Методологічний бюлетень

Серійний номер: МінФін-AML-2025-04

Січень 2025

Мета

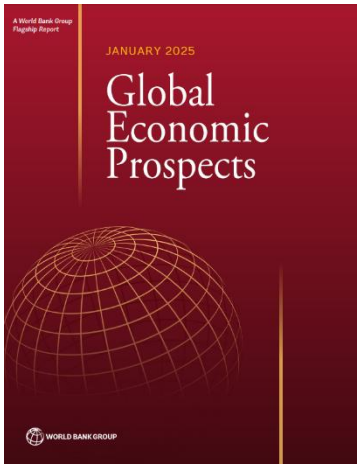
Методологічний Бюлетень видається Міністерством Фінансів України на регулярній основі починаючи з січня 2025 р. та містить інформацію щодо національних та світових тенденцій у сфері протидії відмиванню коштів, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення (ПВК/ФТ/ФР). 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

Глобальні економічні перспективи[1]



Звіт Світового банку є ґрунтовним дослідженням глобальних економічних перспектив на найближчі роки. У ньому аналізуються як загальні тенденції розвитку світової економіки, так і специфічні виклики, з якими стикаються країни з різним рівнем доходу. Головна увага приділяється наслідкам економічних криз, що відбулися у попередні роки, геополітичній напруженості, зміні клімату та структурним проблемам, які обмежують зростання. Звіт не лише відображає поточний стан глобальної економіки, але й надає прогнози на 2025–2026 роки, пропонуючи детальний аналіз регіональних перспектив і політичних викликів.

Згідно зі звітом, глобальне економічне зростання стабілізується на рівні 2,7% у 2025–2026 роках, що є недостатнім для забезпечення стійкого розвитку. Інфляція поступово повертається до цільових показників, а пом'якшення монетарної політики сприяє активізації економічної діяльності. Однак це зростання не компенсує втрати, які зазнала світова економіка через низку потрясінь, таких як пандемія COVID-19, глобальні економічні кризи та геополітичні конфлікти. Серед ключових ризиків відзначаються зростання політичної невизначеності, обмежувальні заходи у міжнародній

[1] https://openknowledge.worldbank.org/server/api/core/bitstreams/e463cf9f-a07e-4848-bf7b-316515429b5d/content

торгівлі, геополітична фрагментація, а також посилення негативного впливу кліматичних катастроф.

Звіт підкреслює, що країни з низьким і середнім рівнем доходу (EMDEs) зазнали особливо значного впливу цих факторів. Зростання в цих країнах залишається на рівні близько 4%, а в багатьох із них рівень доходу на душу населення залишається нижчим за показники розвинених економік. Особливий акцент зроблено на тому, що темпи конвергенції доходів із розвиненими країнами сповільнилися, а для багатьох економік перспективи досягнення середнього рівня доходу до середини століття залишаються сумнівними. Також відзначається, що економіки з низьким рівнем доходу (LICs) стикаються з ще більшими труднощами через конфлікти, слабке інституційне середовище, високий рівень боргу та низьку продуктивність.

Важливе місце у звіті займає аналіз регіональних перспектив. У Східній Азії та Тихоокеанському регіоні очікується уповільнення через слабкий внутрішній попит у Китаї. У Європі та Центральній Азії прогнозується скорочення темпів зростання через економічне уповільнення у великих країнах регіону. Водночас у Латинській Америці, на Близькому Сході, у Південній Азії та Африці на південь від Сахари прогнозується покращення ситуації, частково завдяки стійкому внутрішньому попиту. Проте навіть у цих регіонах зберігаються значні ризики, пов'язані з нестабільністю, змінами у світовій торгівлі та кліматичними викликами.

Документ також акцентує увагу на необхідності структурних реформ і координації міжнародної політики. Пропонується зосередитися на розбудові людського капіталу, модернізації інфраструктури, підвищенні рівня інклюзивності на ринках праці та зміцненні фінансової стійкості. Особлива увага приділяється питанням глобальної співпраці для боротьби зі змінами клімату, подолання фрагментації світової торгівлі та вирішення проблем надмірного боргового навантаження. Водночас зазначається, що країни мають застосовувати індивідуальні підходи до реформ, враховуючи їхню унікальну ситуацію.

У довгостроковій перспективі звіт вказує на необхідність адаптації до демографічних змін, подолання соціальних нерівностей та стимулювання інвестицій у стійке зростання. В умовах обмежених ресурсів, політики мають зосередитися на створенні стабільного макроекономічного середовища, стимулюванні інновацій та підтримці найбільш уразливих груп населення.

Висновки:

- **Стабільне, але низьке зростання**: Очікуване зростання світової економіки на рівні 2.7% у 2025–2026 рр. не дозволить країнам із низьким і середнім рівнем доходу швидко наблизитися до рівня розвинених країн.
- **Ризики конфліктів і кліматичних змін**: Економічні втрати, спричинені конфліктами та катастрофами, потребують термінових заходів для зміцнення стабільності, включаючи міжнародну допомогу.
- **Необхідність структурних реформ**: Для прискорення зростання слід інвестувати у модернізацію інфраструктури, розвиток людського капіталу та вирішення проблем соціальної нерівності.
- **Інтеграція та співпраця**: Розвиваючі країни повинні поглиблювати економічні зв'язки між собою, що створить можливості для збільшення торгівлі та інвестицій.

Загалом звіт Світового банку не лише аналізує поточні економічні реалії, а й надає конкретні рекомендації щодо дій, які дозволять країнам із низьким і середнім рівнем доходу краще адаптуватися до нових викликів, підвищити свою економічну стійкість та забезпечити тривалий розвиток.

Стаття 142 MiCAR[2]

Документ підготовлений EBA та ESMA на основі статті 142 MiCAR. Він аналізує розвиток ринків криптоактивів із фокусом на децентралізовані фінанси (DeFi), кредитування, позики та стейкінг криптоактивів. Доповідь є частиною аналітичного звіту для Європейського парламенту і Ради ЄС щодо регулювання та моніторингу новітніх фінансових практик.

Доповідь окреслює, що DeFi, хоча і залишається нішевим явищем, демонструє значний потенціал з огляду на масштаби ринку, який у 2024 році оцінювався в 78 мільярдів євро (Total Value Locked, TVL). Основні протоколи, такі як Lido та Aave, концентрують значну частину активів. Однак DeFi має високий рівень ризиків, серед яких відсутність регуляторних механізмів для боротьби з ВК/ФТ, а також технологічні ризики, пов'язані з використанням смарт-контрактів і oracles*.

У розділі про кредитування, позики та стейкінг криптоактивів аналізуються бізнес-моделі, що включають централізовані та децентралізовані платформи. Звіт підкреслює недоліки у прозорості умов для користувачів, особливо щодо комісій, відсоткових ставок та вимог до забезпечення. Виявлено також високий рівень ризику, пов’язаний із надмірним використанням кредитного плеча, інформаційними асиметріями та системними загрозами.

Що стосується технологічних ризиків, DeFi стикається з викликами, пов’язаними з хакерськими атаками, втратою приватних ключів користувачів, вразливістю смарт-контрактів та механізмами міжланцюгових мостів (cross-chain bridges). Часті атаки спрямовані на маніпуляцію цінами через oracles, що є ключовими компонентами технологічної інфраструктури DeFi.

Висновки:

- **Ризики ВК/ФТ у DeFi:** Відсутність регуляторних механізмів, таких як KYC, збільшує ризики ВК/ФТ. Це потребує термінового впровадження процедур з ПВК/ФТ.
- **Технологічна вразливість**: Смарт-контракти та міжланцюгові мости залишаються основними точками атак, що підкреслює необхідність впровадження стандартів безпеки.
- **Недостатня прозорість**: Для користувачів криптопослуг бракує інформації щодо умов кредитування, стейкінгу та забезпечення, що створює значні ризики.
- **Регуляторні прогалини**: Поточні норми MiCAR недостатні для регулювання DeFi, тому потрібна подальша гармонізація на міжнародному рівні.

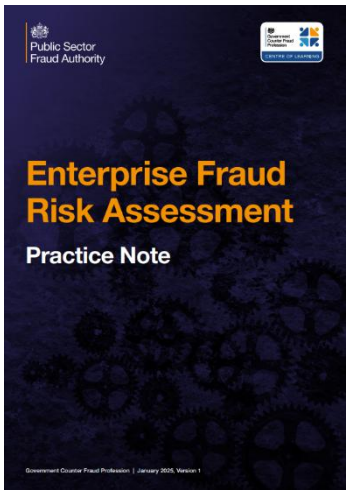
Доповідь також аналізує регуляторні аспекти. Визначено, що поточна нормативна база, включаючи MiCAR, не повністю охоплює DeFi через децентралізований характер. Це підкреслює необхідність подальшого дослідження можливостей регулювання, включаючи інтеграцію KYC-процедур у DeFi-протоколи та впровадження стандартів цифрової операційної стійкості (DORA) для захисту споживачів.

Загалом документ акцентує на важливості розвитку моніторингових механізмів для підвищення прозорості та стабільності ринку, а також на необхідності посилення міжнародної співпраці для протидії ризикам, пов’язаним із криптоактивами.

