Методологічний бюлетень

Серійний номер: МінФін-AML-2025-01

Січень 2025

Мета

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

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

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

Звіти міжнародних організацій та окремих юрисдикцій

Шахрайство з ідентифікацією: виклики, наслідки та стратегія протидії у цифрову епоху [1]

Документ є глибоким аналізом проблеми шахрайства з ідентифікацією, яка стає дедалі серйознішою загрозою для економічної та національної безпеки Великої Британії. У ньому розглядається як поточний стан проблеми, так і шляхи її еволюції, а також надаються практичні рекомендації щодо покращення існуючої системи протидії.

Шахрайство з ідентифікацією досягло масштабів епідемії, викликаючи значні економічні втрати та сприяючи іншим формам організованої злочинності, таким як відмивання коштів, фінансування тероризму та ухилення від санкцій. За оцінками, щорічні збитки від такого виду шахрайства у Великій Британії становлять £1.8 мільярда, а його цифровізація суттєво ускладнює боротьбу з ним. Використання сучасних технологій, зокрема штучного інтелекту та технології deepfake, дозволяє злочинцям створювати високоякісні фальшиві документи, що ускладнює їх виявлення навіть сучасними системами.

Документ наголошує, що ключовим викликом є недостатнє розуміння масштабів загрози, особливо у взаємозв'язку з іншими видами злочинної діяльності. Учасники обговорення, на

[1] https://static.rusi.org/identity-fraud-conference-report.pdf

основі якого підготовлено звіт, відзначають, що юридична база не завжди сприяє ефективній боротьбі. Викрадення ідентифікаційної інформації саме по собі не є кримінальним злочином у Великій Британії, а переслідується лише тоді, коли використовується для скоєння інших злочинів. Це знижує пріоритетність таких справ у правоохоронних органах та сприяє недостатньому розслідуванню.

Окрему увагу приділено ролі державного та приватного секторів у боротьбі із шахрайством. Розглядається позитивний досвід операції Amberhill, яка дозволяє ділитися даними між секторами для виявлення фальшивих документів. Однак операція потребує суттєвого оновлення та розширення, включаючи використання цифрових технологій і автоматизації.

Крім того, відзначається низький рівень підтримки жертв шахрайства з ідентифікацією. Переважно, фінансові втрати покривають фінансові установи, але жертви зазнають значного психологічного впливу та адміністративного навантаження, що ігнорується чинною системою. Необхідна розробка урядових програм підтримки, які враховували б ці аспекти.

Документ також підкреслює важливість підвищення довіри до цифрових ідентифікаційних систем. Незважаючи на перспективність, їхнє впровадження у Великій Британії гальмується відсутністю культури використання національних ідентифікаційних систем. Існують ризики, пов'язані з недостатнім регулюванням якості таких послуг, що може перетворити цифрову ідентифікацію на новий вектор шахрайства.

Висновки:

- **Необхідність координації:** Підвищення взаємодії між державним і приватним секторами, включаючи створення реальних інструментів перевірки ідентифікаційних даних, є критично важливо.
- **Масштабування операції Amberhill:** Інвестиції в цю ініціативу дозволять ефективніше ідентифікувати фальшиві документи та зменшити втрати.
- **Підтримка жертв:** Розробка державної програми підтримки з урахуванням психологічних і адміністративних наслідків для жертв.
- **Законодавчі зміни:** Оцінка необхідності криміналізації дій, які сприяють викраденню ідентифікаційних даних, для спрощення роботи правоохоронців.

Звіт завершується низкою практичних рекомендацій, зокрема щодо посилення правового регулювання, покращення обміну даними між секторами, модернізації існуючих ініціатив і забезпечення підтримки жертв. Він закликає до колективного оновлення підходів до боротьби із шахрайством з ідентичністю, що включає дослідження нових загроз, впровадження технологічних рішень та підвищення обізнаності серед усіх зацікавлених сторін.

Нові підходи до належної перевірки активів: Практичні рекомендації від CSSF[2]

Документ є офіційним роз'ясненням щодо вимог до проведення належної перевірки активів у контексті протидії відмиванню коштів (ПВК) та фінансуванням тероризму (ПФТ). Його зміст орієнтований на професіоналів, які працюють у регульованій інвестиційній діяльності, і базується на положеннях статті 34(2) Регламенту CSSF № 12-02, що стосується оцінки ризиків та заходів перевірки активів. Документ має мету надати чіткі практичні рекомендації у форматі запитань і відповідей, зосереджуючись на ризик-орієнтованому підході.

[2] https://www.cssf.lu/wp-content/uploads/FAQ-on-AML-Assets-Due-Diligence.pdf

У контексті застосування вимог документ наголошує на тому, що відповідальність за оцінку ризиків відмивання коштів (ВК) і фінансування тероризму (ФТ), а також за розробку та реалізацію відповідних заходів, лежить на професіоналах. Водночас вказується, що цей документ не охоплює питання міжнародних фінансових санкцій чи специфічних вимог до них. Замість цього акцент робиться на належній перевірці активів у межах ризик-орієнтованого підходу.

Однією з ключових тем є визначення підходу до активів, що торгуються на регульованих ринках. У документі підкреслюється, що такі активи вважаються менш ризиковими через їхню прозорість та ринковий контроль. У цьому контексті CSSF зазначає, що для забезпечення відповідності статті 34(2) достатньо лише підтвердити факт торгівлі активу на регульованому ринку. Це спрощує процес перевірки для професіоналів, зменшуючи адміністративне навантаження.

Висновки:

- **Спрощення перевірки для активів на регульованих ринках:** Належна перевірка активів, які вже перебувають у лістингу регульованих ринків, мінімізується завдяки наявним ринковим механізмам прозорості.
- **Гнучкість для нерегульованих активів:** Повторна оцінка ризиків не є обов'язковою, якщо протягом року відсутні суттєві зміни у стані активу, що дозволяє оптимізувати ресурси.
- **Обов'язок адаптації заходів:** Професіонали зобов'язані підходи залежно від характеру активу, типу операцій та оціненого рівня ризику.
- **Значення документування:** Всі заходи належної перевірки повинні бути відповідно задокументовані, щоб у разі перевірки можна було підтвердити дотримання вимог статті 34(2) Регламенту CSSF № 12-02.

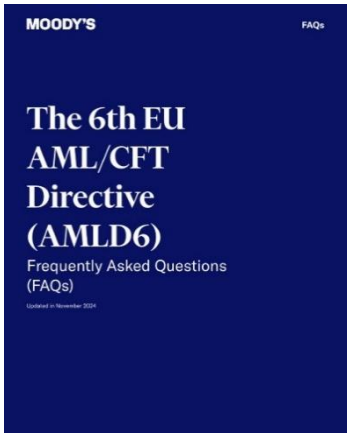
Щодо активів, які не торгуються на регульованих ринках, вказується, що ризик-орієнтована оцінка повинна проводитися ретельніше, залежно від рівня ризику ВК/ФТ. При цьому повторна щорічна оцінка не вимагається, якщо протягом року відсутні суттєві зміни в активі або операціях із ним. Такий підхід забезпечує гнучкість для професіоналів, дозволяючи їм зосереджувати зусилля на активах із вищим ризиком.

Документ також встановлює вимоги щодо належної перевірки активів, які не є об'єктом торгів на регульованих ринках. Вона має здійснюватися у випадках змін у стані активу, що можуть збільшити ризик ВК/ФТ, або під час проведення операцій, які вимагають підвищеної уваги. У таких випадках заходи перевірки мають відповідати рівню ризику та бути відповідно задокументованими.

