іншими OSINT-методами, вона дає змогу заповнювати суттєві прогалини в розумінні архітектури спецслужб рф і їхньої матеріальної інфраструктури.

Висновки:

- **Вперше ідентифіковано структуру 16-го Центру ФСБ як розгалужену організацію, що включає щонайменше 10 департаментів (A, B, V, D, K, P, S, SP, ST, T) та кілька підрозділів.** На основі аналізу емблем і фалеристичних даних встановлено наявність внутрішньої організації Центру, яка раніше не була відома з відкритих джерел. Це дозволило оцінити чисельність персоналу щонайменше у 566 осіб.
- **Геолокація 10 активних SIGINT-об'єктів (ЦСС) по всій території рф, які, імовірно, підпорядковуються 16-му Центру.** Ідентифіковані об'єкти оснащені системами типу CDAA, MBTA, SATCOM-антенами та працюють на перехоплення супутникових, радіо- та високочастотних сигналів. Об'єкти охоплюють географію від Калінінграда до Далекого Сходу.
- **Підтверджено спадковість 16-го Центру від КДБ та ФАПСІ, з чітким збереженням символіки, умовних номерів і функціонального профілю (SIGINT, криптоаналіз, CNO).** Деякі підрозділи Центру вважають своєю датою заснування ще радянські або навіть дореволюційні роки (1918, 1921), що свідчить про безперервність традицій і функцій в межах російських спецслужб.
- **Фалеристика доведена як валідний OSINT-інструмент для дослідження закритих структур, з можливістю достовірної атрибуції, картографування та аналізу функціональної спеціалізації.** Аналіз понад 200 емблем дозволив реконструювати організаційну структуру, історичну спадковість, функції та навіть розміщення об'єктів, використовуючи відкриті джерела.

Колумбія: Земля можливостей і небезпек [10]

Документ, опублікований InSight Crime, пропонує глибокий аналіз феномену міграції еквадорських кримінальних лідерів до Колумбії, висвітлюючи подвійну природу цієї країни як привабливого притулку та небезпечної пастки для злочинців. Колумбія приваблює лідерів еквадорських банд, таких як Choneros, Águilas і Lobos, можливостями для уникнення

[10] https://insightcrime.org/news/colombia-land-opportunity-danger-ecuadors-crime-bosses/

переслідувань і насильства на батьківщині, а також шансом розширити свої злочинні операції через доступ до потужних колумбійських мереж наркоторгівлі. Водночас документ підкреслює значні ризики, пов'язані з арештами та атаками, які роблять Колумбію небезпечною територією для цих осіб.

Основна причина міграції еквадорських злочинців до Колумбії полягає в ескалації насильства в Еквадорі, спричиненій як конфліктами банд, так і масштабними операціями поліції та армії, спрямованими на ліквідацію кримінальних лідерів. Наприклад, у квітні 2025 року підполковник Ернан Гусман, начальник поліції району Нуева Просперіна в Гуаякілі, зазначив, що лідери банд, такі як Гало Ксав'єр Суарес Роміс, відомий як «Віча», не можуть вільно пересуватися в Еквадорі через постійну загрозу арешту чи загибелі. Ця ситуація змушує їх шукати безпечнішого місця за кордоном. Колумбія, завдяки своїй географічній і культурній близькості до Еквадору, стає природним вибором, адже значна кількість еквадорців живе або відвідує цю країну, що дозволяє злочинцям легко інтегруватися та залишатися непоміченими серед співвітчизників. Крім того, нижча вартість життя в Колумбії порівняно з Еквадором дає змогу кримінальним лідерам вести розкішніший спосіб життя, що є додатковим стимулом для переїзду. Однак ключовою привабливістю Колумбії є її статус світового центру виробництва кокаїну, що відкриває можливості для еквадорських злочинців налагодити прямі зв'язки з постачальниками наркотиків, минаючи посередників, і таким чином посилити свої позиції в глобальній наркоторгівлі.

Документ наводить конкретні приклади діяльності еквадорських злочинців у Колумбії, які ілюструють як їхні успіхи, так і невдачі. Вашингтон Прадо Альва, відомий як «Джеральд» або «Еквадорський Пабло Ескобар», є прикладом успішного злочинця, який у 2017 році був заарештований у колумбійському департаменті Наріньйо, розташованому на кордоні з Еквадором. Джеральд створив одну з найприбутковіших мереж наркоторгівлі, транспортуючи щонайменше 250 тонн кокаїну та заробляючи сотні мільйонів доларів завдяки прямим зв'язкам із колумбійськими постачальниками.