[2] https://www.esma.europa.eu/sites/default/files/2025-01/ESMA75-453128700-1391_Joint_Report_on_recent_developments_in_crypto-assets__Art_142_MiCA_.pdf

** У криптовалютній та блокчейн-індустрії оракули – це служби або системи, які надають блокчейну доступ до зовнішніх даних, необхідних для виконання смарт-контрактів. Наприклад, оракули можуть передавати інформацію про ціни, результати подій чи погодні умови.*

Практична примітка щодо оцінки ризиків шахрайства підприємств[3]



Документ є керівництвом, розробленим Державною службою з протидії шахрайству, яке описує практичні підходи до проведення оцінки ризиків шахрайства на рівні організації (Enterprise Fraud Risk Assessment, EFRA). Головна мета документа — надати спеціалістам із протидії шахрайству інструменти для ідентифікації основних ризиків, оцінки їхнього впливу та розробки стратегій управління, які можуть ефективно підтримувати керівництво організацій у прийнятті рішень.

Оцінка EFRA представляє собою вищий рівень аналізу ризиків шахрайства, який розглядає всю організацію загалом, і надає інформацію, яка дозволяє зрозуміти, наскільки організація вразлива до шахрайських дій. Документ визначає EFRA як інструмент взаємодії з керівництвом, який зосереджується на найбільших ризиках, спрямовує ресурси на їхнє пом'якшення та демонструє важливість ефективної боротьби з шахрайством для забезпечення стійкості організації.

Особливістю EFRA є адаптивний підхід, який враховує унікальні особливості кожної організації, включаючи її цілі, структуру та операційне середовище. EFRA також повинна відображати результати інших оцінок ризиків (наприклад, тематичних або повних FRA) і забезпечувати інтеграцію даних у вигляді єдиної картини ризиків.

Документ підкреслює важливість базування оцінки ризиків на доказах, а не на думках чи анекдотичних доказах. У ньому зазначено, що важливо уникати надмірної деталізації, щоб зосередитися на ключових ризиках, які матимуть найбільший вплив на організацію. Також рекомендовано розробити індивідуальні підходи до оцінки ризиків, які враховують специфіку галузі чи сектору діяльності організації.

Основні елементи EFRA включають структурування ризиків за ключовими

Висновки:

- **Інтеграція ризиків у стратегію управління**: EFRA має стати невід'ємною частиною процесів управління організацією, забезпечуючи керівництво реалістичними оцінками ризиків для прийняття стратегічних рішень.
- **Залучення керівництва**: Ефективне представлення результатів EFRA через виконавчі резюме, візуальні матеріали та конкретні приклади значно підвищує розуміння та залучення керівництва до управління шахрайством.
- **Оцінка на основі доказів**: Використання доказів і даних (замість суб'єктивних оцінок) є критично важливим для підвищення надійності EFRA, зокрема через моделювання потенційних втрат і використання зовнішніх порівнянь.
- **Динамічний підхід**: EFRA повинна бути постійним процесом, що враховує зміни в організаційному середовищі, нові драйвери ризиків і інноваційні підходи до боротьби з шахрайством.

[3] https://assets.publishing.service.gov.uk/media/6788cfa969b9b76c761d048c/EFRA_Practice_Note_Final.pdf

схемами або бізнес-напрямами, оцінку впливу ризиків, визначення відповідальних за управління ризиками, ідентифікацію ключових драйверів ризиків та виявлення зон невизначеності. Документ наголошує на важливості включення аналітичних даних, таких як фінансові втрати від виявленого шахрайства, та моделювання потенційних втрат для надання реалістичної картини ризиків керівництву.

Крім того, у документі визначено рекомендації щодо візуального представлення EFRA, яке має бути зрозумілим для керівництва. Зокрема, пропонується використовувати тематичний підхід (зосереджуючи увагу на конкретних бізнес-напрямках) або орієнтуватися на перехресні ризики, які впливають на кілька напрямків діяльності організації. Для залучення уваги керівництва до ключових питань ризиків пропонується підготовка виконавчих резюме та графічних матеріалів.

EFRA також описується як процес, який має бути постійним і регулярно оновлюватися. Оновлення повинно відбуватися щонайменше раз на рік або після виникнення «тригерних подій», наприклад, структурних змін в організації. Цей процес включає використання порівняльного аналізу, оцінки нових драйверів ризику та їхнього потенційного впливу.

Пропорційність у наглядовій діяльності: Аналіз впровадження SREP у Європейському Союзі[4]

Звіт є результатом аналізу впровадження принципу пропорційності в рамках Процесу нагляду, перегляду та оцінки (SREP), здійсненого Європейським банківським органом (EBA). Основна увага приділена тому, як компетентні органи ЄС реалізують вимоги до пропорційності, визначені у Керівництвах EBA/GL/2022/03. Пропорційність є ключовим принципом, що дозволяє адаптувати частоту, інтенсивність і фокус наглядових заходів залежно від ризикового профілю, масштабів діяльності та складності установ.

У звіті зазначається, що принцип пропорційності загалом реалізується, однак існують значні варіації у його застосуванні між різними юрисдикціями. Категоризація установ за рівнем їхньої значущості, розміром, ризиковим профілем та складністю є основою для визначення наглядових підходів. Зокрема, установи поділяються на чотири категорії, де категорія 1 охоплює найбільші системно важливі банки, а категорія 4 — малі неконцентровані установи. У цьому процесі використовується низка джерел інформації, таких як дані звітності, попередній аналіз бізнес-моделей, а також класифікація «великих» та «малих неконцентрованих установ» відповідно до Регламенту про вимоги до капіталу (CRR). Однак у ряді країн, таких як Польща та Угорщина, ці підходи ще не повністю впроваджені або мають суттєві недоліки.

Пропорційність також проявляється у частоті та інтенсивності наглядових заходів. Керівництва SREP передбачають мінімальну модель взаємодії, яка визначає періодичність зустрічей наглядових органів із керівництвом установ залежно від їхньої категорії. Проте у деяких країнах спостерігаються відхилення від цих вимог. Наприклад, в Угорщині відсутні регулярні

[4] https://www.eba.europa.eu/sites/default/files/2025-01/6e3232b7-1113-40f7-8ae4-b8d5e20a3802/Peer%20review%20report%20on%20the%20application%20of%20proportionality%20in%20SREP.pdf

зустрічі з керівництвом установ 3-ї та 4-ї категорій, тоді як у Польщі для установ 4-ї категорії взаємодія базується лише на необхідності.

Оцінка ліквідності є ще однією сферою, де застосовується пропорційність. Компетентні органи адаптують інтенсивність аналізу ліквідності залежно від профілю ризику установи. Це стосується таких аспектів, як оцінка коротко- та середньострокових потреб у ліквідності, аналіз внутрішніх процесів управління ліквідністю (ILAAP) та аналіз стійкості до ризиків ліквідності. У ряді юрисдикцій пропорційність у цих аспектах ще не реалізована повною мірою. Наприклад, у Німеччині та Франції проведення аналізу стійкості до ризиків ліквідності не є обов'язковим для всіх установ. У той же час, Люксембург і Польща впровадили практики, що враховують ризиковий профіль установ при плануванні аналізу стійкості до ризиків ліквідності.

Одним із ключових викликів для наглядових органів є забезпечення узгодженості та гармонізації підходів у різних країнах. Розбіжності в категоризації установ і різні моделі взаємодії створюють ризики для рівномірного застосування наглядових заходів у всьому ЄС. Для вирішення цих проблем звіт рекомендує уніфікувати критерії категоризації, забезпечити обов'язковість використання класифікації CRR та вдосконалити підходи до оновлення категоризації у разі значних корпоративних подій.

Висновки:

- **Покращення гармонізації:** Запровадження уніфікованих критеріїв категоризації та адаптація моделей мінімальної взаємодії з установами значно підвищить ефективність та справедливість наглядових заходів.
- **Інновації в аналізі стійкості до ризиків ліквідності:** Рекомендовано впровадити централізовані та автоматизовані системи такого аналізу для всіх установ, враховуючи їхній ризиковий профіль.
- **Навчання та інструменти:** Зміцнення наглядових компетенцій через спеціалізовані тренінги з пропорційності та використання IT-рішень для забезпечення послідовності оцінок.
- **Посилення практичної пропорційності:** Використання тематичних перевірок і кластерного підходу для банків з однаковим профілем ризику сприятиме оптимізації ресурсів.

У звіті також наводяться приклади найкращих практик. Наприклад, у Франції використовуються інструменти порівняльного аналізу ключових ризикових показників, які допомагають наглядовим органам оцінювати ризики на етапі підготовки до ухвалення рішень. У Польщі впроваджені механізми перевірки достовірності інформації, яку надають банки у своїх самооцінках.

Підсумовуючи, звіт рекомендує компетентним органам удосконалити свої підходи до впровадження пропорційності, забезпечивши її ефективну реалізацію у всіх аспектах SREP, зокрема в оцінці ризиків ліквідності, категоризації установ та моделі взаємодії. Водночас звіт наголошує на необхідності подальшого навчання персоналу, використання IT-рішень для забезпечення послідовності наглядових заходів і впровадження інноваційних підходів, таких як тематичні перевірки та кластеризація установ із подібними бізнес-моделями.