Таким чином, документ є практичним посібником для професіоналів, які здійснюють належну перевірку активів у межах вимог CSSF Regulation No 12-02. Він пропонує як концептуальні орієнтири, так і конкретні практичні рекомендації, дозволяючи забезпечити відповідність регуляторним вимогам без зайвого навантаження на ресурси.

Регулювання

6-та Директива ЄС з протидії відмиванню коштів: Нові вимоги та ключові зміни для підзвітних суб'єктів[3]



Документ є оновленою версією поширених запитань (FAQs), що стосуються 6-ї Директиви ЄС з протидії відмиванню коштів та фінансуванню тероризму (AMLD6), ухваленої у травні 2024 року. Ця директива, разом із Регламентом з протидії відмиванню коштів (AMLR), є частиною нового пакету регуляцій, спрямованих на посилення боротьби з фінансовими злочинами у країнах ЄС. Основний акцент зроблено на забезпеченні прозорості корпоративних структур через регламентацію доступу до інформації про кінцевих бенефіціарів та посилення вимог до суб'єктів, які виконують заходи з дотримання стандартів у сфері ПВК/ФТ.

Директива встановлює єдине визначення кінцевого бенефіціара, яке базується на двох ключових компонентах: володінні часткою у компанії та контролі над її діяльністю. Вона закріплює базовий поріг у 25% частки у власності або прав голосу, але передбачає можливість зниження цього порогу до 15% для високоризикових секторів. Ця гнучкість покликана врахувати особливості різних галузей і забезпечити належний рівень нагляду.

Однією з важливих новацій є уніфікація правил доступу до реєстрів кінцевих бенефіціарних власників у країнах-членах ЄС. Доступ до цієї інформації надається компетентним органам, підзвітним суб'єктам, а також іншим категоріям користувачів, які можуть обґрунтувати наявність законного інтересу. Це включає журналістів, неурядові організації, дослідників, а також постачальників рішень у сфері ПВК/ФТ, таких як Moody's, за умови дотримання чітких обмежень щодо використання цих даних.

Директива вимагає від країн-членів забезпечити створення централізованих реєстрів бенефіціарів, що включатимуть історичні дані до 10 років і дозволять проводити перевірку точності внесеної інформації. Верифікація таких даних є обов'язковою, що сприяє підвищенню їхньої достовірності та дозволяє компетентним органам ефективніше розслідувати можливі випадки відмивання коштів.

Висновки:

- **Покращення прозорості структури власності:** Встановлення чітких критеріїв для ідентифікації кінцевих бенефіціарів дозволить зменшити можливість приховування власності через складні корпоративні структури.
- **Розширення кола підзвітних суб'єктів:** Включення нових секторів, таких як криптоактиви та інвестиційна міграція, сприятиме підвищенню ефективності протидії відмиванню коштів у різних сферах економіки.
- **Верифікація даних у реєстрах:** Запровадження історичних записів та зобов'язання щодо перевірки точності даних підвищують рівень довіри до інформації в реєстрах.
- **Підтримка бізнесу через інноваційні інструменти:** Використання API, аналітичних інструментів та доступу до реєстрів кінцевих бенефіціарів від Moody's допомагає підзвітним суб'єктам ефективно дотримуватись регуляторних вимог.

[3] https://www.moodys.com/web/en/us/site-assets/ma-kyc-amld6-faqs.pdf

Важливим аспектом AMLD6 є розширення переліку підзвітних суб'єктів, на яких поширюються вимоги регуляції. До них додано постачальників послуг у сфері криптоактивів, операторів інвестиційної міграції, агентів і клуби у професійному спорті, а також учасників торгівлі предметами розкоші та мистецтва. Це розширення охоплює нові сфери економіки, які раніше могли залишатись поза фокусом регуляторів, і дозволяє посилити контроль над ризиковими транзакціями.

Moody's, як провайдер рішень у сфері дотримання вимог у сфері ПВК/ФТ, пропонує автоматизовані інструменти для ідентифікації клієнтів, визначення кінцевих бенефіціарних власників, аналізу складних структур власності та моніторингу змін у режимі реального часу. Інтеграція таких інструментів у процеси підзвітних суб'єктів дозволяє їм не лише відповідати регуляторним вимогам, але й покращувати операційну ефективність у протидії відмиванню коштів і фінансуванню тероризму.

Цей документ є важливим ресурсом для розуміння регуляторних змін, практичного впровадження вимог AMLD6 та забезпечення відповідності підзвітних суб'єктів новим стандартам у сфері протидії фінансовим злочинам.

Санкції

Перший крок у боротьбі з тероризмом: нові фінансові санкції Великої Британії проти підтримки IRA [4]

Велика Британія вперше застосувала новий режим фінансових санкцій в рамках боротьби з тероризмом, зокрема діяльністю, пов'язаною з Північною Ірландією. Головною метою цього заходу є обмеження доступу до фінансових ресурсів осіб, які сприяють терористичній діяльності, та запобігання їхній подальшій участі у фінансуванні тероризму. Центральною фігурою, проти якої застосовано санкції, є Браян Шерідан, підозрюваний у підтримці "Нової Ірландської республіканської армії" (New IRA). Його звинувачують у сприянні терористичній діяльності через надання фінансових послуг та ресурсів цій організації.

Санкції передбачають повне замороження всіх фінансових та економічних ресурсів, які належать Шерідану або перебувають під його контролем. Це охоплює як особисті активи, так і активи компаній, що асоціюються з ним, зокрема Brisher Limited. Будь-яка фінансова чи економічна взаємодія з підсанкційною особою або компаніями, які вона контролює, без попередньо отриманої ліцензії від Міністерства фінансів Великої Британії є забороненою та вважається кримінальним правопорушенням. Цей крок демонструє серйозність намірів уряду Великої Британії захищати мир і стабільність у Північній Ірландії, а також підтримувати принципи Белфастської угоди, яка є основою для врегулювання конфліктів у цьому регіоні.

Замороження активів означає повну заборону на використання або передачу фінансових ресурсів чи інших економічних активів, які належать або контролюються підсанкційною особою. При цьому активи залишаються у власності первинного власника, але доступ до них блокується. Це обмеження унеможливлює здійснення будь-якої діяльності, яка могла б прямо чи опосередковано сприяти фінансуванню тероризму.

Законодавчою основою для цих дій є Регламент "Counter-Terrorism (Sanctions) (EU Exit) Regulations 2019", який надає Міністерству фінансів Великої Британії повноваження запроваджувати санкції проти фізичних осіб та організацій, підозрюваних у терористичній

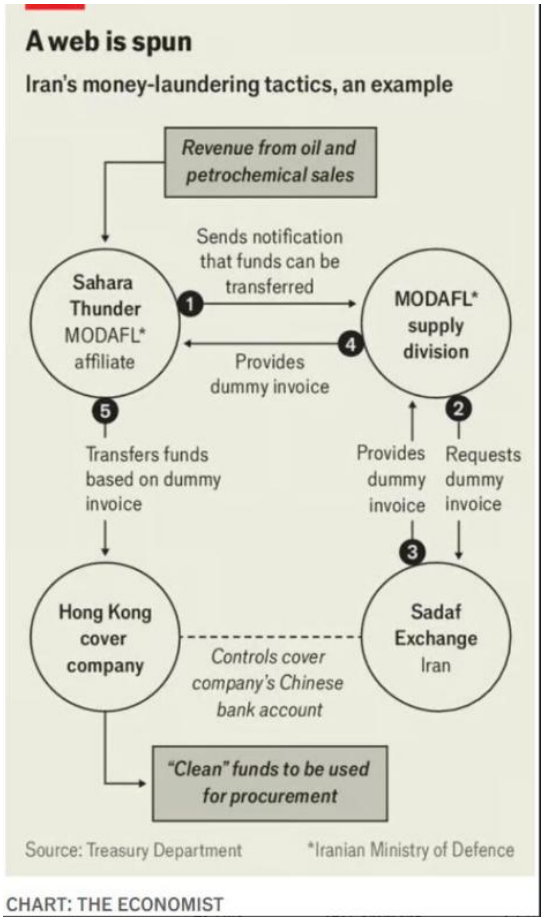
[4] https://www.gov.uk/government/news/new-sanctions-under-domestic-counter-terrorism-regulations

діяльності. Цей правовий інструмент дозволяє Великій Британії діяти незалежно від міжнародних санкційних режимів, адаптуючи заходи до конкретних викликів національної безпеки.