Його успіх демонструє, як Колумбія може слугувати платформою для амбітних еквадорських злочинців, які прагнуть піднятися в ієрархії наркоторгівлі. Інший приклад — Хорхе Луїс Замбрі, відомий як «Раскіта», який відіграв ключову роль у піднесенні банди Choneros у тюремній системі Еквадору. Його заарештували в Колумбії в 2013 році після втечі з еквадорської в'язниці суворого режиму, що підкреслює Колумбію як місце, куди злочинці тікають, щоб уникнути правосуддя.

Хуніор Ролдан, відомий як «JR», лідер банди Águilas і близький союзник лідера Choneros Хосе Адольфо Масіаса Вільямара («Фіто»), був знайдений мертвим у травні 2023 року в сільській місцевості департаменту Антіокія, хоча чутки про інсценування його смерті додають загадковості цій історії.

Колумбія пропонує еквадорським злочинцям значні можливості, зокрема доступ до прямих джерел кокаїну, що дозволяє їм вийти на вищий рівень у ланцюгу наркоторгівлі. Успіх Джеральда є яскравим прикладом того, як прямі зв'язки з колумбійськими постачальниками можуть принести величезні прибутки та вплив. Однак Колумбія також становить серйозні небезпеки.

Луїс Фернандо Кіхано, колумбійський експерт з організованої злочинності, зазначає, що атаки на еквадорських лідерів у Колумбії часто організовуються їхніми суперниками з Еквадору через союзників у Колумбії, що робить ризик для них у цій країні не меншим, ніж удома. Крім того, присутність еквадорських злочинців загрожує усталеним колумбійським мережам наркоторгівлі, які накопичили значну владу та багатство завдяки історичному контролю над експортом кокаїну. Ця конкуренція може провокувати насильство проти еквадорців, які намагаються зайняти вищі позиції в кримінальному світі. Підполковник Сантьяго Гавіланес, начальник поліції Дурана, підкреслює, що колумбійські наркоторговці не розглядають еквадорських злочинців як рівних партнерів, а лише як другорядних гравців, що ускладнює їхню інтеграцію в місцеві кримінальні структури та робить їх вразливими до атак.

Висновки:

- **Посилення транскордонної співпраці правоохоронних органів:** Еквадору та Колумбії необхідно активізувати спільні операції та обмін розвідданими, особливо в прикордонних регіонах, таких як Наріньйо, щоб запобігти втечі кримінальних лідерів і їхній інтеграції в колумбійські мережі.
- **Розрив зв'язків із постачальниками кокаїну:** Колумбійській владі слід зосередити зусилля на виявленні та блокуванні прямих контактів між еквадорськими злочинцями та місцевими постачальниками наркотиків, щоб обмежити їхній вплив у наркоторгівлі.
- **Запобігання транскордонному насильству:** Необхідно розробити стратегії моніторингу діяльності еквадорських банд у Колумбії, щоб попереджати атаки, які організовуються через альянси між бандами двох країн.
- **Контроль прикордонних потоків:** Посилення прикордонного контролю та моніторингу міграційних потоків між Еквадором і Колумбією допоможе ускладнити непомітне пересування злочинців і їхню інтеграцію в місцеве суспільство.

Еквадорські банди, такі як Choneros і Lobos, зазвичай виконують другорядні ролі в глобальній наркоторгівлі, займаючись транспортуванням та зберіганням товару для колумбійських, мексиканських та європейських мереж. Проте окремі лідери, такі як Джеральд, прагнуть вийти на вищий рівень, що робить Колумбію ключовою ареною для реалізації їхніх амбіцій. Водночас присутність еквадорських злочинців у Колумбії може дестабілізувати місцеві кримінальні мережі, що призводить до додаткових конфліктів і насильства. Документ підкреслює, що Колумбія є одночасно «землею можливостей» і «цвинтарем» для еквадорських злочинців, де їхні амбіції стикаються з реальними загрозами арештів, атак і конкуренції.

Шахрайські центри М'янми: прикордонні притулки сучасного рабства [11]

Розслідування, опубліковане Nikkei Asia, розкриває масштабну кризу шахрайських центрів у східній М'янмі, зосереджених переважно в прикордонному районі М'явадді, штат Каян, та вздовж кордону з Таїландом. Ці центри, які часто називають «в'язницями» через їхні жорсткі умови, є осередками організованої злочинності, де тисячі людей, зокрема іноземні громадяни, примусово залучаються до шахрайської діяльності, такої як онлайн-шахрайство та афери. Використовуючи комбінацію супутникових знімків,

[11] https://asia.nikkei.com/static/vdata/infographics/myanmar-scam-centers/

свідчень очевидців, інтерв'ю з експертами, даних про переміщення мобільних пристроїв і відкритих джерел, Nikkei Asia детально описує масштаби, стійкість і характерні риси цих кримінальних осередків, які продовжують процвітати, попри спроби влади їх придушити.