Провали експортного контролю США: Чому технології продовжують підтримувати агресію росії та зміцнювати Китай[5]

Документ аналізує діяльність Бюро промисловості та безпеки США (BIS) у контексті контролю експорту напівпровідників як одного з ключових інструментів національної безпеки США. Зокрема, звіт зосереджується на тому, як експортні обмеження використовуються для обмеження доступу Китаю до передових технологій, здатних надати йому стратегічну перевагу в оборонній та технологічній сферах, а також для унеможливлення використання напівпровідників у російських військових системах, що підтримують війну проти України. Попри впровадження жорстких заходів, ці інструменти виявилися малоефективними в досягненні поставлених цілей.

Звіт зазначає, що BIS, як основний регулятор експорту товарів подвійного призначення, має широкі повноваження, але стикається з численними викликами. Основна проблема – це недостатнє фінансування, яке залишається майже незмінним із 2010 року, попри значне зростання обсягів експорту та відповідно збільшення навантаження на BIS. Через обмежений бюджет BIS не має достатніх ресурсів для здійснення належного контролю за кінцевим використанням товарів у країнах, які ідентифікуються як транзитні пункти для поставок напівпровідників до росії. Такі країни, як Вірменія, Казахстан, Туреччина та інші, використовуються для обходу експортних обмежень, що дозволяє російському ВПК отримувати необхідні технології.

Крім того, звіт акцентує увагу на застарілій IT-інфраструктурі BIS, яка значно обмежує можливості аналізу даних та моніторингу порушень. Технологічна база установи не зазнавала значних змін із 2006 року, що змушує аналітиків витрачати до 80% робочого часу на пошук інформації замість її аналізу. Така ситуація серйозно послаблює здатність BIS ефективно реагувати на нові виклики.

Ще однією проблемою є недостатнє використання BIS своїх повноважень для посилення відповідальності компаній за порушення. У звіті зазначено, що BIS не накладає жорстких санкцій за свідомі порушення експортного контролю, навіть за наявності явних доказів обізнаності компаній про ризики обходу санкцій. Також BIS покладається на добровільну співпрацю компаній у розробці програм експортного контролю, що виявилося недостатньо ефективним. Компанії не зобов'язані

Висновки:

- **Проблема фінансування:** BIS потребує щонайменше $75 мільйонів додаткового річного фінансування та $100 мільйонів одноразово для модернізації IT-систем, які критично необхідні для боротьби з нелегальним експортом.
- **Недостатність заходів контролю:** У 2022–2023 роках BIS провело лише 1304 перевірки кінцевого використання у країнах, залучених до реекспорту до росії. Цього недостатньо для ефективного запобігання порушенням.
- **Неадекватність санкцій:** BIS не застосовує достатньо жорстких штрафів за «свідомі» порушення, що обмежує стимулювання компаній до дотримання експортного контролю.
- **Рекомендації щодо змін:** Конгресу США рекомендується терміново переглянути фінансування BIS, а також запровадити обов'язкові стандарти для компаній, залучених до експортної діяльності.

[5] https://www.hsgac.senate.gov/wp-content/uploads/The-U.S.-Technology-Fueling-Russias-War-in-Ukraine-Examing-BISs-Enforcement-of-Semiconductor-Export-Controls.pdf

дотримуватися обов'язкових стандартів, і більшість із них не мають адекватних механізмів контролю.

Документ пропонує низку рекомендацій для покращення ситуації. По-перше, BIS потребує збільшення фінансування на $75 мільйонів щорічно та одноразового гранту в розмірі $100 мільйонів для модернізації IT-систем. По-друге, BIS має запровадити обов'язкові стандарти для експортного контролю в компаніях і регулярно проводити їх перевірки. По-третє, BIS слід прискорити процес впровадження жорсткіших санкцій за порушення, включаючи значно більші штрафи. Ці заходи дозволять зробити експортний контроль більш ефективним та підвищити відповідальність компаній за дотримання правил.

Загалом, документ підкреслює важливість комплексного підходу до експортного контролю, що включає збільшення фінансування, технологічну модернізацію та регуляторні реформи для забезпечення національної безпеки США та підтримки міжнародних санкцій.

Токенізація активів і технології DLT: потенціал, виклики та майбутнє фінансових ринків за даними OECD[6]

У звіті OECD детально аналізуються перспективи впровадження токенізації активів та технологій розподіленого реєстру (DLT) у фінансовій сфері. Основний акцент зроблено на потенційних вигодах, існуючих бар'єрах для розвитку ринків токенізованих активів та політичних і регуляторних імплікаціях. Незважаючи на великий інтерес до DLT серед учасників ринку та регуляторів, реальне впровадження цієї технології залишається на початкових стадіях і здебільшого обмежується пілотними проєктами та експериментами.

У доповіді зазначено, що токенізація активів має значний потенціал трансформувати фінансові ринки завдяки таким перевагам, як автоматизація процесів, зниження витрат, підвищення прозорості та ліквідності активів. Завдяки DLT можливо реалізувати програмовані функції, що дозволяють автоматизувати післятрейдингові процеси, зменшити ризики та прискорити розрахунки. Це особливо важливо для активів із низькою ліквідністю, де DLT може значно підвищити доступність для інвесторів. Крім того, токенізація сприяє розвитку нових фінансових продуктів, таких як смарт-контракти, які дозволяють автоматизувати операції та полегшують транснаціональні транзакції.

Проте в документі виділяється низка проблем, які стримують масштабне впровадження токенізації. Основним викликом є відсутність зрілої екосистеми та достатньої ліквідності на ринку токенізованих активів. Багато проєктів залишаються експериментальними, без переходу до комерційного впровадження через високі витрати на інфраструктуру та невизначеність стосовно економічної доцільності таких інвестицій. Відсутність глобальних стандартів, включаючи ідентифікацію токенів і учасників ринку, також значно ускладнює інтеграцію DLT із традиційними фінансовими системами.

Юридичні аспекти токенізації є однією з найбільших перешкод. У багатьох юрисдикціях досі не визначено, чи надає володіння токеном юридичні права на базовий актив, а статус смарт-контрактів залишається неврегульованим. Ця невизначеність створює додаткові ризики для інвесторів, особливо в разі банкрутства емітента токенів або кастодіана.

[6] https://www.oecd.org/en/publications/tokenisation-of-assets-and-distributed-ledger-technologies-in-financial-markets_40e7f217-en.html

Висновки:

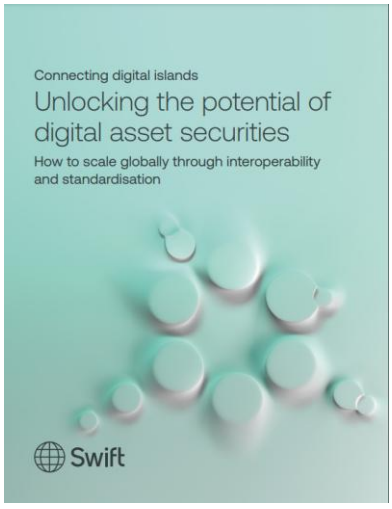
- **Ліквідність та екосистема:** Створення ліквідного ринку токенізованих активів потребує участі ключових учасників ринку (наприклад, банків та кастодіанів) та інтеграції з традиційними фінансовими інфраструктурами.
- **Роль CBDC:** Цифрові валюти центрального банку можуть сприяти інтеграції платіжних систем з DLT, дозволяючи безперервне врегулювання транзакцій (DvP).
- **Регуляторні ініціативи:** Дерегуляція для пілотних проєктів (як-от Digital Securities Sandbox у Великобританії) сприяє дослідженню нових технологій та формуванню нових бізнес-моделей.
- **Юридична визначеність:** Необхідно врегулювати правовий статус токенів і смарт-контрактів, щоб забезпечити довіру інвесторів і знизити правові ризики.

У звіті наголошується на важливості інтеграції платіжних систем із DLT, зокрема через впровадження цифрових валют центрального банку (CBDC) чи інших форм токенізованих грошей. CBDC можуть забезпечити безпечні та ефективні розрахунки в режимі «поставка проти оплати» (DvP), що є ключовим для функціонування токенізованих ринків. Разом із цим наголошується на необхідності розробки стандартів взаємодії між різними мережами DLT, щоб уникнути фрагментації ринків.

У звіті також наведено приклади успішних пілотних проєктів, таких як Digital Securities Sandbox у Великобританії, які сприяють впровадженню інновацій шляхом адаптації регуляторного середовища. Окремо розглядається досвід Швейцарії, яка впроваджує цифрові облігації та використовує wholesale CBDC для розрахунків на платформі розподіленого реєстру.

Загалом звіт підкреслює, що для успішного впровадження токенізації необхідно забезпечити регуляторну підтримку, розвинути інфраструктуру ринків і стандартизацію процесів. Технології розподіленого реєстру можуть стати основою для нових фінансових інновацій, однак їх впровадження вимагає вирішення значних юридичних, технологічних і економічних викликів.

Майбутнє токенізації активів: можливості, бар'єри та роль регуляторів у трансформації фінансових ринків[7]



Документ детально аналізує перспективи використання токенізації активів та технологій розподіленого реєстру (DLT) у фінансових ринках. Він досліджує потенційні переваги, ризики, фактори, які обмежують впровадження, та надає рекомендації для регуляторів і учасників ринку.

