



“Роби все, що в твоїх силах. Більше не може зробити ніхто”

Джон Вуден

Мета

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

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

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

Звіти міжнародних організацій та окремих юрисдикцій



НОР Бахрейн 2025 ¹

THE KINGDOM OF BAHRAIN'S NATIONAL
RISK ASSESSMENT 2025
Public Version



Звіт про Національну оцінку ризиків (НОР) Королівства Бахрейн за 2025 рік є комплексною та структурованою самооцінкою, проведеною з метою оновлення попередніх оцінок (2017 та 2021 років) у світлі стрімкого технологічного розвитку та появи нових продуктів і послуг. Методологія дослідження ґрунтується на інструментарії Світового банку, включаючи спеціалізовані модулі для оцінки ризиків, пов'язаних з віртуальними активами, юридичними особами, неприбутковими організаціями та фінансуванням тероризму, і супроводжувалася активними консультаціями з державним та приватним секторами.

Ключовим елементом звіту є детальний аналіз загроз відмивання коштів. НОР ідентифікує «незаконний обіг наркотиків» та «шахрайство» як два найбільш значущі

¹ https://www.bahrainfiu.gov.bh/mcms-store/magazine/ar/risk_assessment-2025/index.html

предикатні злочини, що генерують основні обсяги злочинних доходів в країні. Практичні приклади (case studies) у звіті демонструють використання сучасних методів для відмивання цих коштів, зокрема P2P-переказів через постачальників послуг віртуальних активів (VASP) у справах про наркотики та використання схем відмивання через торгівлю (TBML) і мереж «Хавала» для відмивання доходів від предикатних злочинів, скоєних за кордоном.

У розрізі секторів, найвищий рівень ризику ВК («Середньо-Високий») присвоєно ключовим фінансовим інституціям: роздрібним та оптовим банкам, обмінним пунктам (Money Changers) та VASP. Водночас, ризики в секторі визначених нефінансових установ та професій (ВНУП) оцінені як помірніші. Наприклад, сектор юристів отримав «Середній» рівень ризику, тоді як сектори нерухомості та дилерів дорогоцінних металів (DPMS) оцінені як «Середньо-Низькі». Це значною мірою пояснюється впровадженням жорстких практичних заходів контролю, зокрема встановленням низьких порогів для готівкових розрахунків: заборонені готівкові операції на суму понад 2 000 бахрейнських динарів у секторі нерухомості та понад 3 000 динарів у секторі дорогоцінних металів, що змушує проводити високоцінні транзакції через регульовану банківську систему.

Оцінка ризиків зловживання юридичними особами та утвореннями є показовою. Ризик, пов'язаний з юридичними особами (компаніями), визначено як «Середній». Звіт визнає високу «привабливість для реєстрації компаній нерезидентами» як фактор вразливості, однак це компенсується надійними механізмами контролю, такими як централізований онлайн-реєстр «Sijilat» та суворі вимоги до розкриття кінцевих бенефіціарних власників. Правові утворення, такі як трасти та вакфи (Waqfs), отримали «Низький» рівень ризику завдяки суворому нагляду з боку Центрального банку (CBB) та Міністерства юстиції (MOJ) відповідно.

У другій частині звіту аналізуються ризики фінансування тероризму та фінансування розповсюдження зброї масового знищення. Загальний ризик ФТ в країні оцінено як «Середньо-Низький», що обґрунтовується наявністю потужної національної контртерористичної стратегії та ефективної системи впровадження цільових фінансових санкцій. Проте, VASP все ще вважаються сектором «Середньо-Високого» ризику у контексті ФТ. Ризик зловживання неприбутковими організаціями (НПО) оцінено як «Середній»; ключовим запобіжником тут є вимога до НПО отримувати попередній дозвіл від наглядового органу (MOSD) на будь-яку діяльність зі збору коштів та на всі транскордонні перекази. Ризик ФР визначено як «Низький», в основному через відсутність будь-яких зв'язків чи фінансових потоків з юрисдикціями високого ризику, такими як КНДР.

Висновки:

- Основними загрозами відмивання коштів визначено доходи від «незаконного обігу наркотиків» та «шахрайства». Для їх відмивання активно використовуються сучасні методи, зокрема P2P-перекази через VASP та платіжні додатки небанківських постачальників послуг.
- Найвищий сукупний ризик ВК («Середньо-Високий») сконцентрований у чотирьох ключових секторах: роздрібні банки, оптові банки, обмінні пункти та VASP.
- Ефективним практичним заходом для зниження ризиків у секторі ВНУП є запровадження жорстких низькопорогових обмежень на готівкові розрахунки. Зокрема, транзакції з нерухомістю на суму понад 2 000 BHD та купівля дорогоцінних металів на суму понад 3 000 BHD мають здійснюватися виключно через банківську систему.
- Для контролю за «Середнім» ризиком у секторі НПО впроваджено ключовий запобіжник: неприбуткові організації зобов'язані отримувати попередній дозвіл від регулятора (MOSD) на будь-яку діяльність зі збору коштів та на всі транскордонні грошові перекази.