Криза шахрайських центрів у М'янмі набула загрозливих масштабів. Навіть після масштабної операції з придушення в лютому 2025 року, будівництво нових комплексів не припиняється, що свідчить про неспроможність місцевих і міжнародних зусиль повністю ліквідувати ці кримінальні хаби. Nikkei ідентифікувала щонайменше 16 підозрілих об'єктів, вісім із яких перебувають у процесі активного будівництва. Ці центри мають глибоке коріння: у другій половині 2010-х років китайські компанії почали розвивати в регіоні казино-комплекси, які після економічного спаду, спричиненого пандемією COVID-19, були перепрофільовані в осередки онлайн-шахрайства. Ця трансформація дозволила злочинним групам адаптувати інфраструктуру для нових видів злочинів, таких як романтичні афери, де жертв обманом змушують переказувати гроші, вірячи в фіктивні романтичні стосунки.

Умови в цих центрах є надзвичайно суворими і нагадують сучасне рабство. Свідчення чоловіка з Південної Азії, який провів шість місяців у комплексі KK Park — одному з найбільших шахрайських центрів, — ілюструють жахливі реалії. Його змушували працювати 16 годин на день у тісній кімнаті разом із сімома іншими людьми, займаючись шахрайськими схемами. Насильство є повсякденною практикою: чоловік розповів, як його били чоботом, а іншого працівника катували в спеціальній «кімнаті тортур» до такої міри, що той не міг стояти. Працівники, які не виконують поставлені завдання, зазнають електрошоку та інших форм фізичних покарань. За оцінками ООН, у 2023 році шахрайські центри в Східній і Південно-Східній Азії завдали збитків на суму до 37 мільярдів доларів, що перевищує доходи наркосиндикатів, роблячи ці операції одними з найприбутковіших у світі організованої злочинності.

Розслідування виділяє три ключові риси, спільні для всіх шахрайських центрів. По-перше, їхнє планування розроблене для максимального контролю над працівниками. Комплекси оточені високими парканами, стінами та вишками спостереження, а камери безпеки спрямовані всередину, щоб стежити за тими, хто перебуває в середині. Супутникові знімки та відеоматеріали, зокрема з китайської платформи Douyin, підтверджують наявність таких елементів, як високі стіни та укріплені ворота.

По-друге, ці центри мають величезні масштаби, що дозволяє розміщувати велику кількість людей. Комплекси складаються з десятків будівель, деякі з яких сягають чотирьох поверхів, що є унікальним для регіону.

По-третє, більшість центрів розташовані вздовж річок, що полегшує логістику, зокрема контрабанду чи переміщення людей і ресурсів. Наприклад, Nikkei геолокалізували відео, які показують внутрішню інфраструктуру таких комплексів, включаючи баскетбольні майданчики, ресторани та навіть будівлю, позначену як «лікарня» китайською мовою. Як зазначив Бо з EOS Collective, ці місця створені як закриті громади, де люди не мають права вільно пересуватися.

Торгівля людьми є ключовим елементом функціонування цих центрів. Велика кількість іноземних громадян, зокрема з Японії та країн Південної Азії, потрапляє до М'янми через обман або примус. У лютому 2025 року японського старшокласника, якого, ймовірно, утримували в полоні, вдалося врятувати, але згодом його заарештували за шахрайство. З жовтня 2023 року по червень 2025 року влада М'янми депортувала понад 60 000 іноземців, які незаконно перебували в країні та брали участь у шахрайстві чи азартних іграх. У Камбоджі, в місті Пойпет, місцева влада затримала японських громадян, підозрюваних у зв'язках із «анонімними» злочинними групами (Tokuryu), які формуються через соціальні мережі. Ці групи є особливо складними для відстеження через їхню гнучку та децентралізовану структуру.

Деякі шахрайські центри, такі як Yatai New City, Apolo Park і Yulong Bay Park, пов'язані з конкретними компаніями, які, ймовірно, мають зв'язки з місцевими озброєними групами, зокрема Прикордонною гвардією (BGF). Документи з бази даних Управління інвестицій та компаній М'янми (DICA) підтверджують ці зв'язки, хоча після військового перевороту доступ до таких даних став обмеженим. Дані про переміщення мобільних пристроїв, надані французькою компанією nPerF, показують, що особи, задіяні в шахрайських операціях, переміщалися між різними центрами, такими як KK Park і Huanya Park, що вказує на скоординовану мережу.