У документі зазначено, що токенізація активів, яка включає створення цифрових аналогів реальних активів на основі технологій розподіленого реєстру, має потенціал для трансформації фінансових ринків. Вона здатна забезпечити автоматизацію процесів, дезінтермедіацію (зменшення ролі посередників), підвищити прозорість операцій та ліквідність активів, які раніше були малоліквідними. Завдяки токенізації

[7] https://www.swift.com/sites/default/files/files/swift_digit_asset_securities_whitepaper_final_171224.pdf?utm_source=dem&utm_medium=email&utm_campaign=%%__AdditionalEmailAttribute1%%&utm_term=%%__AdditionalEmailAttribute2%%&utm_id=194270&crmId=%%TFEncryptedIdURLEncoded%%&LoC=%%IsContact%%

можливе скорочення циклів розрахунків, підвищення ефективності клірингових та розрахункових процесів, а також впровадження програмованих операцій за допомогою смарт-контрактів. Технологія також створює можливості для інновацій, таких як випуск «зелених» облігацій або впровадження механізмів автоматизованого управління заставами.

Попри значний інтерес, реальне впровадження токенізації залишається обмеженим. Документ описує основні причини цього, зокрема відсутність зрілої екосистеми для підтримки токенізованих активів, низький рівень ліквідності, а також відсутність масштабованих доказів економічної доцільності впровадження DLT. Багато транзакцій, пов'язаних із токенізацією, реалізуються у межах пілотних проєктів чи експериментів, без створення інтегрованих інфраструктур для повномасштабного використання.

Окрему увагу в документі приділено потребі інтеграції платіжних систем із технологіями DLT. Для реалізації ефективних операцій «поставка проти оплати» (Delivery versus Payment) необхідно забезпечити наявність токенізованих форм грошей, таких як цифрові валюти центральних банків (CBDC) або стабільні токени, які можуть використовуватись для здійснення розрахунків у розподіленому середовищі. Проте впровадження CBDC, особливо в масштабі міждержавних розрахунків, потребує значного часу та вирішення юридичних, регуляторних і технологічних проблем.

Документ також підкреслює ключові технологічні виклики. Основними серед них є складність забезпечення інтероперабельності між різними блокчейнами, а також інтеграція нових технологій із традиційними фінансовими системами. Відсутність глобальних стандартів для ідентифікації токенів, обліку токенізованих активів, а також механізмів управління правами власності створює додаткові бар'єри для впровадження токенізації.

Юридичні питання також є суттєвим стримуючим фактором. У багатьох юрисдикціях не визначено, чи є цифрові активи власністю, як саме здійснюється юридичне підтвердження права власності на токенізовані активи, а також якими є зобов'язання сторін у випадку банкрутства або дефолту. Крім того, використання смарт-контрактів вимагає чіткого регулювання, щоб уникнути ризиків, пов'язаних із помилками в програмному коді або відсутністю чітких правил виконання.

Документ наголошує на важливості збереження «технологічного нейтралітету» у регулюванні, де однакові ризики ідентифікуються та регулюються незалежно від застосовуваної технології. Однак регулятори повинні враховувати специфічні ризики, притаманні DLT, такі як кібербезпека, анонімність транзакцій, а також непрозорість окремих операцій.

Автори дійшли висновку, що для стимулювання впровадження токенізації необхідно створити стимулюючу екосистему, яка включатиме як регуляторну підтримку, так

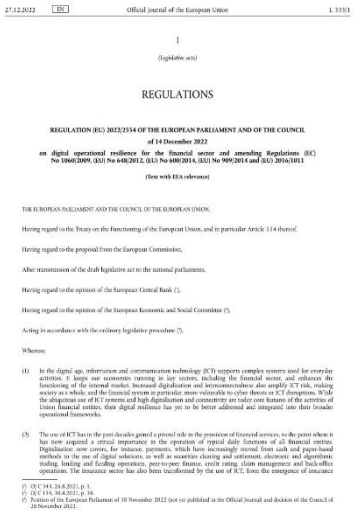
Висновки:

- **Ефективність можлива лише за умови масштабування:** Впровадження DLT та токенізації потребує створення інтегрованої екосистеми, яка охоплює ліквідність, стандартизацію процесів та участь традиційних учасників ринку.
- **Потреба у законодавчій гармонізації:** Без чіткої правової бази, включаючи вирішення питань власності токенів, їх правового статусу та розрахунків, технології не зможуть масштабуватись.
- **Інтеграція CBDC як ключ до успіху:** Використання цифрових валют центральних банків (CBDC) може забезпечити прозорі та безпечні розрахунки, але реалізація цього рішення потребує ще кількох років.
- **Ризик фрагментації ринку:** Невідповідність стандартів та використання приватних блокчейнів може призвести до фрагментації ліквідності, що зменшить переваги від токенізації.

і розвиток стандартів та інфраструктур. Тільки за умови широкої участі всіх зацікавлених сторін, впровадження токенізації може забезпечити заявлені переваги без ризику фрагментації ринків та зниження їхньої ефективності.

Регулювання

Регламент DORA: Нові стандарти цифрової стійкості для фінансового сектору ЄС[8]



27.12.2022 EN Official Journal of the European Union L 333/1

I

(Legislative acts)

REGULATIONS

REGULATION (EU) 2022/2554 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022

on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Central Bank (1),

Having regard to the opinion of the European Economic and Social Committee (2),

Acting in accordance with the ordinary legislative procedure (3),

Whereas:

(1) In the digital age, information and communication technology (ICT) supports complex systems used for everyday activities. It keeps our economies running in key sectors, including the financial sector, and enhances the functioning of the internal market. Increased digitalisation and interconnectedness also amplify ICT risk, making society as a whole, and the financial system in particular, more vulnerable to cyber threats or ICT disruptions. While the ubiquitous use of ICT systems and high digitalisation and connectivity are today core features of the activities of Union financial entities, their digital resilience has yet to be better addressed and integrated into their broader operational frameworks.

(2) The use of ICT has in the past decades gained a pivotal role in the provision of financial services, to the point where it has now acquired a critical importance in the operation of typical daily functions of all financial entities. Digitalisation now covers, for instance, payments, which have increasingly moved from cash and paper-based methods to the use of digital solutions, as well as securities clearing and settlement, electronic and algorithmic trading, lending and funding operations, peer-to-peer finance, credit rating, claim management and back-office operations. The insurance sector has also been transformed by the use of ICT, from the emergence of insurance

(1) OJ C 343, 26.8.2021, p. 1.
(2) OJ C 155, 30.4.2021, p. 38.
(3) Position of the European Parliament of 10 November 2022 (not yet published in the Official Journal) and decision of the Council of 28 November 2022.

Регламент (ЄС) 2022/2554, також відомий як DORA (Digital Operational Resilience Act), був ухвалений Європейським Парламентом та Радою 14 грудня 2022 року і набрав чинності з 27 грудня 2022 року. DORA встановлює єдину правову рамку для забезпечення цифрової операційної стійкості фінансового сектору Європейського Союзу. Цей документ спрямований на підвищення здатності фінансових установ протистояти ризикам, пов'язаним із використанням інформаційно-комунікаційних технологій (ІКТ), а також забезпечити стабільність і безпеку фінансової системи ЄС.

У сучасному світі, де цифрові технології стали основою фінансових операцій, використання ІКТ охоплює всі аспекти фінансової діяльності, включаючи електронні платежі, алгоритмічну торгівлю, кредитування, страхування, кліринг і розрахунки. Водночас високий рівень цифровізації робить фінансові установи більш уразливими до кіберзагроз, системних збоїв і локалізованих інцидентів, які можуть швидко поширюватися через тісну взаємозалежність ІКТ-систем у межах фінансової екосистеми. DORA є відповіддю на ці виклики, заповнюючи прогалини у попередніх регулюваннях та гармонізуючи підходи до управління цифровими ризиками.

Регламент визначає основні вимоги до управління ризиками ІКТ, які повинні впроваджувати всі фінансові установи, що працюють у ЄС. Серед цих вимог: впровадження ефективної системи управління ризиками, регулярне тестування цифрової стійкості, налагодження процедур для виявлення, реагування та відновлення після інцидентів, а також управління ризиками, пов'язаними зі сторонніми постачальниками ІКТ-послуг. DORA зобов'язує фінансові установи документувати

Висновки:

- **Гармонізація вимог до цифрової стійкості:** Документ встановлює єдиний набір правил для управління ризиками ІКТ у фінансовому секторі, що дозволяє зменшити витрати на дотримання регуляцій та уникнути дублювання зобов'язань у різних країнах ЄС.
- **Стратегічне управління ризиками:** Регламент наголошує на необхідності включення управління ризиками ІКТ у загальну стратегію фінансових установ із залученням керівництва до моніторингу ризиків та інцидентів.
- **Моніторинг сторонніх постачальників:** Встановлюються вимоги щодо оцінки ризиків, пов'язаних із постачальниками ІКТ-послуг, з особливим фокусом на критичних постачальниках та захисті даних.
- **Підвищення прозорості:** Запровадження стандартизованих механізмів звітування про інциденти сприятиме швидшій реакції на загрози та покращить загальний стан кібербезпеки в фінансовій екосистемі.

[8] https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng

всі контракти з ІКТ-постачальниками, оцінювати потенційні ризики, проводити перевірки їхньої відповідності стандартам безпеки та впроваджувати стратегії на випадок припинення співпраці з постачальниками.

Окремий акцент зроблено на гармонізації підходів до звітування про інциденти, пов'язані з ІКТ. DORA встановлює єдиний механізм подачі звітів про значні інциденти до наглядових органів, що сприяє більш швидкій реакції на потенційні загрози та забезпечує надійний моніторинг цифрових ризиків у масштабах ЄС. Крім того, регламент передбачає створення центрального «ЄС-хабу» для централізованого обміну інформацією про інциденти, який сприятиме колективному захисту фінансових установ.