Криптоактиви та децентралізовані фінанси. Звіт про стейблкоїни, криптоінвестиційні продукти та багатофункціональні групи²

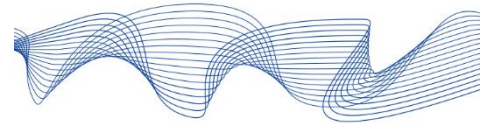
Документ Європейської Ради з Системних Ризиків висвітлює зростаючі ризики для фінансової стабільності, пов'язані з криптоактивами, стейблкоїнами, криптоінвестиційними продуктами (КІП) та багатофункціональними групами (БФГ). Зростання ризиків відбувається на тлі швидкого розширення ринку криптоактивів до рекордних оцінок, значною мірою підтримуваного політичними заходами США, спрямованими на зміцнення домінування долара. Зв'язки між сектором і традиційним фінансовим сектором посилюються, вимагаючи ретельного моніторингу.



Crypto-assets and decentralised finance

October 2025

Report on stablecoins, crypto-investment products and multi-function groups



Стейблкоїни, які розроблені для підтримки стабільної вартості щодо фіатної валюти або кошика активів, становлять значний ризик, особливо через їх швидке зростання та посилення зв'язків із традиційними фінансами через резервні активи. Загальна ринкова капіталізація стейблкоїнів досягла 300 мільярдів доларів США до вересня 2025 року, при цьому 99% ринку складають стейблкоїни, прив'язані до долара США. Основне використання стейблкоїнів залишається у сфері криптоеко системи як міст для переходу між фіатом і криптоактивами, а також як застава у децентралізованому фінансуванні. Всупереч широко поширеній увазі, їхня роль у глобальних платіжних системах залишається обмеженою (близько 0,2% світових транзакцій електронної комерції у 2024 році). Однак, їхній потенціал для широкого використання у платежах викликає занепокоєння щодо їхньої надійності та прозорості, особливо з огляду на їхню вразливість до операційних ризиків (включно з кібервразливістю) та можливості використання для незаконної діяльності, такої як відмивання грошей та ухилення від санкцій. Стейблкоїни, зокрема, не мають ключових властивостей надійних грошей, як-от єдність (singleness), еластичність (elasticity) та цілісність (integrity), що робить їх непридатними для великомасштабних платежів.

Ключовим викликом для фінансової стабільності ЄС є регуляторна фрагментація та неявна вразливість, що виникає через схеми мультиемітентів стейблкоїнів, які не були прямо передбачені Регламентом ЄС про ринки криптоактивів (MiCA). Така схема передбачає випуск ідентичного, взаємозамінного стейблкоїна (fungible stablecoin) установами в ЄС та третій країні (наприклад, США), при цьому резерви розподілені між юрисдикціями. Ця модель збільшує ризики для емітентів у ЄС, оскільки власники токенів, випущених у третій країні (де захист може бути слабшим, наприклад, дозволені комісії за викуп), можуть прагнути викупити токени через емітента в ЄС, де викуп має бути швидким та безкоштовним згідно з MiCA. Це може виснажити резерви ЄС, зробивши їх недостатніми для покриття зобов'язань перед власниками в ЄС та потенційно спричинивши нестабільність. Крім того, несанкціоновані стейблкоїни, особливо USDT (Tether), залишаються ризиком, оскільки їхній глобальний вплив може призвести до примусового продажу резервних активів (fire sales), таких як казначейські векселі США, у разі масового викупу, що опосередковано вплине на ЄС.

Криптоінвестиційні продукти (КІП) та Багатофункціональні групи (БФГ)

КІП (які включають, наприклад, біржові продукти — ETP) значно зросли (до 235 мільярдів доларів США станом на липень 2025 року), демонструючи інтеграцію індустрії у традиційні

² https://www.esrb.europa.eu/pub/pdf/reports/esrb.report202510_cryptoassets.en.pdf

фінанси та зростаючий інтерес інституційних та роздрібних інвесторів. Це зростання підсилює потенційні загрози фінансовій стабільності через ризики перетікання (spillovers) у традиційну фінансову систему.

Ключовим аспектом, що підвищує системний ризик, є висока концентрація ринку для основних криптопослуг, особливо послуг зберігання (custody). Три найбільші провайдери зберігання обслуговують близько 39% усіх КІП та 60% загальної ринкової капіталізації. Для продуктів із фізичним забезпеченням (physically backed CIPs) концентрація ще вища. Така концентрація створює вразливість: фінансові або операційні труднощі одного з цих ключових постачальників (наприклад, через кібератаки чи збої) можуть вплинути на широкий спектр КІП, посилити втрати інвесторів і мати ширший дестабілізуючий вплив на крипторинки, з потенційними негативними наслідками для традиційних фінансових ринків.

Багатофункціональні групи (БФГ) — це групи, які можуть пропонувати комплексні послуги (випуск, обмін, зберігання). Незважаючи на потенційні переваги (інновації, зниження витрат), ці групи створюють серйозні макропруденційні проблеми, зумовлені їхнім масштабом, централізацією та взаємопов'язаністю. Ризики включають: фінансову залежність усередині групи, операційні вразливості (особливо кіберзагрози, зважаючи на великі хаки, як-от Bybit та FTX), недоліки управління, нерегульовані конфлікти інтересів та репутаційні ризики. Справа FTX 2022 року наочно продемонструвала ризики міжгрупової взаємопов'язаності, злиття власних та клієнтських коштів, а також використання власних токенів як застави, що спричинило каскадний ефект ліквідації. Регуляторний нагляд ускладнюється через непрозорі корпоративні структури та транскордонний регуляторний арбітраж, особливо для небанківських БФГ, для яких практично відсутні консолідовані механізми нагляду на рівні групи. Це підриває здатність наглядових органів ідентифікувати та пом'якшувати макропруденційні ризики ex ante.