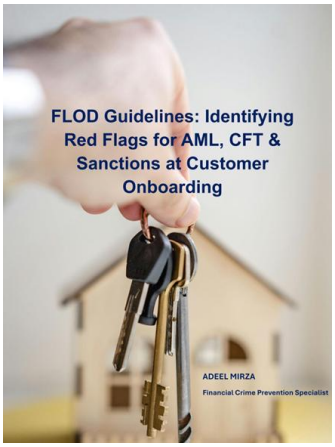
Розслідування показало, що лише один із комплексів припинив діяльність після лютневого придушення, тоді як решта продовжують працювати у звичному режимі. Генерал-лейтенант поліції Трайронг Фівфан із Бюро розслідувань кіберзлочинів підкреслив, що шахрайські групи швидко адаптуються, змінюючи схеми та місця діяльності, що ускладнює боротьбу з ними. Він наголосив на необхідності посилення міжнародної співпраці для ефективного протистояння. Іван Франчесчіні, викладач Університету Мельбурна, охарактеризував ці центри як приклад «сучасного рабства», де багато працівників змушені працювати проти своєї волі, хоча деякі беруть участь у шахрайстві добровільно.

Висновки:

- **Посилення міжнародної співпраці:** Необхідно створити міжнародну коаліцію для обміну розвідданими, проведення спільних операцій і запровадження санкцій проти компаній та озброєних груп які підтримують шахрайські центри.
- **Таргетовані операції проти торгівлі людьми:** Країни, чиї громадяни стають жертвами, повинні співпрацювати з владою М'янми та сусідніх країн, використовуючи супутникові знімки та дані про переміщення, для виявлення та порятунку жертв торгівлі людьми.
- **Моніторинг прикордонних зон:** Впровадження постійного супутникового моніторингу річкових і прикордонних районів для раннього виявлення нових шахрайських центрів.
- **Профілактичні заходи:** Уряди країн, звідки походять жертви, повинні проводити інформаційні кампанії про ризики шахрайства через соціальні мережі, щоб зменшити кількість людей, які потрапляють до цих центрів через обман.

FLOD у дії: ефективне виявлення ризиків під час залучення клієнтів [12]

Документ є методичним посібником, спрямованим на посилення ефективності першої лінії захисту (FLOD) у фінансових установах шляхом вдосконалення процесу ідентифікації ризиків під час залучення нових клієнтів. Центральною ідеєю документа є те, що саме співробітники, які безпосередньо взаємодіють із клієнтом на початковому етапі — менеджери із залучення, фахівці з відкриття рахунків та обслуговування клієнтів — є першими, хто може виявити потенційні ознаки відмивання коштів, фінансування тероризму або порушення санкційного законодавства. З огляду на це, документ пропонує структурований підхід до виявлення так званих червоних прапорців — які можуть сигналізувати про підвищений ризик.



[12] https://www.linkedin.com/posts/mirzaadeel_flod-guidelines-identifying-red-flags-activity-7357653781414608896-1mM7?utm_source=share&utm_medium=member_ios&rcm=ACoAAENtfVEBPg5yYQyZX6TW5v3XHcJMaoRqA5I

Підхід, викладений у документі, заснований на поєднанні технічних знань, розуміння типологій ВК/ФТ та культури критичного мислення. Персонал FLOD повинен вміти не лише розпізнати типові індикатори ризику, а й усвідомлено аналізувати поведінку клієнта, його документи, бізнес-модель та географічні зв'язки. Документ надає чіткий перелік ключових зон, у яких найчастіше проявляються ознаки потенційного зловживання фінансовими послугами. Серед них — процес ідентифікації та верифікації клієнта (з підробленими або суперечливими документами, небажанням надавати інформацію, використанням номінальних осіб або третіх сторін); джерело коштів та багатства (із неясним або неперевіреним походженням, що не відповідає заявленому доходу); профіль клієнта і характер бізнесу (включаючи випадки використання складних структур власності, відсутність інформації про КБВ або діяльність у високоризикових секторах, як-от криптовалюти або переказ грошових коштів); географічні ризики (зв'язки з юрисдикціями, що мають статус високого ризику за оцінкою FATF або потрапляють під санкції); санкційна перевірка (виявлення прямих або опосередкованих зв'язків із особами чи структурами з санкційних списківч); та очікувана транзакційна поведінка (прохання про високі ліміти, незвична структура транзакцій, орієнтація на готівкові операції, уникнення розкриття інформації).

Окрема увага приділяється переліку конкретних дій, яких повинен вживати персонал FLOD у разі виявлення червоних прапорців. Зокрема, йдеться про обов'язкове документування усіх спостережень у клієнтській справі, ініціювання посиленої перевірки (EDD), вимогу щодо надання додаткових або уточнюючих документів, перевірку клієнта та всіх пов'язаних осіб у санкційних списках, базах PEP та Adverse Media, ескалацію справи до підрозділу комплаєнсу або фінансової розвідки, а також — за потреби — повну зупинку процесу початкового встановлення ділових відносин до отримання чіткого дозволу. Наголошується на важливості зберігання повного сліду усіх дій, рішень та комунікацій, що мають відношення до процесу залучення клієнта.