Дії Великої Британії у цьому випадку є важливим кроком у розбудові більш ефективної системи протидії фінансуванню тероризму. Це створює прецедент для подальшого застосування таких заходів, а також слугує прикладом для інших країн, які можуть використовувати подібні санкційні механізми у своїх юрисдикціях. Уряд Великої Британії підкреслює свою прихильність до запобігання тероризму, захисту своїх громадян і забезпечення безпеки на національному рівні.

Як Іран обходить санкції

Іран застосовує складні методи для обходу санкцій, що дозволяє країні спрямовувати мільярди від таємних продажів нафти на глобальні рахунки. Ці кошти підтримують терористичні атаки Хезболли та ХАМАС проти Ізраїлю, постачання безпілотників Росії для війни в Україні та просування ядерної програми Ірану.



- Станом на липень 2024 року Іран мав 53 мільярди доларів і 17 мільярдів євро, які зберігалися за кордоном. Китай купує більшу частину іранської нафти та відмиває доходи. Різні світові банки та фінансові установи, часто мимоволі, беруть участь у цих операціях, переміщуючи гроші в обхід санкцій.
- У продажу нафти Іраном беруть участь різноманітні міністерства та військові групи, що діють незалежно, створюючи феодальну структуру, яка фінансує урядові та військові ініціативи, включаючи Вартових Ісламської революції.
- У торгівлі нафтою часто використовуються підставні компанії та посередники, які переважно знаходяться в Китаї, Туреччині та Малайзії. Транзакції здійснюються через слабо регульовані території, такі як Гонконг, із використанням підроблених сертифікатів походження, щоб уникнути виявлення.
- Китай відіграє вирішальну роль, використовуючи свою банківську систему для полегшення ухилення Іраном санкцій. Кошти непомітно перераховуються до Гонконгу, де іранські ріали обмінюються та переміщуються по всьому світу, часто в обхід регулятивного контролю.
- Тіньова банківська мережа Ірану включає великі нафтові компанії, які діють як банки та створюють підставні компанії по всьому світу. Але через посередницькі збори Іран отримує лише 30-50% потенційної ринкової вартості.

Звіти окремих інституцій та експертів

Готівка у злочинному світі: чи залишається вона королевою у цифрову епоху? [5]

Дослідження, написане Еммою Баркер, аналізує роль готівки у кримінальному світі на тлі змін у глобальній фінансовій екосистемі, таких як зростаючий перехід до безготівкової економіки та популяризація криптовалют. Автор, базуючись на своєму багаторічному досвіді у сфері фінансових розслідувань, розглядає, чи залишається готівка ключовим інструментом у злочинній діяльності та чи може цифрова економіка зменшити її вплив.

У вступі підкреслюється, що готівка традиційно була як засобом, так і результатом злочинної діяльності, особливо в таких сферах, як торгівля наркотиками, відмивання грошей та фінансування тероризму. Автор згадує про дослідження Europol 2015 року, яке встановило домінуючу роль готівки у злочинному світі, але зазначає, що з моменту публікації цього звіту виникли нові фінансові системи, які дозволили злочинцям урізноманітнити свої засоби роботи.

Зазначається, що готівка залишається популярною серед злочинців через її анонімність та мінімальний ризик відстеження. Ці аспекти роблять її менш уразливою для виявлення правоохоронцями порівняно з електронними фінансовими системами. Водночас, автор звертає увагу на зростання використання криптовалют, які також мають анонімний характер, але менш зрозумілі для багатьох злочинців.

Методологія дослідження заснована на анкетуванні, яке проводилося серед правоохоронців і громадськості, щоб отримати думки про використання готівки у злочинних схемах. Відповіді респондентів підкреслюють, що готівка залишається широко використовуваною, особливо в низових рівнях злочинності, де її переваги, такі як легкість у використанні та обіг без необхідності звертатися до фінансових установ, переважують її недоліки. Однак на вищих рівнях злочинності спостерігається тенденція до відмивання готівки через інші фінансові інструменти для легалізації доходів.

Висновки:

- **Готівка залишається важливим інструментом злочинців:** Анонімність та простота використання роблять її ключовою в схемах відмивання грошей і фінансування тероризму.
- **Безготівкова економіка не обов'язково знижує злочинність:** Попри тенденцію до зменшення використання готівки, злочинці адаптуються до цифрових платежів та криптовалют.
- **Криптовалюти та нові виклики для правоохоронців:** Зростання використання криптовалют створює нові ризики, які потребують адаптації правоохоронних стратегій та підвищення кваліфікації фахівців.
- **Необхідність покращення міжвідомчої співпраці:** Скоординована робота між урядом, правоохоронними органами та фінансовим сектором є критично важливою для боротьби з використанням готівки у злочинах.

[5] https://www.college.police.uk/article/cash-still-king

Результати дослідження підтверджують, що, попри зниження використання готівки у суспільстві, вона все ще залишається важливим інструментом у злочинному середовищі. Згідно з думкою респондентів, ключовими причинами цього є анонімність, відсутність слідів транзакцій та низький ризик відстеження правоохоронцями. Водночас перехід до безготівкової економіки викликає неоднозначні оцінки щодо його впливу на зменшення злочинності. Деякі респонденти вказують на нові ризики, які виникають через використання цифрових валют і платежів.

Автор робить висновок, що, попри зростаючий вплив цифрової економіки, готівка все ще виконує ключову роль у злочинних операціях завдяки своїм унікальним властивостям. Вона рекомендує подальше проведення досліджень із більшим обсягом вибірки для отримання більш детальних даних про використання готівки злочинцями. Також підкреслюється важливість розробки ефективних механізмів для боротьби з готівковими злочинними схемами та адаптації правоохоронних органів до нових викликів, зокрема пов'язаних із криптовалютами.

Стійкість гібридних систем контрабанди у Лівії: аналіз тенденцій та викликів [6]

Дослідження детально аналізує сучасний стан контрабанди людей у Лівії, акцентуючи увагу на гібридних системах контрабанди, які об'єднують легальні та нелегальні маршрути міграції. Гібридна модель стала домінуючою завдяки поєднанню відносної стабільності в Лівії після завершення та хронічної політичної фрагментації, яка унеможливлює ефективну координацію боротьби з цим явищем. Головним елементом цієї системи є переміщення мігрантів легальними маршрутами, зокрема через аеропорт Беніна, що став основною точкою в'їзду для людей, які пізніше намагаються нелегально перетнути Середземне море до Європи.