Висновки:

- **Негайне усунення лазівок мультиемітентів стейблкоїнів:** Провести формальний перегляд регуляторної бази МіСА з метою прямої заборони або встановлення суворих обмежень на схеми мультиемітентів за участю суб'єктів із третіх країн. Це необхідно для запобігання регуляторному арбітражу, захисту резервних активів, що зберігаються в ЄС, від вимог викупу, ініційованих власниками токенів із третіх країн.
- **Формалізація нагляду за небанківськими БФГ:** Терміново створити формалізовані міжвідомчі структури (за участю ЕВА, ESMA, ECB, NCAs та ESRB) для посилення наглядового діалогу та координації щодо небанківських багатофункціональних груп. У середньостроковій перспективі необхідно запровадити вимоги до звітності на рівні групи для БФГ для моніторингу ліквідності, левериджу, операційної стійкості та взаємозв'язків, особливо з огляду на їхню високу ринкову концентрацію.
- **Посилення управління операційними ризиками та даними:** З огляду на високу концентрацію в критично важливих криптопослугах, таких як зберігання, необхідно заповнити прогалини в даних, вимагаючи від небанківських фінансових установ та БФГ детальної звітності про їхні криптоактиви, КІП та взаємозв'язки з сектором. Це забезпечить необхідні кількісні дані для стрес-тестування та своєчасного виявлення ризиків, що виникають через операційні збої або кібератаки у ключових провайдерів.
- **Забезпечення застосування МіСА до несанкціонованих активів:** Компетентним органам слід повною мірою використовувати наявні повноваження МіСА, зокрема статтю 94, для заборони авторизованим CASP пропонувати будь-які регульовані послуги, пов'язані з несанкціонованими стейблкоїнами (наприклад, USDT). Крім того, необхідно вузько тлумачити винятки через суворе дотримання керівних принципів ESMA, щоб запобігти обходу вимог МіСА транскордонними фірмами.

Наявні регуляторні прогалини та недостатня звітність, особливо щодо обсягів левериджу (leverage) фінансових установ, криптоактивів, що утримуються небанківськими фінансовими установами, та інформації про контрагентські ризики, обмежують аналіз схильності фінансового сектору до крипторизиків. Хоча MiCA є важливим кроком вперед, необхідне посилення наглядових заходів, законодавчих реформ та тіснішої міжнародної співпраці для захисту від фінансових ризиків.

CBDC під мікроскопом: як знижки та комісії формують попит на нову форму грошей³



Документ присвячено глибокому аналізу потенційного попиту на роздрібну цифрову валюту центрального банку (CBDC) та чинників, які формують вибір користувачів між різними платіжними засобами. Дослідження має експериментальний характер і є однією з найдетальніших емпіричних спроб кількісно оцінити ймовірність використання CBDC на етапі до її реального

впровадження. Роботу виконано групою економістів із Сеульського національного університету та Університету Кореї за підтримки Банку Кореї та Банку міжнародних розрахунків (BIS).

Основна мета дослідження полягає у визначенні, які саме атрибути платіжних інструментів впливають на споживчі переваги та які характеристики CBDC забезпечили б її конкурентоспроможність порівняно з іншими формами платежів — готівкою, банківськими картками та мобільними сервісами. На відміну від більшості попередніх опитувань, що ґрунтувалися на гіпотетичних запитаннях про готовність користуватися CBDC, автори застосували метод дискретного вибору (DCE), який дає змогу виявити причинно-наслідкові зв'язки між характеристиками платіжного інструменту та ймовірністю його вибору. Дослідження охопило 3561 респондента, репрезентативних для дорослого населення Південної Кореї, які протягом онлайн-експерименту робили повторні вибори між парами гіпотетичних платіжних засобів. Кожен інструмент у парі мав унікальну комбінацію дев'яти атрибутів, випадково згенерованих таким чином, щоб уникнути кореляції між ними й забезпечити статистично чисту оцінку впливу кожного чинника. Серед досліджуваних атрибутів — емітент (центральный банк, приватна фінансова установа або BigTech-компанія), форма випуску (банкнота, пластикова картка або мобільний застосунок), рівень розкриття персональної інформації, ступінь прийняття торговцями, ризик втрати коштів, наявність знижки при використанні, затримка платежу, час остаточного розрахунку та щомісячна комісія. Така структура дала можливість відтворити реальні ринкові умови та змодельувати поведінку споживачів у випадку появи CBDC.