Особливо цінним елементом посібника є перелік типових сценаріїв, за яких початкове встановлення ділових відносин повинне бути негайно ескальоване, наприклад: позитивні спрацювання на санкційних або PEP-базах; невідповідності в документах; відмова клієнта співпрацювати; використання заплутаних структур без чіткої ділової логіки; зв'язки з країнами, які є джерелом фінансування тероризму, або секторами, що історично пов'язані з ВК/ФТ. Автор також наголошує на критичному значенні безперервного навчання фахівців FLOD — через регулярні тренінги, симуляційні кейси, оновлення знань про нові типології та санкційні режими, а також через забезпечення доступу до сучасних інструментів перевірки.

У підсумку, документ формує цілісну методологічну платформу для

Висновки:

- **FLOD повинна діяти як активна бар'єрна система на етапі залучення клієнта,** виявляючи типові червоні прапорці у шести ключових категоріях ризику. Будь-яка підозріла ознака має бути зафіксована та ескальована до підрозділу комплаєнсу.
- **Жоден процес відкриття рахунку не повинен бути завершений без повної санкційної перевірки, верифікації КБВ та оцінки ризику клієнта.** Якщо дані суперечливі або неузгоджені — початкове встановлення ділових відносин має бути зупинене.
- **Посилена перевірка (EDD) є обов'язковою у випадках зв'язку з юрисдикціями високого ризику, складних корпоративних структур, незрозумілого джерела статків або ознак ухилення від перевірки.**
- **Регулярне навчання персоналу FLOD, доступ до актуальних інструментів перевірки (санкційні та PEP-бази, нові типології) та налагоджені внутрішні канали комунікації —** критично важливі для стійкості системи ПВК/ФТ в установі.

ефективного виявлення та реагування на ознаки фінансових злочинів ще на ранньому етапі клієнтського циклу. Він не лише підтримує виконання нормативних вимог (відповідно до стандартів FATF, директив ЄС і внутрішніх вимог регуляторів), але й сприяє побудові зрілої комплаєнс-культури, яка підвищує стійкість фінансових установ до зовнішніх загроз і захищає їхню репутацію в очах регуляторів, партнерів і суспільства в цілому.

ВНУП

Класифікація ризиків, внутрішні процедури, дерево рішень: як це робиться на практиці? [13] [14] [15]

Представлені документи від Директорату національної розвідки та митних розслідувань Франції (DNRED) слугують практичними посібниками для фахівців, які перебувають під їхнім наглядом, зокрема, торговців витворами мистецтва та антикваріатом, а також торговців дорогоцінним камінням та металами. Ці посібники, хоч і не є вичерпними, пропонують методичний підхід для переходу від теорії до практики у сфері ПВК/ФТ і можуть бути адаптовані іншими фахівцями відповідно до їхнього сектора та специфіки діяльності. Ключовою вимогою для цих професій є обов'язкове створення та формалізація двох основних документів: класифікації ризиків та внутрішньої процедури з ПВК/ФТ.

Класифікація ризиків ПВК/ФТ розроблена для того, щоб дозволити фахівцям зосередити зусилля на моніторингу діяльності клієнтів та постачальників, які представляють найвищі ризики ВК/ФТ. Вона повинна ідентифікувати та оцінювати ризики ВК/ФТ, яким піддається підзвітний суб’єкт. Ідентифікація ризиків включає виявлення ситуацій, що можуть викликати сумніви щодо законності операції, та повинна бути унікальною для кожної професії, враховуючи специфіку її діяльності. Ризики можуть бути пов'язані з відмиванням капіталів (приховування незаконного походження активів, як-от торгівля наркотиками, культурними цінностями, крадіжки, податкове шахрайство), відмиванням майна (приховування незаконного походження об'єктів, як-от викрадені чи розграбовані цінності), а також з обходом цільових фінансових санкцій, наприклад, через торгівлю діамантами. Класифікація ризиків ґрунтується на п'яти регуляторних осях ризику: характер продуктів чи послуг (наприклад, інвестиційне золото без підтвердження походження вважається високим ризиком), умови транзакцій (як-от оплата готівкою або платежі частинами, що підвищують ризик), канали постачання (наприклад, дистанційні продажі або залучення посередників, які ускладнюють ідентифікацію), клієнти (політично значущі особи, складні юридичні структури, такі як трасти, або клієнти з несприятливою публічною репутацією), а також географічні фактори (наприклад, країни з високим ризиком ВК/ФТ, що входять до "сірого" або "чорного" списків FATF, або не співпрацюють з податковими органами). Ідентифікація ризику не означає автоматичну подачу повідомлення про підозрілу діяльність, але вказує на ситуації, що вимагають підвищеної уваги. Для ідентифікації ризиків фахівці можуть використовувати національну оцінку ризиків ВК/ФТ, публікації FATF, галузевий аналіз, звіти ПФР. Оцінка ризиків, визначена як присвоєння рівня ризику кожній ситуації (наприклад, низький, помірний, високий, дуже високий), дозволяє адаптувати заходи пильності. Цей документ має