Звіт наголошує на важливості східного Лівійського вузла Беніна–Тобрук у контрабандних схемах. У першій половині 2023 року цей маршрут був ключовим для нелегальної міграції, забезпечуючи приблизно 40% усіх морських відправлень. Контроль над цим вузлом здебільшого належить Лівійській арабській армії (ЛАА), яка отримує вигоду від організації потоків мігрантів через аеропорт Беніна та морські перевезення з Тобрука. Однак у липні 2023 року операції в Тобруці були припинені внаслідок урядових дій. Це призвело до зміни напрямків міграції, зокрема до зростання активності на західному узбережжі, де Зувара стала новим епіцентром контрабанди.

Зувара, розташована на західному узбережжі Лівії, довела свою роль як ключовий вузол завдяки наявності добре організованих контрабандних мереж. У жовтні та листопаді 2023 року відбулося різке збільшення кількості відправлень з цього регіону, що стало можливим завдяки зміні підходів місцевих правоохоронців, які тимчасово припинили боротьбу з контрабандою після повітряних ударів. Після відновлення дій правоохоронців наприкінці

[6] https://globalinitiative.net/wp-content/uploads/2024/08/Rupert-Horsley-Libya-Hybrid-human-smuggling-systems-prove-resilient-GI-TOC-September-2024.pdf

року активність на узбережжі дещо зменшилась, але Зувара залишилася ключовою точкою у гібридних схемах контрабанди.

Дослідження також розглядає роль транс-сахарських маршрутів у контрабанді людей. З 2017 року ці маршрути залишаються здебільшого покинутими через підвищені ризики для мігрантів, зростання рівня насильства та посилення контролю в країнах транзиту, таких як Нігер. Проте громадянська війна в Судані та зміни в політиці сусідніх країн, таких як скасування обмежень на перевезення мігрантів у Нігері, можуть створити нові ризики, сприяючи відновленню потоку людей через Лівію.

Основним висновком документа є те, що гібридні системи контрабанди в Лівії надзвичайно стійкі завдяки політичній нестабільності, відсутності єдиного управління та високому рівню організованості контрабандних мереж. Попри періодичні зусилля урядових структур і міжнародних партнерів щодо стримування контрабанди, відсутність координації та системного підходу ускладнює реальні зміни. Автори підкреслюють важливість глибшої міжнародної співпраці, цільових дій на локальному рівні та зміцнення інфраструктури для протидії нелегальній міграції.

Реформування режиму ПВК/ФТ в Австралії[7]

FIH Insights за грудень 2024 року надає всебічний аналіз нещодавно прийнятого Закону про внесення змін до AML/CTF 2024 року, який став найбільш значущою реформою у сфері протидії відмиванню коштів (AML) та фінансуванню тероризму (CTF) в Австралії за останні десятиліття. Ця реформа спрямована на модернізацію регуляторного середовища, розширення його охоплення на високо ризиковані професії (юристів, бухгалтерів, агентів з нерухомості та дилерів дорогоцінними металами) та впровадження ризик-орієнтованого підходу. Зміни передбачають обов'язкову реєстрацію близько 90,000 нових звітних суб'єктів у AUSTRAC до березня 2026 року та їхню повну відповідність новим зобов'язанням до липня того ж року.

У випуску підкреслюється, що Австралія не лише наздоганяє міжнародні стандарти, але й стикається з численними викликами, зокрема необхідністю ефективної підтримки малого та

Висновки:

- **Tranche 2 зменшує регуляторні прогалини:** Новий закон значно розширює охоплення ПВК/ФТ, включаючи раніше виключені високоризикові професії (юристи, ріелтори). Це покращує національну відповідність стандартам FATF.
- **Ризик-орієнтований підхід:** Введення обов'язкових оцінок ризиків ВК/ФТ як центрального елементу програм з ПВК дозволяє суб'єктам ефективніше розподіляти ресурси та запобігати фінансовим злочинам.
- **Критичність підготовки та підтримки:** Впровадження навчання, консультацій і підтримки для малих підприємств та професійних асоціацій є обов'язковим для забезпечення ефективного виконання нових регуляцій.
- **FATF 2026 — визначальний виклик:** Для досягнення позитивної оцінки необхідно показати реальну ефективність реформ через підвищення якості звітності, наглядових заходів і практичного використання законів.

[7] https://media.licdn.com/dms/document/media/v2/D561FAQFJQ170RNtqog/feedshare-document-pdf-analyzed/B56ZP1jtKXGsAY-/0/1734991619322?e=1736985600&v=beta&t=rjE2ROEB-3Fvt1d3ibPKtXtOQ-0nP4YOZNb__OdQp24

середнього бізнесу в адаптації до нових регуляцій. Автори видання відзначають, що введення обов'язкових оцінок ризиків ML/TF стане основою для більш ефективної боротьби з фінансовими злочинами. У той же час особлива увага приділяється підготовці Австралії до майбутньої оцінки FATF у 2026 році, яка стане випробуванням для нових регуляторних змін.

Значну частину випуску присвячено глобальним урокам у сфері AML/CTF, зокрема досвіду Великобританії та Нової Зеландії, що демонструє важливість співпраці між регуляторами, професійними асоціаціями та правоохоронними органами. Автори також наголошують на необхідності навчання, технологічної підтримки та створення керівництв, які полегшать бізнесу виконання нових зобов'язань. Видання завершується оглядом майбутніх викликів, підкреслюючи необхідність цілеспрямованої роботи над підвищенням ефективності нагляду та реалізацією реформ.

Регуляція криптовалют у Великій Британії 2024: Комплексний посібник для бізнесу та інвесторів[8]

Документ є всебічним посібником з регулювання криптовалют у Великій Британії. Його метою є надання зрозумілої та структурованої інформації щодо нормативної бази, що регулює криптовалютний сектор. Авторка звертає увагу на складність регуляторного середовища, спричинену розрізненістю джерел нормативних вимог, і прагне створити єдиний ресурс для зручного доступу до інформації.

Висновки:

- **Сфера регуляторного впливу та комплаєнс:** Усі криптобізнеси, що працюють у Великій Британії, повинні реєструватися у FCA та відповідати вимогам ПВК/ФТ. Відсутність реєстрації може призвести до заборони діяльності.
- **Нові вимоги до фінансових рекламних кампаній:** Впровадження строгих правил щодо реклами криптоактивів, включаючи попередження про ризики, оцінку відповідності клієнтів та інші обмеження.
- **Проблеми доступу до банківських послуг**: Законні криптобізнеси стикаються з труднощами через «debanking», що може гальмувати розвиток галузі.
- **Необхідність швидких дій:** Велика Британія ризикує втратити позиції на глобальному ринку криптоактивів через відсутність чіткої та всеосяжної регуляторної бази.

Документ починається з огляду регуляторного середовища у Великій Британії. Уряд країни, на відміну від інших держав, використовує фазовий підхід до впровадження регуляцій, адаптуючи чинне законодавство до криптовалютного сектору. Це дозволяє регулювати криптоактиви на основі їхньої реальної функції, а не лише технічних характеристик. Основні типи криптоактивів включають токени обміну, утилітарні токени та токени безпеки. Головними регуляторами виступають FCA, HM Treasury, Банк Англії, PRA та OFSI, які координують політику в різних аспектах ринку.

Друга частина документа присвячена протидії відмиванню коштів (ПВК). У 2020 році криптоактиви були включені до

[8] https://media.licdn.com/dms/document/media/v2/D4E1FAQGWlao3w_Fq-w/feedshare-document-pdf-analyzed/B4EZPUL0hUHkAY-/0/1734431750825?e=1736985600&v=beta&t=AgmvvyTGSUJiHEu8vb9COliR2Ezp7Mx5fHKdHYLXrLU

законодавства про ПВК, що наклало обов'язок на бізнес реєструватися у FCA. Документ описує вимоги, що включають перевірку клієнтів, моніторинг транзакцій та звітування про підозрілі операції. Також у 2023 році був запроваджений «Travel Rule», який зобов'язує бізнес ділитися інформацією про сторони транзакцій, особливо за участі міжнародних контрагентів.