Отримані результати демонструють, що вибір платіжного засобу споживачами насамперед визначається фінансовими стимулами. Навіть незначна комісія, наприклад 5000 KRW на місяць (близько 3,5 долара США), зменшує ймовірність вибору методу на 14 відсоткових пунктів, тоді як наявність знижки при оплаті (3–5 %) підвищує ймовірність використання на 8–11 пунктів. Це свідчить, що економічні вигоди — головний рушій споживчої поведінки у платіжній сфері. Поряд із цим дослідники виявили, що нефінансові атрибути також мають значення, хоча їхній вплив помірніший. Перехід від готівкової форми до цифрової (застосунок або картка) підвищує ймовірність вибору приблизно на 7–8 пунктів, що підтверджує важливість зручності, швидкості та технологічності платіжного інструменту. Високий рівень прийняття торговцями (80–100 %) збільшує привабливість способу оплати на 5–7 пунктів, а низький ризик втрати коштів (1 % проти

³ <https://www.bis.org/publ/work1296.pdf>

10 %) — на 6 пунктів. Натомість фактори, пов'язані з приватністю, мають відносно слабший ефект: небажання розкривати персональні дані додає лише близько 2 пунктів до ймовірності вибору. Цікаво, що роль емітента не є вирішальною: платіж, емітований центральним банком, підвищує довіру лише на 2 пункти, а випуск BigTech-компаніями практично не впливає на вибір.

Щоб перевірити достовірність моделі, автори порівняли передбачені частки використання традиційних засобів платежу з фактичними статистичними даними Банку Кореї. Модель точно відтворила реальні співвідношення: приблизно 60 % припадає на кредитні та дебетові картки (реально — близько 70 %), 19 % — на мобільні платежі (реально — 15 %), решта — на готівку. Це підтвердило зовнішню валідність експерименту і дозволило використовувати оцінені переваги для прогнозування попиту на CBDC.

Далі дослідники змоделивали кілька сценаріїв дизайну гіпотетичної цифрової валюти центрального банку. У базовій конфігурації CBDC описується як інструмент, випущений центробанком у формі картки чи застосунку, без комісій і знижок, з часом транзакції до 10 секунд, негайним розрахунком, рівнем прийняття 80 % та повним розкриттям персональних і транзакційних даних. За таких умов CBDC обрали 19 % респондентів, що робить її другим за популярністю засобом платежу після карток і значно більш привабливою за готівку чи мобільні сервіси. Якщо додати дисконт у розмірі 3–5 %, частка зростає до 27 %, що свідчить про критичну роль фінансового стимулювання. Водночас обмеження розкриття персональної інформації (залишаючи анонімність або часткову ідентифікацію) підвищує попит лише на 0,6–1,6 пунктів — це демонструє, що приватність для користувачів важлива, але не визначальна, тоді як матеріальні вигоди значно сильніше формують попит.

Автори також провели додаткові симуляції, у яких приватні банки чи BigTech-компанії реагують на появу CBDC, знижуючи свої комісії або підвищуючи бонуси. Такі дії помітно зменшують привабливість CBDC — приблизно на 6 %, що підкреслює конкурентний характер платіжного ринку і те, що впровадження CBDC потребує продуманої політики стимулів, аби зберегти інтерес користувачів. Додаткові розрахунки із використанням моделі вкладеного логу (nested logit) підтвердили стійкість отриманих результатів і продемонстрували, що очікувана частка використання CBDC коливається від 15 % до 27 %, залежно від її дизайну.

Окрему увагу приділено соціально-демографічним відмінностям. Стать, рівень освіти та доходу не мають істотного впливу на вибір, натомість вік є важливим чинником. Молодші респонденти (19–39 років) демонструють вищу довіру до BigTech та більшу прихильність до мобільних додатків, тоді як старші (40–70 років) більш схильні до використання продуктів, емітованих центральним банком, і віддають перевагу картковому формату. Це означає, що прийняття CBDC може мати вікову сегментацію, а комунікаційна стратегія центральних банків має враховувати різні очікування поколінь.

Висновки:

- **Фінансові стимули — вирішальний чинник:** навіть невеликі знижки (3–5 %) різко підвищують ймовірність вибору CBDC; комісії, навпаки, істотно знижують попит.
- **CBDC здатен швидко замінити готівку:** за базового дизайну її потенційна частка становить 19 – 27 % — вище, ніж у мобільних платежів.
- **Конфіденційність має обмежений ефект:** зниження рівня розкриття даних збільшує попит лише незначно, що свідчить про домінування прагматичних мотивів над приватністю.
- **Вік користувачів — ключ до впровадження:** старші споживачі більше довіряють центробанку, тоді як молодші — технологічним компаніям; це вимагає сегментованих стратегій комунікації при запуску CBDC.

У висновках автори наголошують, що ймовірне впровадження CBDC не лише технологічне, але й поведінкове питання, у якому ключову роль відіграють стимули, довіра й практична зручність. Головними чинниками, що визначатимуть успіх цифрової валюти центрального банку, є економічна привабливість (знижки, відсутність комісій), функціональна зручність (швидкість, мобільність) і достатній рівень довіри до емітента. При цьому фактор приватності, попри його політичну значущість, має другорядне значення у виборі користувача. Робота BIS дає кількісні орієнтири для центральних банків, що готуються до запуску власних цифрових валют: щоб досягти суттєвого рівня прийняття, CBDC повинна конкурувати з комерційними платіжними інструментами не лише безпекою та надійністю, а передусім економічними вигодами та користувацьким досвідом, які визначають повсякденну поведінку споживачів у платіжній екосистемі.