[13] https://www.douane.gouv.fr/sites/default/files/2025-07/18/Vf-Fiche-pratique-Classification-des-risques-LCB-FT-Juillet-2025.pdf
[14] https://www.douane.gouv.fr/sites/default/files/2025-07/18/Vf-Fiche-pratique-Procedure-interne-LCB-FT-Juillet-2025.pdf
[15] https://www.douane.gouv.fr/sites/default/files/2025-07/18/Vf-Fiche-pratique-arbre-decisionnel-LCB-FT-Juillet-2025.pdf

бути затверджений відповідальним працівником та регулярно оновлюватися, враховуючи регуляторні зміни та актуальні списки країн з високим ризиком. Відповідальність за класифікацію ризиків залишається на керівнику компанії.

Внутрішня процедура з ПВК/ФТ визначає порядок реалізації компанією зобов'язань з ПВК/ФТ. Вона має бути задокументована, доведена до відома відповідних співробітників (комерційного відділу, відділу комплаєнсу та внутрішнього контролю) та бути операційною, адаптованою до діялності компанії, включаючи деталі про доступ до інформації. Ця процедура передбачає призначення відповідального працівника, який повинен мати високу управлінську позицію та достатні знання, а також бути відповідальним за застосування процедур з ПВК/ФТ у компанії. Обов'язковою є регулярне навчання керівників та співробітників, відповідальних за ПВК/ФТ. Навчання повинно виходити за рамки простих пам'яток, а його відвідування має бути підтверджене. Для забезпечення дотримання зобов'язань з ПВК/ФТ необхідно створити систему внутрішнього контролю, що дозволяє виявляти інциденти, вживати коригувальні заходи та інформувати керівні органи. Контроль повинен бути адаптований до розміру та структури компанії, здійснюватися регулярно та, бажано, особою, відмінною від тієї, що проводить комерційні операції.

Обов’язковим є здійснення моніторингу операцій, особливо тих, що дорівнюють або перевищують 10 000 євро, а також відстежувати пов’язані операції, спрямовані на уникнення порогових спрацювань. Важливою є відмінність між клієнтом, з яким започатковано ділові відносини, та разовим клієнтом, оскільки застосовувані зобов'язання з ПВК/ФТ відрізняються. Процедури ідентифікації та верифікації особи клієнта (фізичної або юридичної особи) та кінцевого бенефіціарного власника (КБВ) є ключовими, і вони мають бути визначені в процедурі з ПВК/ФТ. Верифікація КБВ є обов'язковою, і операція не може бути виконана, якщо її неможливо здійснити. Для французьких юридичних осіб використовується Реєстр бенефіціарних власників (RBE) INPI – в Україні діє Єдиний державний реєстр юридичних осіб, фізичних осіб-підприємців та громадських формувань – а для іноземних суб'єктів вимагаються еквівалентні документи. Процедура KYC для ділових відносин передбачає збір інформації про мету та характер відносин, походження та призначення коштів, а також економічне обґрунтування, що дозволяє оцінити профіль ризику відносин. Залежно від рівня ризику, застосовуються різні заходи обачності: спрощені (для низького ризику), постійні (за замовчуванням) або посилені (для політично значущих осіб, високоризикових клієнтів чи клієнтів з

Висновки:

- **Обов'язкова розробка та постійне оновлення системи з ПВК/ФТ:** Кожен фахівець чи компанія мають розробити та формалізувати власну класифікацію ризиків та внутрішню процедуру з ПВК/ФТ, регулярно оновлюючи їх відповідно до змін законодавства та нових ризиків, щоб ефективно фокусувати зусилля на найбільш вразливих зонах.
- **Застосування ризик-орієнтованого підходу з заходами належної обачності:** Необхідно ідентифікувати та оцінювати специфічні ризики для кожного клієнта та операції, використовуючи п'ять регуляторних осей, та адаптувати інтенсивність заходів обачності (від спрощених до посилених) відповідно до визначеного рівня ризику, що дозволяє ефективно розподіляти ресурси та протидіяти ВК/ФТ.
- **Постійний моніторинг та своєчасне повідомлення про підозрілі операції:** Важливо здійснювати постійний моніторинг операцій для виявлення атипових транзакцій; у разі, якщо посилена перевірка не знімає сумнівів щодо законності операції, фахівець зобов'язаний негайно подати обґрунтоване та конфіденційне повідомлення про підозрілу операцію до ПФР.

високоризикових юрисдикцій). Ці заходи можуть включати частоту оновлення даних KYC та вимоги до підтверджуючих документів.