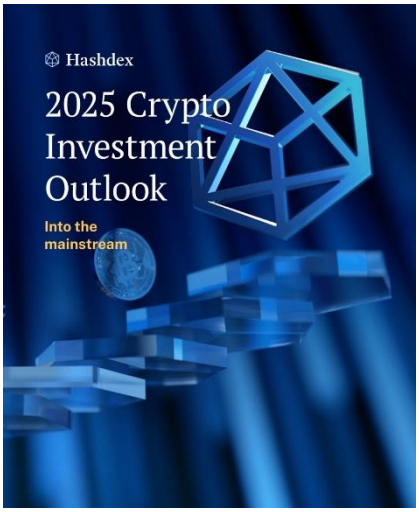
Фінансові промоції криптоактивів у Великій Британії регулюються через оновлений Financial Promotions Order. З 2023 року реклама криптоактивів повинна відповідати строгим стандартам: містити попередження про ризики, оцінювати знання інвесторів та забезпечувати 24-годинний період очікування для нових інвесторів. Це спрямовано на захист роздрібних споживачів від необґрунтованих ризиків.

Документ також описує ширшу регуляторну базу для криптовалютного сектору. Спочатку планувалося, що регулювання буде впроваджуватись у дві фази: перша зосереджена на стейблкоїнах, друга – на ширшому спектрі активів. Однак у 2024 році з'явилися ознаки відходу від фазового підходу на користь одночасного впровадження регуляцій для всього сектору.

Окремо розглядаються інші аспекти, як-от заборона криптодеривативів для роздрібних споживачів, розробка цифрового фунта (CBDC) та створення правової категорії для цифрових активів. Введено «Digital Securities Sandbox» – платформу для тестування інновацій у сфері цифрових цінних паперів.

Документ підкреслює значні виклики для галузі, включаючи обмежений доступ до банківських послуг для криптокомпаній та ризик втрати конкурентоспроможності через відсутність всеосяжної нормативної бази. Авторка закликає до швидких і рішучих дій, щоб Велика Британія могла зберегти свої позиції на глобальному ринку криптоактивів.

Криптовалюти у 2025: Нові горизонти інвестицій та виклики ринку[9]



Документ від Hashdex пропонує глибокий аналіз поточного стану криптовалютного ринку та перспектив його розвитку у 2025 році. Звіт підсумовує досягнення 2024 року, коли криптоіндустрія пройшла значну трансформацію, і окреслює ключові тенденції, які, ймовірно, впливатимуть на ринок у наступному році. Основний акцент зроблено на інституційному попиті, технологічних інноваціях, регуляторних зрушеннях та потенціалі криптовалют у глобальній економіці.

Автори звіту зазначають, що 2024 рік був визначальним для ринку криптовалют завдяки двом значущим подіям: затвердженню ETF на основі Bitcoin та Ethereum і виборам у США, що привели до влади уряд із про-криптовалютною політикою. Ці події посилили впевненість інституційних інвесторів і сприяли значному зростанню ринку, включаючи рекордні показники Bitcoin. ETF на основі криптовалют привернули мільярдні інвестиції завдяки прозорості та регульованості, які вони забезпечують. Це дозволило зробити криптовалюту більш доступною для великих гравців ринку, таких як пенсійні фонди та корпоративні скарбниці.

[9] https://media.licdn.com/dms/document/media/v2/D4E1FAQE1tWBn1tNMoA/feedshare-document-pdf-analyzed/B4EZQHvAxwHkAY-/0/1735296635817?e=1736985600&v=beta&t=oPlx4mKWIFvVkW4a2VRas3Blhgnu2gNHuOCJdPTh4SU

У 2025 році основними драйверами зростання ринку, на думку авторів, будуть інституційний попит, масштабування інфраструктури блокчейнів та розвиток нових децентралізованих застосунків. Особливий акцент зроблено на двох фундаментальних тенденціях. Перша – це подальше утвердження Bitcoin як глобального активу для збереження вартості в умовах економічної нестабільності та дедоларизації. Зростаючий попит на Bitcoin серед інституційних інвесторів та навіть можливість використання його як стратегічного резервного активу державами підкреслюють його значущість. Друга тенденція – це перехід до нової ери інтернету, або Web3, що ґрунтується на блокчейн-технологіях. Це відкриває можливості для децентралізованих додатків, які надають користувачам контроль над їхніми даними та цифровими активами.

Технологічні інновації залишаються основою для подальшого розвитку галузі. Звіт виділяє значущість масштабування блокчейн-інфраструктури, зокрема завдяки Layer-2 рішенням і оновленню Dencun для Ethereum, які знизили витрати на транзакції та підвищили їх швидкість. Однак конкуренція між блокчейнами, такими як Ethereum та Solana, свідчить про невизначеність лідерства в цій сфері. Водночас, інтеграція штучного інтелекту (ШІ) і блокчейну представляється як перспективний напрямок, здатний забезпечити нові способи використання криптовалют, зокрема в автоматизованих екосистемах.

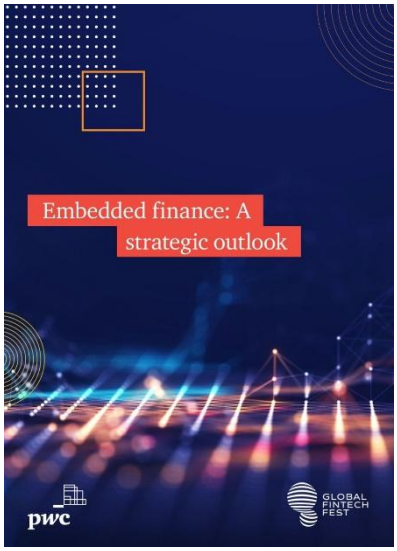
Висновки:

- **Інституційний попит:** 2025 рік може стати переломним для інституційного інвестування в криптовалюту. Затвердження ETF забезпечить доступність та прозорість, що сприятиме притоку капіталу від пенсійних фондів, суверенних фондів і корпоративних скарбниць.
- **Правова визначеність:** Очікуване впровадження нових законодавчих актів у США, включаючи закон про стабільні монети та Bitcoin як стратегічний резервний актив, створить стабільне середовище для розвитку індустрії.
- **Інфраструктурні інновації:** Технологічні покращення, такі як Dencun-апгрейд Ethereum і розвиток Layer-2 рішень, забезпечать масштабування блокчейнів, знижуючи витрати та збільшуючи швидкість транзакцій.
- **Web3 та нові застосунки:** Розвиток Web3-технологій відкриє можливості для нових децентралізованих додатків, що можуть змінити способи взаємодії з цифровими активами, зокрема в соціальних мережах, іграх та фінансах.

Регуляторне середовище також вважається ключовим фактором, який може стимулювати подальший розвиток індустрії. Очікується, що у 2025 році в США буде впроваджено нові законодавчі ініціативи, включаючи законопроєкти щодо стабільних монет, Bitcoin як стратегічного резерву та загального регулювання криптовалют. Ці заходи повинні забезпечити необхідну ясність для інституційних інвесторів і сприяти розвитку нових фінансових продуктів.

Звіт підкреслює, що 2025 рік може стати визначальним для криптовалют, відкриваючи нові можливості для інвесторів і підсилюючи їхню роль у глобальній економіці. Водночас, автори наголошують на необхідності врахування потенційних ризиків, таких як геополітична нестабільність, макроекономічні коливання та конкуренція між блокчейнами. Загалом, звіт акцентує увагу на трансформаційних змінах, які можуть вплинути не лише на криптовалютну індустрію, але й на світову фінансову систему в цілому.