Еволюція реагування на інциденти: як NIST SP 800-61r3 змінює підхід до кіберризиків ⁴

Документ є фундаментальним оновленням класичного посібника NIST щодо реагування на кіберінциденти. Ця редакція не просто модернізує підходи до реагування на кіберінциденти (IR), а



концептуально переосмислює його роль у ширшому контексті управління кіберризиками. Якщо попередні версії (зокрема SP 800-61r2 від 2012 року) акцентувалися на технічних етапах реагування, то NIST SP 800-61r3 інтегрує IR у структуру NIST Cybersecurity Framework 2.0 (CSF 2.0), що є основою сучасної моделі управління кібербезпекою для організацій будь-якого типу. У центрі уваги цього документа — перехід від реактивного до проактивного підходу, від розрізнених технічних заходів до цілісної, керованої ризиками системи, де реагування на інциденти є постійним і невід’ємним процесом, а не ізольованою діяльністю окремої команди.

Документ пояснює, що у сучасних умовах, коли кількість інцидентів зростає, їхня складність поглиблюється, а відновлення триває тижні або місяці, традиційна модель «підготовка – виявлення – аналіз – усунення – відновлення» вже не відповідає реальності. Натомість пропонується новий життєвий цикл реагування на інциденти, побудований на шести функціях CSF 2.0: *Управління, Ідентифікація, Захист, Виявлення, Реагування та Відновлення*. Кожна з них відіграє ключову роль у забезпеченні безперервності управління ризиками. Функції *Управління, Ідентифікації та Захисту* допомагають запобігати інцидентам, готуватися до них, мінімізувати наслідки та покращувати внутрішні політики, тоді як *Виявлення, Реагування та Відновлення* спрямовані на оперативне виявлення атак, їхнє стримування, усунення наслідків і повернення систем до нормального стану. Усі ці елементи об’єднує принцип постійного вдосконалення, який визначає, що уроки, отримані під час кожної події, повинні використовуватися для коригування політик, процедур і навчальних програм, щоб підвищувати стійкість організації до майбутніх загроз.

Велика увага приділяється питанням ролей та відповідальності у процесі реагування на інциденти. NIST підкреслює, що у сучасній екосистемі кібербезпеки реагування більше не є виключною функцією окремої команди (CSIRT). Успіх IR залежить від узгоджених дій багатьох суб’єктів: керівництва, яке приймає стратегічні рішення та виділяє ресурси; аналітиків і технічних спеціалістів, які здійснюють діагностику та усунення загроз; юридичного відділу, який забезпечує відповідність вимогам законодавства та договірних зобов’язань; фахівців з

⁴ <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r3.pdf>

комунікацій, які координують взаємодію із громадськістю, клієнтами й ЗМІ; підрозділів з управління персоналом, що працюють із внутрішніми інцидентами; та зовнішніх партнерів — постачальників послуг, провайдерів хмарних рішень, державних органів і правоохоронних структур. Такий розподіл формує модель спільної відповідальності, у якій кожна сторона має визначені контрактом обов'язки, межі дій, процедури інформування та узгоджені канали комунікації. NIST наголошує, що успішне реагування можливе лише за наявності формалізованої системи координації всіх учасників, що ґрунтується на чітких політиках, процедурах та обміні інформацією у режимі реального часу.

Особливе місце у документі займає розроблення політик, процесів і процедур реагування на інциденти. NIST рекомендує кожній організації затвердити офіційну політику IR, яка включає зобов'язання керівництва, визначення ключових термінів (подія, інцидент, загроза, компрометація), процедури ескалації, критерії пріоритетності, правила взаємодії між підрозділами та метрики ефективності. У межах політик мають бути визначені повноваження щодо відключення систем, конфіскації обладнання чи зупинки сервісів у разі інциденту. Рекомендовано створювати плейбуки — покрокові сценарії дій для типових ситуацій (наприклад, злам облікових записів, зараження програмою-зливником (ransomware), компрометація постачальника тощо), які суттєво підвищують швидкість і точність реагування.

Ключова частина публікації представлена у вигляді CSF 2.0 Community Profile, тобто систематизованого набору рекомендацій і практичних орієнтирів, згрупованих за функціями, категоріями та підкатегоріями CSF. Цей профіль є базовою моделлю, яку організації можуть адаптувати під власні потреби. Він поділений на дві великі частини: Підготовка і уроки та Реагування на кіберінциденти. Кожен елемент профілю містить рівень пріоритетності (високий, середній або низький) і набір рекомендацій (R), зауважень (C) чи приміток (N). Серед ключових рекомендацій у блоці *Управління* наголошується на необхідності інтеграції вимог щодо реагування у загальну політику кібербезпеки, документуванні ролей і повноважень, регулярному перегляді стратегії управління ризиками з урахуванням минулих інцидентів, а також включенні постачальників до планування та навчальних заходів. У частині Ідентифікація пріоритетами є автоматизація інвентаризації активів, моніторинг «shadow IT», ведення каталогів даних із класифікацією критичності, отримання та використання розвідки кіберзагроз (Cyber Threat Intelligence, CTI), а також побудова процесів оцінки уразливостей і ризиків на основі реальних атак і TTPs супротивників.