Дерево прийняття рішень з ПВК/ФТ деталізує послідовність дій під час виконання операції. Воно підкреслює обов'язкову перевірку цільових фінансових санкцій щодо кожної операції, незалежно від суми, шляхом перевірки, чи не підпадає клієнт під заходи заморожування активів. Якщо клієнт перебуває під санкціями, операція не повинна виконуватися, а інформація має бути негайно передана до компетентного органу. Для операцій вартістю 10 000 євро і більше процес включає визначення типу комерційних відносин, верифікацію особи клієнта та КБВ, збір даних KYC та оцінку рівня ризику ділових відносин. Під час виконання операції застосовуються заходи належної перевірки клієнта, а операції постійно моніторяться на предмет атипової поведінки (наприклад, невідповідності профілю клієнта, незвичної складності чи суми, відсутності економічного обґрунтування). У випадку виявлення атипової операції проводиться посилена перевірка, яка передбачає додаткові дослідження та збір підтверджуючих документів. Якщо після посиленої перевірки сумніви щодо законності операції залишаються, відповідний фахівець повинен подати повідомлення про підозрілу операцію до ПФР, детально обґрунтувавши свої підозри. Після завершення операції всі зібрані документи та результати досліджень повинні зберігатися протягом 5 років з моменту припинення ділових відносин або останньої операції, а дані KYC та рівні ризику мають підлягати постійному оновленню.

Інші новини

Заява Вольфсберзької Групи щодо ризик-орієнтованого підходу [16]

Документ Вольфсберзької Групи є оновленою та змістовною декларацією, яка підтверджує відданість принципам ризик-орієнтованого підходу (РОП) та закликає як приватний, так і державний сектор відходити від формального виконання вимог на користь досягнення реальних, вимірюваних результатів у сфері протидії фінансовим злочинам. Основна думка полягає в тому, що страх допустити помилку часто змушує регуляторів, правоохоронців та фінансові установи намагатися перестрахуватися — виконувати всі можливі формальні вимоги та перевірки без винятку, навіть якщо це не дає значного ефекту, через що втрачається головний фокус на досягненні реальних результатів. Група наголошує, що пропорційність, пріоритизація та ефективність мають бути ключовими складовими будь-якої програми управління ризиками фінансових злочинів.

Заява підкреслює, що РОП — це не просто набір процедур, а концептуальна основа для побудови та підтримки програм управління ризиками фінансових злочинів, яка охоплює апетит до ризику, політики, заходи та контрольні механізми. Вона визначає РОП у відповідності до стандартів FATF як процес, у межах якого країни, компетентні органи та фінансові установи повинні ідентифікувати, оцінювати та розуміти ризики, а потім уживати пропорційних заходів, які адекватно відповідають рівню виявленого ризику та ефективно його знижують. На думку Групи, застосування РОП є ключовим інструментом для досягнення ефективності та результативності, що є основою її діяльності.

Документ конкретизує три фундаментальні принципи: пропорційність, яка передбачає відповідність програм управління ризиками масштабам, профілю клієнтів, географічному

[16] https://db.wolfsberg-group.org/assets/4f04b8ea-b4d0-4c58-82cd-ec852a2adc43/Wolfsberg_RiskBasedApproach_Statement_July2025%20(2).pdf

охопленню та апетиту до ризику; пріоритизацію, тобто зосередження ресурсів на вищих ризиках і водночас відмову від застарілих або неефективних заходів; та ефективність, що вимагає орієнтації на досягнення реальних результатів, відходу від уніфікованих правил і впровадження гнучких, динамічних рішень.

Група наголошує, що успішне впровадження РОП можливе лише за умови тісної співпраці та діалогу між усіма зацікавленими сторонами — від фінансових установ до регуляторів та правоохоронців. Саме наявність наглядового режиму, який підтримує застосування РОП, є критичним чинником успіху. У цьому контексті Група анонсує оновлення своїх ключових настанов щодо РОП 2006 року та «Risk Assessment FAQs» 2015 року з метою стимулювати ухвалення складних, але необхідних рішень щодо методів для досягнення правильних результатів.

Заява також позиціонує РОП як інтегральну складову інших ініціатив Групи, зокрема тих, що стосуються розробки ефективних програм з ПВК/ФТ, принципів аудиту ефективності, ефективного моніторингу підозрілої діяльності та оцінки ризиків країн. Таким чином, документ є закликом до відмови від підходу «нульових помилок» у комплаєнсі та переходу до більш гнучкої, результативної та ризик-орієнтованої моделі, яка зосереджується на кінцевому ефекті, а не на формальному виконанні вимог.

Як Ісламська держава та інші терористичні угруповання використовують ШІ [17]

У статті The Guardian журналіст Бен Макуч аналізує, як терористичні організації, зокрема Ісламська держава (ІД), активно інтегрують сучасні інструменти штучного інтелекту (ШІ) у свою діяльність, адаптуючи їх для вербування, фінансування, поширення пропаганди, виготовлення зброї та забезпечення оперативної безпеки. Матеріал ґрунтується на даних аналітиків, експертів з протидії тероризму та витоках інформації з урядових структур США.