Вбудоване фінансування: Новий вектор трансформації фінансових послуг та бізнес-моделей[10]



Документ, підготовлений PwC, висвітлює трансформаційний вплив вбудованого фінансування (EmFi) на фінансовий сектор та суміжні індустрії. EmFi передбачає інтеграцію фінансових послуг, таких як платежі, кредити, страхування та інвестиції, безпосередньо у нефінансові платформи, роблячи фінансові транзакції більш доступними, персоналізованими та безшовними для кінцевих користувачів. Цей підхід значно знижує вартість залучення клієнтів для фінансових установ та одночасно збільшує лояльність і зручність для споживачів.

Ринок EmFi демонструє стрімке зростання, він оцінений у 66,8 млрд доларів США у 2022 році, і прогнозується, що до 2032 року цей показник зросте із середньорічним темпом (CAGR) 25,4%. Найбільшими ринками є США, Велика Британія та Німеччина, а в країнах на кшталт Індії очікується значне зростання завдяки широкому впровадженню цифрових фінансових технологій. EmFi відкриває нові можливості для бізнесу, зокрема у сферах електронної комерції, транспортної логістики, охорони здоров'я, аграрного сектору та освіти. Наприклад, інтеграція BNPL-рішень у платформи електронної комерції дозволяє користувачам робити покупки у розстрочку, збільшуючи рівень конверсії та доходи компаній.

Висновки:

- **Фінансова інклюзія:** EmFi допомагає залучити до фінансових послуг раніше незабезпечені групи населення, такі як фермери, мігранти та працівники гіг-економіки, через мобільні платформи та мікрофінансові інститути.
- **Економія ресурсів та швидка інтеграція:** API-інтеграції дозволяють нефінансовим компаніям швидко інтегрувати фінансові послуги, що значно скорочує витрати на розробку власних рішень.
- **Необхідність співпраці:** Для успішного розвитку EmFi необхідна гармонійна співпраця між фінансовими установами, технологічними компаніями та регуляторами.
- **Фокус на безпеці:** Ефективна реалізація EmFi вимагає інвестицій у кібербезпеку, механізми управління ризиками та побудову довіри до фінансових платформ.

Технологічна інфраструктура є ключовою складовою успішного впровадження EmFi. API (програмні інтерфейси додатків) є фундаментом для інтеграції фінансових послуг у платформи. Хмарні технології, аналітика в реальному часі та алгоритми штучного інтелекту дозволяють створювати персоналізовані фінансові рішення, покращуючи користувацький досвід. Однак EmFi стикається з низкою викликів. Це, зокрема, ризики порушення безпеки даних, складність дотримання регуляторних вимог у різних юрисдикціях, конкуренція серед гравців ринку та цифровий розрив, що ускладнює доступ до послуг у сільських і віддалених регіонах.

Регуляторна підтримка є важливою для сталого розвитку EmFi. Документ підкреслює необхідність гармонізації стандартів, забезпечення прозорості транзакцій, захисту даних споживачів та створення умов для справедливої конкуренції. Прикладом є індійський закон про захист цифрових даних (DPDPB), який

[10] https://www.pwc.in/assets/pdfs/consulting/financial-services/fintech/publications/embedded-finance-a-strategic-outlook-final.pdf

визначає права споживачів на контроль над своїми даними. Крім того, пропонується впровадження глобальних стандартів та регуляторних «пісочниць» для тестування інноваційних рішень у безпечному середовищі.

Документ наголошує на ролі співпраці між фінансовими установами, нефінансовими платформами та технологічними компаніями. Така взаємодія дозволяє швидко впроваджувати нові послуги, підвищувати якість обслуговування клієнтів і створювати нові джерела доходу. Важливим аспектом є освіта споживачів, яка допомагає підвищити рівень обізнаності про переваги та ризики EmFi, забезпечуючи довіру до нових сервісів.

Наприкінці документ акцентує увагу на потенціалі EmFi як рушійної сили фінансової інклюзії. Вбудовані фінансові рішення здатні забезпечити доступ до банківських послуг для незабезпечених верств населення, таких як фермери, мігранти та представники малого бізнесу, зменшуючи їхній кредитний розрив та підтримуючи економічне зростання. EmFi не лише змінює спосіб надання фінансових послуг, але й сприяє формуванню більш справедливої, стійкої та інклюзивної фінансової екосистеми.

Тренди криптовалют у 2025 році[11]

Документ, створений командою Messari, є детальним аналізом стану криптовалютного ринку, ключових подій 2024 року та прогнозів на 2025 рік. Він охоплює широкий спектр тем, що стосуються технологічних інновацій, регуляторного середовища, ринкових змін та нових трендів, які визначають подальшу еволюцію криптовалютного сектора. 2024 рік охарактеризувався як рік відновлення та трансформації, коли галузь змогла подолати наслідки попередніх циклів волатильності, зосередившись на відновленні довіри, впровадженні інновацій та посиленні позицій як фінансової, так і технологічної екосистеми.

Одним із головних досягнень року стало схвалення ETF для Bitcoin та Ethereum, що вперше забезпечило легітимізацію цих активів серед інституційних інвесторів. Такі події, як рекордні обсяги торгів ETF та зростання капіталізації ринку, підтвердили зростаючий інтерес інституцій до криптовалют. Зокрема, Bitcoin досяг історичного максимуму у $100,000, що стало важливою віхою для всього ринку. Однак ці досягнення були супроводжені викликами у вигляді регуляторних дій SEC, які, попри критику, стимулювали активізацію законодавчих ініціатив для створення чітких правил гри в галузі.

Окрему увагу документ приділяє успіху Solana, яка перетворилася на важливого гравця, поряд із Bitcoin та Ethereum. 2024 рік став визначальним для Solana, яка завдяки своїй технічній продуктивності, низькій вартості транзакцій та впровадженню інновацій, як-от ZK Compression, змогла залучити нових користувачів і зміцнити свої позиції серед інституцій. Її зростання відображає тенденцію до диверсифікації блокчейн-екосистеми, де більше уваги приділяється новим технологіям та реальним кейсам використання.

Сектор DePIN (децентралізованих фізичних інфраструктур) у 2024 році пережив прорив, збільшивши свою капіталізацію на 132% та досягнувши реальних результатів у сферах енергетики, телекомунікацій і зберігання даних. Такі проекти, як Helium Mobile, Glow та GEODNET, продемонстрували потенціал блокчейну як платформи для масштабних

[11] https://messari.io/report/the-crypto-theses-2025

інфраструктурних рішень, здатних впливати на традиційні галузі. У 2025 році прогнозується подальше зростання доходів DePIN, що може перевищити $150 мільйонів, завдяки реальному попиту на його продукти та послуги.

Серед інших важливих аспектів варто відзначити стрімке впровадження стейблкоїнів у країнах, що розвиваються, таких як Латинська Америка та Східна Європа. Вони стали невід'ємною частиною фінансових операцій завдяки своїй доступності та низькій вартості, особливо у сферах P2P-транзакцій та переказів. Одночасно memecoin продовжували залучати нових користувачів, пропонуючи високий потенціал для спекулятивних інвестицій.

Документ завершується прогнозами на 2025 рік, підкреслюючи необхідність подальшого розвитку технологій, таких як Layer-2 рішення для Ethereum, і активної роботи з регуляторами для забезпечення сприятливого середовища для інновацій. Crypto Theses 2025 пропонує вичерпний огляд основних подій та тенденцій, що формують майбутнє криптовалютного ринку.