У блоці *Захист* документ акцентує увагу на значенні систем резервного копіювання, журналювання (логування), контролю доступу, безпечної розробки ПЗ та навчання персоналу. Особливо підкреслюється роль логів у виявленні та розслідуванні інцидентів, а також необхідність інтеграції практик безперервного тестування безпеки у життєвий цикл продуктів і послуг. Функція *Виявлення* описує механізми безперервного моніторингу, які охоплюють мережеві події, поведінку користувачів, активність постачальників і стан систем. NIST рекомендує застосовувати автоматизовані рішення SIEM, SOAR, кореляцію даних із CTI та постійне зменшення кількості хибнопозитивних і хибнонегативних спрацьовувань. У межах *Реагування* описуються найважливіші елементи керування інцидентом: тріаж, пріоритизація, категоризація, координація з третіми сторонами, розподіл ролей і відстеження статусів через квиткові системи. Завершальний етап *Відновлення* пов'язаний із відновленням бізнес-процесів, тестуванням резервних систем і синхронізацією планів безперервності бізнесу з політиками інцидент-менеджменту.

У ширшому контексті NIST SP 800-61r3 демонструє перехід від вузькотехнічного підходу до екосистемного управління кіберінцидентами, де поєднуються люди, процеси, технології та управлінські практики. Документ наголошує на потребі у міжорганізаційному обміні інформацією, участі у форумах з обміну розвідданими, використанні відкритих стандартів для сумісності даних (зокрема у рамках Cybersecurity and Privacy Reference Tool — CPRT), а також

Висновки:

- **Інцидент-менеджмент = невід’ємна частина управління ризиками.** Організації повинні розглядати реагування на інциденти не як технічну реакцію, а як постійний процес у межах усіх CSF 2.0 функцій — від *Управління до Відновлення*.
- **Впровадження безперервного циклу вдосконалення.** Уроки, отримані під час будь-якого етапу CSF, мають системно оновлювати політики, процедури й тренінги. Рекомендовано формалізовані огляди «lessons learned» після кожного інциденту.
- **Автоматизація та інтеграція даних (СТІ, SIEM/SOAR, CPRT).** Для скорочення часу реагування потрібно поєднати технічні засоби моніторингу, аналітику загроз і централізоване керування інцидентами. Це підвищує точність виявлення й швидкість реагування.
- **Юридична, організаційна та комунікаційна готовність.** Ефективна реакція можлива лише за наявності чітких повноважень, контрактних зобов’язань, визначених ролей і відпрацьованих сценаріїв взаємодії із зовнішніми сторонами (постачальники, CSP, ЗМІ, правоохоронці).

інтеграції заходів реагування із управлінням ризиками постачальників. Велика увага приділяється практичним аспектам — необхідності тестування планів, проведення навчань, аудитів, залучення третіх сторін для незалежної оцінки та створення умов для оперативного виявлення і локалізації загроз.

Таким чином, NIST SP 800-61r3 утверджує новий стандарт мислення у сфері кібербезпеки, де реагування на інциденти не є фінальним етапом, а постійним процесом, який живить систему управління ризиками інформацією, аналітикою та досвідом. Документ надає універсальну рамку для побудови адаптивних програм IR, сумісних з CSF 2.0, SP 800-53 та іншими нормативними документами NIST. Його цінність полягає не лише у структурі рекомендацій, а й у формуванні цілісного підходу до підготовленості організацій, що дозволяє скорочувати наслідки інцидентів, мінімізувати втрати, підвищувати ефективність реагування та забезпечувати довгострокову кіберстійкість.

Південно-Східна Азія як полігон злочинних інновацій: виклики штучного інтелекту для безпеки⁵



Звіт Управління ООН з наркотиків і злочинності (UNODC) є глибоким аналітичним документом, який досліджує злиття технологічних інновацій із кримінальною діяльністю, фокусуючись на тому, як автоматизація та штучний інтелект (AI) змінюють характер і масштаб злочинності в Південно-Східній Азії та Тихоокеанському регіоні. Документ демонструє, що регіон став епіцентром технологічно вдосконаленої злочинності, де злочинні мережі не просто адаптуються до цифрової епохи, а активно формують її правила, використовуючи автоматизовані та інтелектуальні інструменти для розширення своїх операцій, обходу контролю та приховування фінансових слідів.

Автори наголошують, що автоматизація перетворила кіберзлочинність із локалізованої діяльності окремих хакерів на транснаціональні системи, які діють за принципом

⁵ https://www.unodc.org/roseap/uploads/documents/Publications/2025/UNODC_Report_Emerging_threats_-_The_intersection_of_criminal_and_technological_innovation_in_the_use_of_automation_and_AI.pdf

промислового виробництва. У Південно-Східній Азії ця тенденція особливо відчутна: регіон став осередком масштабних «кібершахрайських колоній» — кримінальних комплексів, де кіберзлочини поєднуються з торгівлею людьми для примусової злочинної діяльності. Саме тут відбувається перехрестя між класичними формами злочинності — шахрайством, вимаганням, торгівлею людьми — та новітніми цифровими технологіями. У таких операціях автоматизація виступає не лише як інструмент прискорення злочинних дій, але й як засіб масштабування, який дозволяє атакувати тисячі жертв одночасно без участі людини.