DORA також регулює діяльність критичних сторонніх постачальників ІКТ-послуг, таких як постачальники хмарних обчислень, аналітики даних і центрів обробки даних. Для таких постачальників передбачено спеціальний наглядовий механізм (Oversight Framework), який дозволяє контролювати їхній вплив на фінансову систему, враховуючи рівень залежності фінансових установ від їхніх послуг.

Ключовим елементом DORA є принцип пропорційності, який передбачає адаптацію вимог до розміру, складності та ризиків, притаманних конкретній фінансовій установі. Малим і мікропідприємствам дозволено дотримуватися спрощених вимог, щоб знизити адміністративний тягар, зберігаючи водночас їхню здатність протистояти цифровим загрозам.

Регламент DORA є важливим кроком до зміцнення цифрової безпеки фінансової системи ЄС, сприяючи підвищенню довіри споживачів, забезпеченню стабільності ринку та підтримці ефективного функціонування фінансових послуг навіть у кризових ситуаціях.

Звіти окремих інституцій та експертів

Ініціатива з освіти для запобігання та протидії насильницькому екстремізму, що сприяє тероризму[9]

Документ представляє дослідження глобальної ініціативи, спрямованої на використання освіти як інструменту для запобігання та протидії насильницькому екстремізму, що може сприяти тероризму (PVE-E). Його основою є Меморандум добрих практик Абу-Дабі, ухвалений Глобальним форумом із боротьби з тероризмом (GCTF) у 2014 році. Документ відображає досягнення, виклики та нові уроки, що виникли за останнє десятиліття у впровадженні освітніх програм для протидії екстремізму, з особливим акцентом на міжсекторальний підхід, адаптацію до нових технологій і соціокультурний контекст.

Дослідження виявило, що освіта може бути ефективним інструментом профілактики радикалізації, якщо забезпечити інтеграцію інклюзивних практик, створення безпечних навчальних середовищ і розвиток навичок критичного мислення серед учнів. Зокрема, було підкреслено, що програми соціального й емоційного навчання (SEL) сприяють формуванню психологічної стійкості студентів, допомагаючи їм краще

9 https://www.thegctf.org/Portals/1/Documents/Framework%20Documents/2025/Edu4PCVE/ResearchBrief_clean.pdf?ver=EDmwjdzFOrQLcwmtwkc2yA%3d%3d

долати стрес, виявляти ознаки радикалізації серед ровесників і розвивати емпатію. Особливий акцент зроблено на необхідності адаптації навчальних програм до потреб маргіналізованих груп і створенні інклюзивного простору, який враховує культурні, етнічні, гендерні й економічні особливості.

Документ також висвітлює роль цифрових технологій у сучасному освітньому процесі. Використання штучного інтелекту, соціальних медіа й ігрових платформ може значно покращити доступність і привабливість навчальних програм, але водночас створює ризики через поширення радикальних ідей в інтернеті. Важливим завданням залишається формування цифрової грамотності серед учнів, що включає вміння розпізнавати екстремістський контент і протидіяти його впливу. Особлива увага приділяється інтеграції технологій у кризових і постконфліктних умовах, наприклад, у регіонах, які постраждали від терористичної діяльності, як-от Сахель.

Дослідження наголошує на необхідності підвищення професійної підготовки викладачів, які відіграють ключову роль у запобіганні радикалізації. Освітяни потребують спеціалізованого навчання, яке дозволить їм ідентифікувати ранні ознаки екстремізму, управляти емоційним станом студентів і створювати середовище, яке сприяє відкритому діалогу та взаєморозумінню. Було підкреслено, що програми PVE-E мають уникати надмірної орієнтації на безпеку шкільного середовища, яка може призводити до стигматизації учнів.

Ключовим елементом ефективності програм є залучення громад до освітнього процесу. Громадські лідери, молодь і сім'ї повинні активно брати участь у розробці та впровадженні програм, щоб забезпечити їхню культурну й соціальну релевантність. Також наголошено на важливості взаємодії з приватним сектором, який може сприяти реалізації освітніх ініціатив через корпоративну соціальну відповідальність.

Висновки:

- **Інклюзивна освіта**: Освітні програми повинні забезпечувати доступність для всіх верств населення, зокрема маргіналізованих груп, і формувати безпечне середовище для розвитку критичного мислення.
- **Використання новітніх технологій**: Розробка національних стратегій цифрової грамотності та інтеграція штучного інтелекту й ігрових платформ у навчальний процес є ключовими для протидії онлайн-радикалізації.
- **Підтримка педагогів**: Навчання викладачів із акцентом на виявлення ранніх ознак радикалізації та подолання особистих упереджень сприятиме ефективності програм PVE-E.
- **Взаємодія з громадами**: Участь громадських лідерів, родин та молоді в розробці та впровадженні освітніх ініціатив допоможе створити стійке суспільство та мінімізувати ризики екстремізму.

Документ окреслює нагальну потребу в довгостроковому моніторингу та оцінці ефективності програм PVE-E. Автори вказують на недостатність досліджень, які б аналізували довготривалий вплив таких програм, що обмежує можливості їх вдосконалення. Пропонується використовувати сучасні методології оцінювання, які поєднують кількісний і якісний аналізи, залучаючи студентів і громади до розробки та тестування критеріїв оцінки.

Документ пропонує інтеграцію підходів до подолання радикалізації в надзвичайних і кризових ситуаціях, коли діти та молодь є особливо вразливими до впливу екстремістських ідей через відсутність доступу до якісної освіти. Висвітлено успішні моделі з різних країн, які демонструють, як освіта може використовуватися для зміцнення громадської стійкості, подолання структурних нерівностей і розв’язання соціальних конфліктів.

Загрози від держав[10]

Документ, створений Меттью Р. Редгедом у рамках програми SOC ACE, присвячений аналізу сучасних викликів, пов'язаних із державними загрозами, які здійснюються ревізіоністськими державами для досягнення своїх геополітичних цілей. Автор описує багатогранність цих загроз, підкреслюючи, що вони не обмежуються традиційними методами, такими як шпигунство чи саботаж, а активно використовують новітні технології та гібридні підходи.

Державні загрози визначаються як дії, які спрямовані на підрив суверенітету, економічної стабільності або політичного устрою інших держав без оголошення відкритого військового конфлікту. Їх ключова особливість — діяльність, яка не досягає порогу відкритої війни, що дозволяє агресорам уникати прямого засудження чи відповідальності на міжнародній арені. Документ підкреслює, що ці загрози є результатом посилення конкуренції між великими державами, таких як Китай, Росія, Іран і Північна Корея, які використовують асиметричні методи боротьби для посилення власного впливу.

Особлива увага приділяється гібридним методам, які поєднують традиційні підходи з використанням новітніх інструментів. До них належать:

- Кібератаки, які стають основним механізмом для викрадення інформації, завдання економічних збитків або підриву критично важливої інфраструктури. Наприклад, атаки на енергетичні системи, фінансові установи чи державні бази даних мають потенціал завдати довготривалих збитків без прямого військового втручання.
- Дезінформація через соціальні мережі, яка використовується для впливу на громадську думку, дискредитації політичних лідерів чи маніпуляції виборами. Зокрема, автор зазначає, що вплив через медіа є економічно вигідним інструментом, оскільки дозволяє поширювати пропаганду серед широких верств населення за мінімальних витрат.
- Політичне втручання через підтримку опозиційних груп, спонсорування протестів або маніпуляцію елітами. Такі дії можуть дестабілізувати уряди, які не

Висновки:

- **Кібератаки як ключовий інструмент**: Розвиток і інтеграція кіберзахисту є критично важливими для зменшення ризиків від державних загроз, які активно використовують кібератаки для досягнення своїх цілей.
- **Протидія дезінформації**: Необхідно посилювати цифрову грамотність суспільства та впроваджувати механізми для виявлення й блокування дезінформаційних кампаній, які підривають довіру до урядів і демократичних процесів.
- **Міжнародна співпраця**: Ефективна протидія державним загрозам можлива лише через тісну взаємодію між країнами, міжнародними організаціями та приватним сектором для координації дій і обміну інформацією.
- **Адаптація політик безпеки**: Уряди повинні переглядати свої стратегії національної безпеки, враховуючи динамічний характер сучасних загроз, інвестуючи у технологічні інновації та розвиваючи оперативні механізми стримування.

10 https://static1.squarespace.com/static/63e4aef3ae07ad445eed03b5/t/67852e69ff4ff4079a9c3000/1736781420568/SOCACE-RP32-OldWineNewBottles_final.pdf

відповідають інтересам агресора.

Документ також наголошує на ролі недержавних акторів, які працюють на користь держав. Це можуть бути приватні військові компанії, хакерські групи або навіть міжнародні корпорації, які, свідомо чи несвідомо, сприяють реалізації агресивної стратегії.

Важливою складовою державних загроз є їхній економічний вплив. У документі зазначено, що такі дії можуть бути спрямовані на підрив стратегічних галузей економіки, послаблення конкурентоспроможності або створення умов для залежності держави від агресора. Наприклад, інструментами економічного тиску можуть бути санкції, обмеження експорту ключових ресурсів чи маніпуляції з валютними ринками.