Протягом останнього десятиліття терористичні угруповання ефективно освоювали цифрові інструменти: соціальні мережі, криптовалюти, зашифровані месенджери та навіть 3D-друк зброї. Сьогодні ж технології ШІ — насамперед генеративні моделі, як-от ChatGPT — відкрили перед ними нові можливості. Автор підкреслює, що ШІ не створює цілком нові загрози, але суттєво посилює і масштабує вже існуючі. Замість революції — еволюція терору в цифровому просторі, яка виводить тактики на новий рівень ефективності.

Зокрема, ІД та суміжні угруповання використовують генеративні ШІ для створення текстів, аудіо- та відеоматеріалів з пропагандою. Наприклад, новинні бюлетені Ісламської держави трансформуються в аудіофайли або серії візуального контенту, який централізовано виробляється та розповсюджується в зашифрованих каналах. У чатах, пов'язаних з ІД, вже обговорюються можливості використання ChatGPT як «цифрового порадника» чи навіть «асистента з досліджень». У тому ж середовищі з'являються і обережні дискусії щодо того, наскільки безпечно ставити запити типу «як зробити вибухівку» та чи стежать спецслужби за такими активностями. Деякі користувачі шукають «безпечні альтернативи», а інші – навчають,

[17] https://www.theguardian.com/world/2025/jul/08/terrorist-groups-artificial-intelligence

як обійти виявлення, наприклад, публікуючи технічні креслення транспортних засобів для атак без згадування небезпечних ключових слів.

Особливо тривожною є публікація ІД під назвою «Guide to AI Tools and Risks», яка циркулює в зашифрованих каналах. У ній прямо вказано на необхідність оволодіння ШІ як «сили, що формує війну», а також описуються способи застосування таких технологій у бойових і пропагандистських цілях. Таким чином, ШІ уже інтегрується у світогляд і стратегію терористичних організацій, а не лише використовується ситуативно.

Цей тренд не обмежується лише джихадистськими групами. Ультраправі та неонацистські об'єднання також активно експериментують із ШІ — для створення дезінформаційних мемів, фейкових зображень Гітлера або графіки для онлайн-пропаганди. Аналітики зазначають, що ШІ-технології сприяють і підвищенню рівня оперативної безпеки (OPSEC): зокрема, використовуються зашифровані голосові модулятори, що дозволяють маскувати голос, і загалом — розробляються нові способи анонімізації діяльності.

У контексті цього цифрового зсуву урядові структури західних країн, за словами експертів, втрачають позиції. Значна частина програм протидії тероризму була скорочена (наприклад, у США внаслідок рішень адміністрації Дональда Трампа), а самі уряди і технологічні платформи стали менше приділяти уваги моніторингу та реагуванню на онлайн-загрози. На цьому тлі експерти (зокрема, організація Tech Against Terrorism, що діє під егідою ООН) наголошують на необхідності активізації зусиль, зокрема оновлення механізмів модерації контенту, посилення співпраці з такими платформами, як Meta чи OpenAI, а також впровадження спільних систем виявлення (наприклад, хеш-банків).

Головний висновок статті — ШІ став ще одним інструментом у руках терористів, який значно підвищує швидкість, масштабованість і маскування їх дій. Але справжньою загрозою є не стільки саме ШІ, як слабкість інституційної спроможності держав і технологічних компаній адекватно протидіяти цим викликам. Терористи не створюють нові сценарії, а підсилюють старі, користуючись нашою неготовністю до гібридної цифрової загрози.

Ваша думка важлива!

1. Які механізми контролю та оцінки знань персоналу CASP є найбільш ефективними для зменшення ризиків ВК/ФТ у сфері криптоактивів, з урахуванням положень MiCA?
2. Які методологічні підходи до вимірювання шкоди від економічних злочинів можуть забезпечити найбільш точні результати для національних оцінок ризиків?
3. Як можна підвищити якість SAR, щоб забезпечити їхню максимальну цінність для правоохоронних органів і прискорити повернення активів?
4. Які заходи може вжити Україна для запобігання використання своїх громадян в шахрайських цілях, враховуючи використання соціальних мереж для вербування жертв?
5. Які потенційні загрози для національної безпеки України становить використання ШІ терористичними або екстремістськими угрупованнями, зокрема в умовах війни?
6. Окрім запровадження єдиного національного плану відбудови та прозорих критеріїв пріоритезації проєктів, які ще шляхи існують для ефективного та доброчесного відновлення України? Яким чином вони можуть бути впроваджені?
7. Як вплине включення грінвошингу як окремого ризику на оцінку репутаційних та юридичних ризиків фінансових установ в Україні, зокрема в умовах зростання уваги до сталого фінансування?

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-2025-32

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].