Документ детально описує технічну сторону автоматизованих кіберзлочинів. Фішинг — найпоширеніший інструмент кіберзлочинців — набув нових масштабів завдяки «phishing-as-a-service» платформам на кшталт 16shop, які дозволяють навіть непідготовленим користувачам створювати реалістичні копії сайтів Apple, Amazon чи PayPal, автоматично надсилаючи мільйони електронних листів і SMS із шкідливими посиланнями. Такі сервіси, вартістю лише кілька десятків доларів, фактично «демократизували» кіберзлочинність, знявши технічні бар'єри для участі. Паралельно розвиваються ботнети — мережі заражених пристроїв, що діють як армії під контролем операторів. Прикладом є ботнет Mirai, який використовував уразливі IoT-пристрої для запуску атак обсягом у терабіти даних на секунду, причому значна частина заражених пристроїв розташовувалася саме в Південно-Східній Азії.

Розділ, присвячений автоматизованому відмиванню коштів, показує, як злочинці використовують ботів для масового створення «мулевих» рахунків, автоматичного заповнення онлайн-форм і завантаження підроблених документів. Системи штучного інтелекту дозволяють таким ботам проходити процедури KYC, а потім здійснювати мікротранзакції («smurfing») з метою конвертації коштів у криптовалюту або проведення через міксери, які знищують слід транзакцій. Таким чином, відмивання коштів стає настільки автоматизованим, що одна людина може контролювати сотні рахунків, а обсяги нелегальних потоків грошей сягають мільярдів доларів.

Окремий акцент у звіті зроблено на кримінальному використанні штучного інтелекту, який стає не просто інструментом, а каталізатором нової епохи злочинності. Найбільш небезпечним напрямом є створення та поширення «дівфейків» — синтетичних зображень, відео та аудіо, що імітують зовнішність або голос реальних людей. У звіті наведено низку реальних випадків, зокрема гучний інцидент у Гонконзі, де працівник компанії переказав понад 25 мільйонів доларів після участі у відеоконференції з підробленим «керівником», створеним за допомогою дівфейку. Подібні схеми стрімко поширюються в регіоні, охоплюючи Сінгапур, Малайзію, Таїланд і В'єтнам. Також фіксується нова форма сексуального шантажу за допомогою AI, у якій злочинці генерують фальшиві еротичні зображення жертв — переважно жінок і дітей — і вимагають гроші за нерозповсюдження контенту.

Звіт виявляє також системну тенденцію до використання генеративних моделей і «взламаних» LLM (large language models) для написання шкідливого коду. Зокрема, у Японії було зафіксовано перші арешти підлітків за створення шкідливих скриптів за допомогою ChatGPT та інших генеративних моделей. Злочинці навчаються обходити етичні бар'єри моделей через техніку «jailbreaking», у результаті чого створюють власні безконтрольні інструменти типу WormGPT, призначені для генерування фішингових листів, шпигунського та шифрувального ПЗ. Паралельно AI використовується у створенні самонавчальних вірусів, які адаптуються до середовища, приховують шкідливий код у законних програмах і активуються лише за наявності певних біометричних або геолокаційних ознак жертви. Такі підходи, як доводить прототип IBM DeepLocker, роблять виявлення зараження майже неможливим.

Ще одним проявом технологічної злочинної еволюції є AI-підсилений шантаж і соціальна інженерія. Завдяки генеративним моделям злочинці можуть створювати багатомовні листи, що ідеально імітують корпоративну комунікацію, або телефонні дзвінки із голосами керівників

компаній, згенерованими на основі відкритих записів. Це підвищує успішність атак типу ВЕС (Business Email Compromise) у десятки разів. Додатково, штучний інтелект дозволяє шахрайським центрам вести одночасно сотні розмов у різних месенджерах, автоматично перекладати та адаптовувати повідомлення під мову й культуру жертви. Зокрема, у Таїланді у 2024–2025 роках поліція ліквідувала масштабні центри, де використовували систему AIFace для реального накладання облич поліцейських на злочинців у відеодзвінках, що створювало ілюзію законності.

Описані тенденції показують, що AI почав проникати навіть у сфери маскуванню злочинців і уникнення правосуддя. У доповіді наведено приклади, коли злочинні групи використовують системи розпізнавання облич і аналітику соціальних мереж для відстеження дій правоохоронців або конкурентів, а також створюють фальшиві паспорти та посвідчення особи для обходу процедур KYC. У перспективі це може повністю підірвати ефективність ідентифікаційних механізмів у фінансовому секторі, адже синтетичні особистості стають настільки реалістичними, що банки можуть неусвідомлено відкривати рахунки для неіснуючих клієнтів.

У заключних розділах UNODC наголошує, що Південно-Східна Азія фактично перетворилася на лабораторію для тестування кримінальних технологій. Недосконалість нормативної бази, слабкі системи нагляду, висока цифрова активність населення та легкий доступ до дешевих технологій створили сприятливе середовище для злочинних експериментів. Водночас ці процеси вже виходять за межі регіону, поширюючись у Тихоокеанському басейні та впливаючи на глобальну безпеку. UNODC закликає уряди та правоохоронні структури до створення спільної системи раннього виявлення загроз, розвитку національних центрів з аналізу штучного контенту, інвестування у технології розпізнавання дідфейків, цифрове маркування (watermarking) та міжнародний обмін інформацією про інциденти. Без координаційних дій, попереджають автори, регіон ризикує стати не лише майданчиком для відпрацювання злочинних схем, але й джерелом експорту технологічно вдосконалених злочинних практик у глобальний простір.