Документ підкреслює важливість кіберпростору, який став ключовим середовищем для здійснення державних загроз. Автор пояснює, що кібератаки є відносно дешевими у реалізації, але можуть мати руйнівні наслідки. При цьому ідентифікація джерела атаки залишається складним завданням, що дозволяє агресору зберігати анонімність і уникати прямої відповідальності.

Окремий акцент зроблено на довгостроковому впливі державних загроз. Хоча багато операцій мають короткостроковий характер, деякі з них здатні створювати системні проблеми, підривати довіру до урядів, дестабілізувати суспільства та сприяти економічній деградації.

На завершення документ наголошує на необхідності розробки комплексних політик для протидії державним загрозам. Автор вказує, що ефективна боротьба з такими викликами вимагає координації між державами, приватним сектором і міжнародними організаціями. Зокрема, потрібно вдосконалювати нормативно-правову базу, адаптувати стратегії національної безпеки до нових реалій, інвестувати в кіберзахист і посилювати механізми виявлення та стримування.

Майбутнє цифрових активів: аналіз тенденцій і прогнозів у звіті «2025 Digital Assets Outlook»[11]

Звіт від The Block представляє комплексний огляд тенденцій, досягнень і викликів, які формували криптовалютну і блокчейн-індустрію протягом 2024 року, а також прогнози на 2025 рік. У ньому розглядаються як макроекономічні фактори, так і технічні інновації, регуляторні зміни та впливи на інституційний рівень.

Рік 2024 ознаменувався значним зростанням капіталізації криптовалютного ринку, яка досягла рекордного показника в $3,8 трлн. Основними драйверами цього зростання стали поліпшення глобального економічного середовища, зниження інфляції, інституційне прийняття криптовалют, а також пом'якшення регуляторних обмежень у США. Впровадження спотових Bitcoin ETF стало важливим етапом для галузі, залучивши понад $110 млрд інвестицій і закріпивши статус Bitcoin як важливого фінансового активу.

Solana виділилася як одна з найпродуктивніших блокчейн-мереж 2024 року, завдяки високій пропускній здатності та низьким комісіям, що дозволило їй обійти Ethereum у місячних обсягах торгівлі на децентралізованих біржах (DEX). Інновації, такі як розробка нового валідаторного клієнта Firedancer, продовжують зміцнювати позиції Solana як одного з лідерів ринку. У той же час Ethereum зосередився на зниженні витрат на транзакції за допомогою впровадження EIP-

[11] https://www.tbstat.com/wp/uploads/2024/12/20241230_EOYReport_TBR.pdf

4844, що сприяло експоненціальному зростанню використання Layer-2 рішень, таких як Arbitrum, Optimism і Base.

У сфері децентралізованих фінансів (DeFi) провідні платформи, такі як Uniswap, Aave та Maker, продемонстрували стійкість та адаптивність. Нові продукти, включаючи покращені протоколи кредитування і механізми масштабування, допомогли цим платформам залишатися конкурентоспроможними навіть на тлі регуляторних викликів. Крім того, токенізація реальних активів (RWAs) і стабільних монет стала ключовою темою, залучаючи інституційні інвестиції та розширюючи застосування блокчейнів у традиційних фінансових секторах.

Висновки:

- **Рекордний ріст крипторинку:** Сукупна капіталізація досягла $3,8 трлн, стимульована інституційними інвестиціями, впровадженням спотових ETF і технологічними проривами. Практична дія: стимулювати інвестиції через розширення доступу до ETF.
- **Інновації у масштабуванні блокчейнів:** Ethereum і Solana продемонстрували прорив у зниженні витрат і збільшенні швидкості транзакцій. Solana обігнала Ethereum у DEX-торгівлі. Практична дія: підтримка інфраструктури для високонавантажених мереж.
- **Реалізація DeFi і RWAs:** Токенізація реальних активів стала ключовим драйвером для DeFi, залучаючи традиційні фінансові інституції. Практична дія: інтеграція RWAs з блокчейн-платформами.
- **Регуляторна підтримка:** Адміністрація США знизила бар'єри для криптоіндустрії, створюючи сприятливе середовище для розвитку DeFi та блокчейнів. Практична дія: адвокація за подібні зміни в інших юрисдикціях.

Рік також приніс суттєві зрушення у регуляторній сфері. У США нова адміністрація сприяла пом'якшенню регуляторного клімату для криптоіндустрії, що створило більш сприятливе середовище для інновацій і залучення капіталу. Це надало впевненості інституційним інвесторам, які почали активніше досліджувати можливості децентралізованих фінансів і криптовалют.

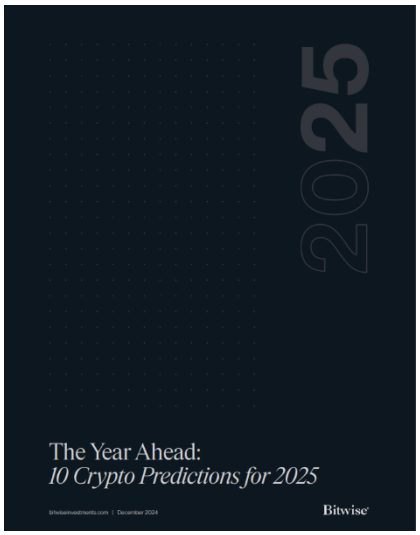
Незважаючи на зростання криптовалютного ринку, деякі сегменти, такі як NFT, зазнали певного спаду. Традиційні NFT втратили популярність, проте нові концепції, такі як Bitcoin Ordinals, повернули інтерес до цієї категорії завдяки інноваційним підходам.

У майбутньому, за прогнозами, ключовими факторами розвитку галузі залишатимуться масштабування блокчейнів, інтеграція реальних активів, посилення регуляторної підтримки і подальша розробка децентралізованих рішень для зниження витрат і покращення ефективності. Звіт підкреслює важливість адаптації до змін і розширення технічних можливостей для збереження лідерських позицій у галузі блокчейнів і криптовалют.

Золота ера криптовалют: 10 проривних прогнозів для 2025 року[12]

Документ відображає амбіційний і оптимістичний погляд на перспективи криптовалютного ринку в найближчому майбутньому. У ньому наводяться десять основних прогнозів, які базуються на економічних, технологічних та регуляторних факторах, що формуватимуть розвиток криптоіндустрії у 2025 році.

[12] https://s3.us-east-1.amazonaws.com/static.bitwiseinvestments.com/Research/Bitwise-The-Year-Ahead-10-Crypto-Predictions-for-2025.pdf



У вступі описується значення 2024 року для криптовалют як поворотного моменту. Автори зазначають рекордні досягнення біткоїна ($103,992) та інших провідних активів, таких як Solana та Ethereum, а також успіх спотових біткоїн-ETF, які зібрали понад $33,6 млрд активів. Перемога кандидатів, які підтримують криптовалютну індустрію, на виборах у США створила більш сприятливі регуляторні умови для індустрії. У документі прогнозується подальше зміцнення криптовалют завдяки підвищенню інституційного інтересу, технологічним інноваціям та глобальному економічному стимулюванню.

Основні прогнози на 2025 рік демонструють очікування значного зростання трьох ключових активів: біткоїна, Ethereum і Solana. Автори передбачають, що біткоїн досягне $200,000 завдяки скороченню пропозиції після хавінгу, новим інституційним покупкам та можливим урядовим закупівлям для резервів. Ethereum, попри втрату популярності у 2024 році, відновить свої позиції завдяки розвитку Layer 2 рішень, зростанню кількості стейблкоїнів та токенізованих активів, які базуються на його мережі. Solana, яка здобула популярність у 2024 році через мемкоїни, привертатиме увагу «серйозних» проєктів, що підсилить її позиції на ринку.

Автори очікують розширення участі інституцій у криптовалютах. Coinbase прогнозується стати найбільшою брокерською компанією у світі, перевершивши Charles Schwab, а її акції можуть досягти ціни $700. Також передбачається, що Coinbase увійде до індексу S&P 500, що зробить криптовалютні активи доступними для більшості американських інвесторів. Водночас регуляторні зміни можуть дозволити криптовалютам увійти до пенсійних планів 401(k), що відкрило б для ринку мільярди доларів інвестицій.

Законодавчі ініціативи відіграють важливу роль у прогнозах. У 2025 році очікується ухвалення законів щодо стейблкоїнів у США, що може подвоїти капіталізацію цього ринку до $400 млрд. Стейблкоїни поступово інтегруються у фінансові сервіси та глобальну торгівлю, конкуруючи з традиційними платіжними системами, такими як Visa. Також очікується різке зростання ринку токенізованих реальних активів, вартість яких може перевищити $50 млрд. Токенізація пропонує швидкі, дешеві та прозорі способи торгівлі активами, що приваблює великі інституції, такі як BlackRock.

Особливий інтерес викликає прогноз щодо нової хвилі мемкоїнів, створених за допомогою агентів ШІ. Це поєднання крипто- та ШІ-технологій демонструє потенціал для масового залучення спекулятивного капіталу, попри високу ризикованість. Автори також

Висновки:

- **Інституційне визнання криптовалют:** Входження великих компаній (Coinbase, MicroStrategy) до ключових біржових індексів значно збільшить обсяг інвестицій у криптовалюти.
- **Законодавчі зрушення:** Прийняття законодавства щодо стейблкоїнів у США сприятиме розвитку фінансових сервісів та інтеграції стейблкоїнів у глобальну економіку.
- **Зростання вартості криптовалют:** Очікується, що біткоїн перевищить $200,000, Ethereum – $7,000, а Solana – $750 завдяки сприятливим регуляторним змінам та технологічним інноваціям.
- **Токенізація активів:** Зростання ринку токенізованих реальних активів до $50 млрд відкриває нові можливості для інвесторів і сприяє пришвидшенню інтеграції крипто у традиційні фінансові ринки.