Висновки:

- **Регуляторна чіткість сприяє залученню інституцій:** Ухвалення ETF для Bitcoin та Ethereum значно розширило доступність криптовалют для інституційних інвесторів, що допомогло стабілізувати ринок та сприяло зростанню капіталізації.
- **Solana формує новий центр впливу:** Зростання Solana у 2024 році свідчить про перехід від дуополії Bitcoin та Ethereum до трикутника, де Solana пропонує масштабованість та інновації.
- **DePIN стає рушієм реальних застосувань блокчейну:** Сектор децентралізованих фізичних інфраструктур (DePIN) продемонстрував значний прогрес у таких сферах, як енергетика, телекомунікації та зберігання даних, з прогнозом на $150 мільйонів річного доходу у 2025 році.
- **Стійкість стейблкоїнів у ринках, що розвиваються:** Використання стейблкоїнів у країнах з обмеженим доступом до традиційних банківських послуг забезпечило їх інтеграцію в повсякденні операції та підкреслило їхню цінність для глобальної фінансової інклюзії.

Інші новини

Операція MATRIX: новий удар по організованій злочинності [12]

Публікація розповідає про масштабну міжнародну операцію, спрямовану на нейтралізацію зашифрованого месенджера MATRIX, який активно використовувався злочинними угрупованнями для координації своєї діяльності. MATRIX був спеціально розроблений для злочинців і відзначався підвищеною безпекою та технічною складністю. Його інфраструктура включала понад 40 серверів, розташованих у різних країнах, серед яких ключовими були Франція та Німеччина. Учасниками цієї операції стали правоохоронні органи Франції, Нідерландів, Литви, Іспанії, Італії, а також Європол і Євроюст.

[12] https://www.europol.europa.eu/media-press/newsroom/news/international-operation-takes-down-another-encrypted-messaging-service-used-criminals

Виявлення системи стало можливим завдяки роботі голландських правоохоронців, які знайшли додаток на телефоні злочинця, засудженого за вбивство журналіста у 2021 році. Подальше розслідування виявило, що платформа була технічно складнішою за попередні зашифровані системи, такі як Sky ECC чи EncroChat. Вона функціонувала на принципі запрошень, а її творці були впевнені у високому рівні захисту. Для перехоплення повідомлень правоохоронці використовували інноваційні технології, що дозволило їм протягом трьох місяців слідкувати за діяльністю злочинців у реальному часі.

Під час операції було перехоплено понад 2,3 мільйона повідомлень, написаних 33 мовами. Ці дані розкрили інформацію про міжнародну торгівлю наркотиками, зброєю та відмивання коштів. 3 грудня 2024 року відбулася скоординована операція із залученням кількох країн. У Франції було заарештовано одного підозрюваного та проведено обшуки. У Іспанії затримали двох осіб за європейським ордером на арешт, а також провели шість обшуків. Подібні дії були здійснені в Литві. Основні сервери системи у Франції та Німеччині були конфісковані.

Результати цієї операції підкреслюють важливість міжнародної співпраці у боротьбі з організованою злочинністю. Спільна слідча група (JIT), створена при Євроюсті, забезпечила швидкий обмін інформацією та доказами між країнами-учасниками, що дозволило провести оперативні дії. Крім того, при Європолі було створено Оперативну робочу групу (OTF), яка здійснювала моніторинг активності злочинців і надала підтримку у подальших розслідуваннях.

Документ також звертає увагу на зміну ландшафту зашифрованої комунікації. Знищення великих платформ, таких як MATRIX, Sky ECC та EncroChat, змушує злочинців переходити до менш відомих або індивідуально створених інструментів зв’язку. Хоча це ускладнює роботу правоохоронців, вони продовжують адаптуватися до нових умов, доводячи, що здатні успішно протистояти викликам сучасних технологій.

Схеми обходу санкцій: Як Білорусь постачає західні мікрочіпи до Росії [13]

Публікація описує масштабне журналістське розслідування, проведене Belarusian Investigative Center (BIC), що досліджує механізми обходу міжнародних санкцій з боку Білорусі. Основна увага приділяється постачанню західних мікрочіпів у Росію через білоруські компанії. Розслідування розкриває, як такі поставки допомагають російському військово-промисловому комплексу забезпечувати виробництво високотехнологічної зброї, яка використовується на війні проти України.

Основний акцент зроблено на обсягах і способах поставок, що здійснюються, попри суворі санкції ЄС і США. Зокрема, було встановлено, що за період з вересня 2022 року до червня 2024 року білоруські компанії перепродали Росії західні мікрочіпи на суму понад $125 млн, із них близько $400,000 — заборонені санкціями компоненти. Ці мікрочіпи використовуються у виробництві винищувачів Су-34 і Су-35S, крилатих ракет «Калібр», а також безпілотників, які активно застосовуються Росією на полі бою.

Розслідування висвітлює роль окремих білоруських компаній і посадовців, причетних до цієї схеми. Наприклад, компанія Alexsvit Ltd, очолювана колишнім заступником голови

[13] https://investigatebel.org/en/investigations/zapadnye-mikroshemy-v-rossii-cherez-belarus

Державного митного комітету Білорусі, активно займалася постачанням мікрочіпів американського, німецького та фінського виробництва. Інша компанія, Logisticheskaya Kompaniya Vostok, була пов'язана з особами з найближчого оточення Олександра Лукашенка. Обидві компанії діяли через складні логістичні маршрути, включаючи перевезення через Туреччину та інші країни.

Автори розслідування зазначають, що значну частину цих операцій прикривають фальсифікацією документів, використанням "буферних" компаній у Білорусі та подальшим перепродажем товарів у Росію. У документі також розкрито, що замовлення мікрочіпів здійснюються через різні маршрути — як через Європу, так і через Азію, залежно від потреб замовника.

Крім того, розслідування проливає світло на те, як ці схеми підривають міжнародні зусилля з дотримання санкційного режиму. Автори звернулися до регуляторів США та ЄС із запитами щодо їхніх заходів протидії таким поставкам, однак на момент публікації відповіді не було отримано. Розслідування підкреслює необхідність тіснішої співпраці між міжнародними партнерами для посилення контролю за походженням і призначенням товарів, які можуть бути використані у військових цілях.

У підсумку, документ демонструє важливість посилення санкційного контролю, виявлення ключових осіб і компаній, залучених до цих схем, а також зміцнення міжнародного співробітництва для припинення незаконного обігу товарів подвійного призначення.

Для загального розвитку

3D загроза: як сучасні технології змінюють незаконний обіг зброї [14]

Публікація розглядає проблему зростаючої загрози виготовлення вогнепальної зброї за допомогою технологій 3D-друку. Автор аналізує цю проблему через конкретний випадок у Фінляндії, де група крайньо-правих екстремістів використовувала такі технології для виробництва зброї з метою підтримки своєї ідеології. Центральною фігурою є Вільям Німан, чия історія розкриває, як особисті переживання, ідеологічна радикалізація та доступ до сучасних технологій можуть призвести до серйозних загроз для громадської безпеки.

Історія починається з опису дитинства Німана, його досвіду цькування, соціальної ізоляції та поступового занурення у крайньо-праві ідеї. Згодом він знаходить однодумців у радикальних інтернет-спільнотах, які поділяють його погляди на "акселераціонізм" — ідею прискорення соціального колапсу через насильство для побудови нових, етно-націоналістичних структур. Разом із трьома іншими учасниками групи він починає виробляти зброю, використовуючи 3D-принтери, а також обговорювати можливі напади на представників етнічних меншин, критичну інфраструктуру та державні установи.