очікують, що кількість країн, які утримують біткоїн у своїх резервах, подвоїться, створюючи своєрідну глобальну гонку за володіння криптовалютою.

Документ завершується довгостроковим прогнозом, згідно з яким біткоїн до 2029 року перевершить ринок золота за капіталізацією ($18 трлн) і коштуватиме понад $1 млн. Автори підкреслюють, що їхні прогнози не є гарантіями, а залежать від багатьох умов, таких як регуляторна підтримка, макроекономічні фактори та технічний розвиток.

У цілому, документ представляє візію крипторинку як динамічного, інноваційного середовища з великим потенціалом для росту, але водночас попереджає про високі ризики та залежність від зовнішніх факторів.

Навігація між санкціями та перевіркою PEP[13]

Документ є вичерпним керівництвом щодо процедур санкційного та PEP-скринінгу у межах антилегалізаційного законодавства Сінгапуру. Він починається з опису ключових вимог, які підзвітні установи, включаючи фінансові установи та ВНУП, повинні виконувати при встановленні бізнес-відносин, зокрема ідентифікацію клієнтів, визначення їх статусу як PEP або близьких до них осіб, а також перевірку наявності в санкційних списках. Належна перевірка клієнтів базується на ризик-орієнтованому підході, спрямованому на зниження ризиків ВК/ФТ.

Детально розкрито процес скринінгу санкцій, який включає перевірку клієнтів за такими списками, як UNSC Designations, списки ІДІЛ, Аль-Каїди та Талібану, а також національні санкції, передбачені законодавством Сінгапуру. Документ підкреслює зобов'язання з негайного заморожування активів осіб, внесених у санкційні списки, припинення фінансових відносин з ними та подання звітів про підозрілі транзакції до відповідних органів.

PEP-скринінг орієнтований на ідентифікацію осіб, що займають важливі державні чи міжнародні посади, таких як політики, судді, військові чи керівники державних компаній. Хоча

Висновки:

- **Пріоритет належної перевірки клієнтів**: Регульовані установи мають впроваджувати скринінг клієнтів за санкційними списками та на статус PEP, застосовуючи посилені заходи для управління ризиками ВК/ФТ. Це включає визначення джерела коштів та отримання схвалення вищого керівництва для роботи з PEP.
- **Автоматизація процесів для підвищення ефективності**: Використання програмного забезпечення на основі ШІ та машинного навчання є важливим для зниження хибних спрацьовувань і забезпечення оперативного реагування на зміни статусу клієнтів.
- **Зобов'язання щодо звітності**: Усі випадки виявлення санкційних осіб повинні супроводжуватись негайним замороженням активів, припиненням ділових відносин та поданням звітів про підозрілі транзакції до відповідних органів.
- **Підтримка від спеціалізованих консультантів**: AML Singapore пропонує комплексні послуги з управління ризиками ВК/ФТ, включаючи навчання, розробку політик та постійний супровід для забезпечення відповідності регуляторним вимогам.

[13] https://amlsingapore.com/wp-content/uploads/2024/07/Navigating-the-Sanctions-and-PEP-Screening-under-Singapore-AML-Regime-A-Complete-Guide.pdf

законодавство не забороняє відносини з PEP, підкреслюється необхідність застосування посилених заходів належної перевірки, включаючи визначення джерела коштів і багатства, а також отримання схвалення вищого керівництва.

Документ також наголошує на важливості використання сучасних технологій для автоматизації процесів скринінгу. Автоматизовані рішення, зокрема ті, що базуються на штучному інтелекті, допомагають знижувати кількість хибних спрацьовувань, забезпечують постійний моніторинг клієнтів і покращують ефективність реагування на зміни статусу клієнтів.

Окремий розділ присвячений підтримці, яку надає AML Singapore, зокрема допомозі у виборі програмного забезпечення, розробці політик і процедур, навчанні персоналу, а також створенні внутрішніх відділів комплаєнсу.

Рекомендовані матеріали та заходи

Європейський саміт щодо боротьби з фінансовими злочинами 2025[14]

European Anti-Financial Crime Summit 2025 — це один із найзначущих щорічних заходів у сфері протидії фінансовим злочинам, який збирає провідних фахівців з усього світу для обговорення сучасних викликів, тенденцій і рішень у галузі фінансових розслідувань, регулювання та відповідності. Саміт відбудеться 7 травня 2025 року в Дубліні, Ірландія, у RDS Convention Centre, і вже обіцяє стати ключовою платформою для обміну знаннями та досвідом.

Хто організовує захід?

Саміт організований AML Intelligence, одним із провідних міжнародних джерел інформації, досліджень та аналітики у сфері боротьби з фінансовими злочинами, відмиванням коштів, фінансуванням тероризму та іншими пов'язаними ризиками.

Ключові спікери

На саміті виступлять найвпливовіші представники регуляторних органів та провідні фахівці з фінансових технологій та банківського сектора. Серед них:

- Еліза де Анда Мадрасо, Президент FATF, яка очолить дискусію щодо впровадження новітніх стандартів з ПВК/ФТ та глобальної координації.
- Авалон Інгрем, Голова відділу комплаєнсу фінансовим злочинам у SWIFT, яка обговорить роль фінансових технологій у посиленні ефективності боротьби з фінансовими злочинами.
- Провідні представники фінансових регуляторів ЄС, фахівці правоохоронних органів та приватного сектора.

Саміт 2025 року буде присвячений кільком важливим темам:

1. Майбутнє боротьби з фінансовими злочинами: аналіз глобальних викликів та рішень для зміцнення фінансової системи.
2. Інновації у сфері фінансових технологій: використання штучного інтелекту, машинного навчання та блокчейну для виявлення та запобігання фінансовим злочинам.

[14] https://www.amlintelligence.com/asp-products/european-anti-financial-crime-summit-2025/

3. Регуляторні зміни в Європі: огляд нових директив та регуляторних ініціатив у сфері ПВК/ФТ.
4. Роль співпраці між приватним і державним секторами: обмін найкращими практиками у розслідуванні транзакцій та фінансуванні тероризму.

Саміт розрахований на широку аудиторію фахівців, зокрема: а) Керівників та фахівців банків та фінансових установ, які прагнуть удосконалити свої системи контролю та моніторингу; б) Представників регуляторних органів та політиків, які формують політику у сфері фінансових злочинів; в) Технологічних компаній, які розробляють інноваційні рішення для фінансового сектору; г) Правоохоронних органів, зацікавлених у покращенні ефективності розслідувань фінансових злочинів.

European Anti-Financial Crime Summit 2025 є унікальною можливістю для учасників дізнатися про останні тенденції у сфері боротьби з фінансовими злочинами, розширити свою професійну мережу, знайти нові підходи до впровадження інновацій та дізнатися про найкращі практики від провідних експертів. Особливо важливим є те, що саміт зосереджений на інтеграції інноваційних технологій, таких як ШІ та блокчейн, у стратегії протидії злочинності.

Участь у саміті доступна за попередньою реєстрацією на офіційному сайті AML Intelligence. Вартість участі складає €470. Цей захід стане визначною подією у 2025 році для всіх, хто зацікавлений у розвитку більш ефективних та інноваційних підходів до боротьби з фінансовими злочинами.

Інші новини

Штраф компанії Block у розмірі 255 мільйонів доларів США[15]

Компанія Block, співзасновником якої є Джек Дорсі, зіткнулася зі значним штрафом у розмірі 255 мільйонів доларів США через недоліки у дотриманні вимог законодавства щодо ПВК. Цей штраф став одним із найбільших у сфері фінансових технологій і є вагомим сигналом для компаній, які працюють у сфері цифрових платежів. Проблеми, які привели до штрафу, пов'язані з неналежним управлінням ризиками, недоліками в політиках ПВК та неефективним моніторингом транзакцій.

Регулятори визначили такі основні порушення:

1. Відсутність ефективної системи моніторингу транзакцій. Block не змогла забезпечити належний аналіз транзакцій для виявлення підозрілої активності, що дозволило певним користувачам використовувати платформу для потенційного відмивання коштів.
2. Недоліки у процедурі перевірки клієнтів (KYC). Було виявлено, що компанія не забезпечила належної ідентифікації клієнтів у відповідності до регуляторних вимог, що збільшило ризик використання її сервісів злочинцями.
3. Недостатня реакція на ризики фінансування тероризму. Block не впровадила необхідних заходів для оцінки та управління ризиками, пов’язаними з ФТ.

[15] https://www.linkedin.com/pulse/jack-dorseys-block-fined-massive-255m-anti-fraud-failings-unype/?trackingId=UEl2ciACRmWQO0QoMvZsyw%3D%3D

4. Неналежний обсяг звітності щодо підозрілих транзакцій (STRs). Регулятори наголосили на низькій кількості звітів, що свідчить про недооцінку ризиків і слабку взаємодію з ПФР.

Штраф у розмірі 255 мільйонів доларів США був накладений для посилення відповідальності компанії за дотримання вимог законодавства. Регулятори наголосили, що фінансові технологічні компанії повинні приділяти особливу увагу боротьбі з відмиванням коштів, оскільки їхні інноваційні платформи можуть бути легко використані злочинцями для приховування незаконного походження коштів.

Такий масштабний штраф є серйозним ударом для репутації Block і може вплинути на довіру інвесторів та користувачів. Крім того, це створює прецедент, який регулятори можуть використовувати в майбутньому щодо інших компаній, які порушують правила ПВК.

Висновки та уроки для сфери фінансових технологій

- Необхідність посилення контролю. Подібні кейси демонструють, що недотримання стандартів ПВК та ФТ може призвести до серйозних фінансових втрат і втрату репутації.
- Інвестиції у технології моніторингу. Фінансові технологічні компанії повинні активно впроваджувати передові системи моніторингу транзакцій, що базуються на штучному інтелекті.
- Акцент на співпрацю з регуляторами. Компанії повинні не лише відповідати регуляторним вимогам, але й проактивно взаємодіяти з органами нагляду для вдосконалення своїх політик ПВК/ФТ.
- Навчання персоналу. Професійна підготовка співробітників є ключовою для забезпечення дотримання нормативних вимог.

Ця новина нагадує про критичну важливість відповідності законодавству у сфері ПВК/ФТ для всіх учасників фінансового ринку, особливо для тих, хто працює з інноваційними технологіями, які можуть бути вразливими до ризиків зловживань.

Як експортний контроль ставить під загрозу переваги Заходу у сфері військових технологій[16]

Стаття, опублікована на платформі Королівського Об'єднаного Інституту Оборонних Досліджень (RUSI), висвітлює проблематику експортного контролю та його вплив на військово-технологічну перевагу країн Заходу. Авторка звертає увагу на складну взаємодію між необхідністю захисту критично важливих технологій та ризиком створення додаткових перешкод для розвитку інновацій у військовій сфері. У сучасних умовах, коли технології є ключовим фактором у військових конфліктах, збереження доступу до новітніх розробок є стратегічно важливим. Експортний контроль спрямований на те, щоб перешкодити недружнім державам отримувати доступ до передових технологій, які можуть бути використані проти інтересів Заходу. Водночас надмірне регулювання може створити значні складнощі для компаній, які працюють у сфері високих технологій, особливо для малих та середніх підприємств.

[16] https://www.rusi.org/explore-our-research/publications/commentary/how-export-controls-endanger-wests-military-technology-advantage

Особливу увагу стаття приділяє останнім ініціативам Бюро промисловості та безпеки США (BIS), яке у жовтні 2024 року видало нові рекомендації для фінансових установ. Хоча ці рекомендації формально не мають статусу юридично обов'язкових норм, на практиці вони вимагають від банків та інших фінансових установ запроваджувати складні процедури для забезпечення відповідності новим правилам. Основною проблемою стає те, що банки часто не мають достатнього доступу до необхідної інформації про транзакції, зокрема про товари, кінцевих користувачів і їхнє призначення. Це створює значні виклики для прийняття обґрунтованих рішень щодо підтримки певних операцій.

Авторка також підкреслює, що зростаючі витрати на дотримання регуляторних вимог можуть стимулювати явище, відоме як «де-ризкінг». Фінансові установи, побоюючись ризиків або надмірного регуляторного тиску, можуть відмовлятися від обслуговування певних клієнтів або цілих секторів, які вважаються високоризиковими. У контексті оборонної промисловості ця ситуація особливо небезпечна для малих та середніх підприємств, які є основними джерелами інновацій та розвитку новітніх технологій. Великі оборонні підрядники можуть продовжувати отримувати доступ до фінансування, але менші компанії ризикують бути витісненими зі сфери через обмеження у фінансовій підтримці. Це може призвести до уповільнення розвитку нових технологій, які є життєво важливими для збереження військової переваги Заходу.

На думку авторки, такі наслідки можуть серйозно послабити позиції Заходу у військово-технологічній сфері. Вона закликає BIS переглянути свої підходи, зокрема до банківського сектора, щоб забезпечити кращий баланс між необхідністю захисту національної безпеки та підтримкою технологічного розвитку. Запропоновано вдосконалити взаємодію між державними установами та фінансовими організаціями для того, щоб створити більш ефективну, але менш обтяжливу систему експортного контролю.

Стаття є критичним аналізом складного питання, яке знаходиться на перетині інтересів національної безпеки, фінансових систем та інноваційної діяльності. Вона чітко демонструє, що навіть благі наміри, такі як захист передових технологій, можуть призводити до небажаних наслідків, якщо регуляторні підходи є недостатньо збалансованими. Авторка наголошує на необхідності перегляду існуючих практик, щоб уникнути довгострокових втрат у ключових секторах, від яких залежить стратегічна перевага Заходу.

Для загального розвитку

Розширення санкцій: ключові тенденції 2024 року та нові виклики на 2025 рік[17]

Стаття аналізує трансформацію санкцій як інструменту міжнародної політики та підкреслює нові виклики, які постають перед державами, бізнесом та міжнародними організаціями. Увага зосереджена на тому, як санкції, розширюючись, охоплюють нові сфери, зокрема технології, стратегічні ресурси та фінансові транзакції. Санкції перестають бути виключно економічним інструментом і перетворюються на комплексний механізм впливу, що включає вторинні санкції, обмеження у використанні новітніх технологій та цільові заходи щодо окремих галузей або осіб.

[17] https://www.linkedin.com/pulse/expanding-sanctions-landscape-key-trends-from-2024-gizem-fyp8e/?trackingId=WkEwXauzKX1JZSwk3BU5vQ%3D%3D

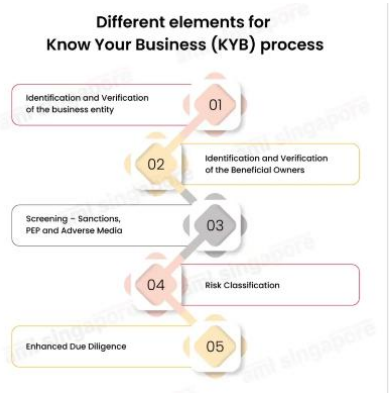
Зростаюча геополітична напруженість, особливо між США та Китаєм, а також військові конфлікти в різних регіонах світу сприяють активізації санкційних ініціатив. У статті підкреслюється, що конкуренція між державами у стратегічно важливих сферах, таких як рідкоземельні елементи або штучний інтелект, ускладнює узгодження санкцій на міжнародному рівні, водночас посилюючи їхній вплив на глобальну економіку. Впровадження санкцій часто супроводжується економічними потрясіннями для країн, які є об'єктами цих заходів, а також створює ризики для компаній, які змушені адаптуватися до складних умов міжнародного регулювання.

Стаття акцентує увагу на нових викликах для бізнесу, особливо у сфері дотримання міжнародних норм і забезпечення відповідності вимогам санкційного режиму. Глобальні корпорації стикаються зі зростанням витрат на моніторинг ризиків та необхідністю впровадження технологій для аналізу транзакцій і запобігання порушенням. З іншого боку, уряди мають посилювати інституційний потенціал для ефективного застосування санкцій та забезпечення прозорості фінансових потоків. У статті також підкреслюється роль новітніх технологій, таких як блокчейн і штучний інтелект, які можуть бути використані як для моніторингу транзакцій, так і для обходу санкційних обмежень.

Окремо виділяються прогнози щодо майбутнього санкцій у 2025 році. Передбачається, що вони стануть більш інтегрованими, цілеспрямованими та технічно складними, що потребуватиме як поглиблення міжнародної співпраці, так і розробки нових інструментів для управління ризиками. У статті робиться висновок, що ефективність санкцій залежить від їхньої адаптивності до змін у глобальній економіці, а також від здатності урядів і бізнесу впроваджувати інноваційні підходи до їх моніторингу та виконання.

Know Your Business: важливий елемент CDD[18]

Стаття на сайті AML Singapore підкреслює важливість процесу Know Your Business (KYB) як невід'ємної частини програми протидії відмиванню грошей. Автори зазначають, що KYB часто недооцінюється порівняно з процедурою Know Your Customer (KYC), хоча обидві є критичними для ідентифікації та верифікації клієнтів.



KYB спрямована на перевірку юридичних осіб, з якими фінансові установи та визначені нефінансові установи та професії (DNFBPs) встановлюють ділові відносини. Цей процес включає:

- Верифікацію особи компанії, включаючи її реєстраційні дані та місце діяльності.
- Оцінку характеру бізнес-діяльності та профілю компанії.
- Ідентифікацію осіб, які приймають бізнес-рішення від імені компанії.

Метою KYB є визначення, чи є юридична особа справжньою та не використовується як прикриття для відмивання коштів або інших фінансових злочинів. Зокрема, підкреслюється, що фіктивні компанії часто використовуються для легалізації незаконних коштів, проходячи через легальну фінансову систему під виглядом законної діяльності.

Процес KYB дозволяє регульованим організаціям переконатися в легітимності компанії, її реальному існуванні, а також отримати інформацію про історію компанії, здійснювані транзакції, джерела фінансування та фінансовий стан компанії.

[18] https://amlsingapore.com/know-your-business-an-critical-element-of-customer-due-diligence/

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-2025-04

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].