Ключовим моментом є використання FGC-9, напівавтоматичної зброї, яка стала революцією у світі 3D-друкованої зброї. На відміну від ранніх моделей, які були ненадійними і вимагали використання регульованих компонентів, FGC-9 повністю виготовляється з доступних матеріалів і не включає деталей, які підлягають контролю. Це робить її особливо

[14] https://www.theguardian.com/lifeandstyle/2024/dec/07/gun-control-is-dead-and-we-killed-it-firearms-that-can-be-printed-at-home

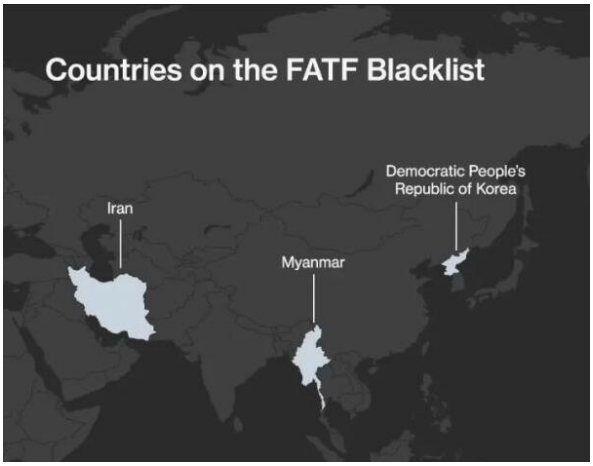
привабливою для екстремістів та організованих злочинних угруповань. Креслення FGC-9 та детальна інструкція зі створення зброї, яку легко знайти в інтернеті, підкреслюють складність контролю за цими технологіями.

Стаття також аналізує діяльність поліції у Фінляндії, яка змогла запобігти потенційним атакам, зібравши докази, що включали як фізичні зразки зброї, так і матеріали переписок між членами групи. Це дозволило правоохоронцям вперше в історії Фінляндії домогтися засудження за звинуваченнями у тероризмі крайньо-правого спрямування. Водночас автор підкреслює складнощі правового переслідування, адже, попри наявність зброї та ідеологічних мотивів, конкретних планів нападів у підозрюваних виявлено не було.

Окрему увагу приділено питанням правового регулювання. Уряди різних країн намагаються адаптувати законодавство до нових викликів, забороняючи як володіння зброєю, так і компонентами або кресленнями для її виготовлення. Однак ці заходи мають обмежений ефект через відкритість технології 3D-друку, дешевизну та доступність обладнання. Зростаюча складність і популярність таких технологій створює значні ризики, особливо у країнах зі строгими законами про зброю, які в іншому разі обмежували б доступ до вогнепальної зброї.

Завершується матеріал міркуваннями про майбутнє: автор наголошує, що ця проблема потребує глобального підходу. Відсутність скоординованих міжнародних дій і реактивний характер політичної системи залишають простір для подальшого поширення цієї загрози. Технології 3D-друку перетворили зброю з контрольованого ресурсу на щось, доступне будь-кому з достатньою кількістю грошей, часу та навичок.

Чорний список FATF: Інструмент глобальної фінансової безпеки



Чорний список FATF, офіційно відомий як список юрисдикцій із високим ризиком, є потужним інструментом у боротьбі з ВК/ФТ. Група з розробки фінансових заходів боротьби з ВК (FATF) створила цей список, щоб ідентифікувати країни, які не дотримуються міжнародних стандартів фінансового моніторингу. У 2024 році до списку входять такі країни, як Північна Корея, Іран та М'янма.

Що таке чорний список FATF і чому він важливий?

Чорний список FATF — це не просто символічний інструмент, а потужний механізм тиску. Країни, включені до нього, стикаються з серйозними економічними наслідками, такими як обмеження доступу до міжнародних фінансових ринків, зростання транзакційних витрат і недовіра інвесторів. Цей список також спонукає фінансові установи до більш прискіпливого підходу під час роботи з такими країнами, що зменшує можливості для незаконної діяльності.

Як країни потрапляють до списку?

FATF включає до чорного списку юрисдикції, які не виконують рекомендації організації щодо боротьби з ВК і ФТ. Основними критеріями є недостатній нагляд за фінансовими потоками, слабкі механізми перевірки транзакцій та відсутність ефективного співробітництва з міжнародними організаціями.

Вплив на юрисдикції зі списку

Для країн, що потрапляють до списку, це не лише репутаційний удар, а й значні економічні втрати. Наприклад:

- Іран стикається з обмеженнями на експорт нафти та фінансові операції.
- Північна Корея потерпає від майже повної ізоляції в міжнародних банківських системах.
- М'янма зазнає труднощів із залученням іноземних інвестицій через нестабільну фінансову систему.

Геополітичний контекст

Включення до чорного списку FATF має і геополітичне підґрунтя. Воно демонструє солідарність міжнародної спільноти у боротьбі з фінансовими злочинами, але також підкреслює важливість політичного впливу у формуванні глобальної фінансової політики.

Чорний список FATF — це нагадування про важливість міжнародної співпраці для забезпечення прозорості фінансових систем. Для країн, які прагнуть виключення зі списку, це шанс реформувати свої регуляторні механізми, а для світової спільноти — можливість посилити безпеку та стабільність.

Ключові тенденції, що формують ПВК/ФТ/ФР у 2025 році

З огляду на 2025 рік очікується, що сфера ПВК/ФТ/ФР швидко розвиватиметься. Ось деякі з найбільш впливових тем, які формуватимуть те, як організації боротимуться з фінансовими злочинами в наступному році:

1. Впровадження передових технологій: ШІ та машинне навчання відіграватимуть більшу роль у моніторингу в режимі реального часу, а регулятори очікують, що фірми використовуватимуть ці інструменти для боротьби зі все більш складними загрозами.
2. Прозорість бенефіціарної власності: завдяки більш ретельній перевірці кінцевих бенефіціарних власників (КБВ) організації стикаються з більш суворими вимогами належної перевірки.
3. Санкції та комплаєнс протидії ФР: зі зростанням геополітичної напруженості дотримання стандартів фінансування протидії розповсюдженню стане критично важливим.
4. Регулювання віртуальних активів: криптовалюти та децентралізовані фінанси (DeFi) створюють нові можливості та ризики. Очікуйте посилення нагляду за постачальниками послуг віртуальних активів (VASP).
5. Боротьба з відмиванням грошей у торгівлі (TBML): Організаціям потрібно буде посилити контроль над ланцюгами постачання та діяльністю, пов'язаною з торгівлею, щоб подолати зростаючі ризики.
6. Транскордонне співробітництво: розширене міжнародне співробітництво та обмін даними сприятиме узгодженості глобальних систем ПВК/ФТ.
7. Посилена увага FATF: від юрисдикцій з сірого та чорного списків вимагатимуть суворішого контролю ризиків для транскордонних операцій.
8. Фінансування торгівлі людьми: подолання фінансової основи експлуатації людей і сучасного рабства залишатиметься ключовим викликом.
9. Стійкість до кіберзлочинності: зі зростаючим перетином кібератак і фінансових злочинів організаціям потрібно буде посилити інтеграцію кібербезпеки та боротьби з відмиванням коштів.

2025 рік вимагатиме проактивного та адаптивного підходу до дотримання вимог у сфері фінансових злочинів, який поєднує передові технології з узгодженими на глобальному рівні рамковими підходами. Щоб залишатися попереду, необхідно еволюціонувати разом із загрозами та регуляторними вимогами.

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-2025-01

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

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