Висновки:

- **AI-злочинність стає системною та масштабованою.** Інтеграція AI і автоматизації перетворила кіберзлочинність на промисловий сектор із власною інфраструктурою, сервісами й бізнес-моделями.
- **Гібридизація злочинних схем.** Традиційні шахрайства поєднуються з торгівлею людьми, фінансовими махінаціями та кібершпигунством, що створює «конвергентну» кримінальну екосистему.
- **Регуляторні прогалини й технологічна асиметрія.** Швидкість упровадження AI злочинцями значно перевищує темпи розробки нормативного контролю; діючі механізми KYC, CDD і моніторингу вже стають неефективними.
- **Необхідність нової архітектури реагування.** Регіональні уряди й фінансові установи мають інвестувати в інструменти виявлення дідфейків, аналітику даних, а також у програми міжнародного обміну розвідданими між правоохоронними органами.

Таким чином, звіт UNODC демонструє нову епоху злочинності, у якій штучний інтелект і автоматизація стали не просто допоміжними інструментами, а структурними елементами злочинного бізнесу, що створює безпрецедентні виклики для урядів, фінансових установ і суспільства в цілому.

Санкції

19-й Пакет санкцій ЄС проти росії⁶



Рада Європейського Союзу ухвалила 19-й пакет обмежувальних заходів проти російської федерації 23 жовтня 2025 року, після того, як остання держава-член, а саме Словаччина, зняла свої застереження, отримавши необхідні запевнення від Європейської Комісії. Цей пакет є відповіддю на ескалацію агресії росії проти України, зокрема на жорстокі військові кампанії, спрямовані проти цивільної інфраструктури, включаючи енергетичні, водні та медичні об'єкти. Головною метою є подальше

послаблення здатності кремля фінансувати війну, націлюючись на ключові сектори, такі як енергетика, фінанси та військово-промисловий комплекс (ВПК).

I. Обмеження в енергетичному секторі та боротьба з "тіньовим флотом"

Посилення тиску на російський енергетичний сектор є одним із центральних елементів 19-го пакета.

1. Заборона на імпорт зрідженого природного газу (ЗПГ): Впроваджується заборона на імпорт, купівлю або передачу російського ЗПГ до ЄС. Ця заборона набуде чинності поетапно: для короткострокових контрактів — протягом шести місяців, а для довгострокових контрактів — з 1 січня 2027 року. Зазначається, що повна заборона для довгострокових контрактів набуде чинності на рік раніше, ніж передбачалося у початковому плані Комісії.

2. Посилення контролю над нафтовими гігантами та обходом санкцій: Пакет значно посилює існуючу заборону на транзакції щодо двох великих російських державних нафтовиробників: "Роснефть" (Rosneft) та "Газпром Нефть" (Gazprom Neft). Скасовано винятки, які раніше дозволяли цим компаніям імпортувати нафту та газ до ЄС, за винятком транзиту нафти або нафтопродуктів, що походять із третіх країн, або нафти, що відповідає механізму граничної ціни на нафту (Oil Price Cap). Крім того, під санкції потрапляє ТОВ "Ядран-Груп" (LLC Yadran-Group), татарстанський конгломерат, що працює в російському нафтовому секторі, оскільки цей сектор є значним джерелом доходу для уряду рф.

3. Удар по "тіньовому флоту" та його помічникам: Для протидії обходу механізму граничної ціни на нафту та іншим незаконним морським операціям, що використовують нерегулярні та високоризикові практики судноплавства, було додано 117 додаткових суден до списку. Загальна кількість суден у "тіньовому флоті", на які поширюється заборона на доступ до портів ЄС та надання широкого спектру послуг, досягла 557.

Санкції також націлені на ключових посередників "тіньового флоту":

- Litasco Middle East DMCC (Дубай, ОАЕ), дочірня компанія "Лукойла", що сприяє діяльності "тіньового флоту".

⁶ <https://www.consilium.europa.eu/en/press/press-releases/2025/10/23/19th-package-of-sanctions-against-russia-eu-targets-russian-energy-third-country-banks-and-crypto-providers/>

- Морські реєстри (наприклад, Aruba Maritime Administration & Offshore Company Registry, International Maritime Ship Registry, MSTA-International Maritime Registries & Regulatory Inc.), які надають суднам фальшиві прапори, створюючи шахрайське враження дотримання вимог сертифікації.
- Також запроваджено заборону на перестраховання суден, які належать до "тіньового флоту".

4. Санкції щодо третіх країн в енергетиці: Щоб перекрити потоки доходів, чотири організації, пов'язані з нафтовою промисловістю Китаю, були включені до списку. Серед них дві нафтопереробні заводи (Liaoyang Petrochemical Company та Shandong Yulong Petrochemical Co., Ltd.) та одна торгова компанія (Chinaoil (Hong Kong) Corporation Limited), які є значними покупцями російської сирої нафти.

Ці енергетичні заходи доповнюються повною забороною на купівлю, імпорт або передачу всіх ациклічних вуглеводнів.

II. Посилення фінансових обмежень та фокус на криптоактивах

Фінансові заходи в 19-му пакеті демонструють значний розвиток, особливо у сфері боротьби з обходом санкцій через криптоактиви та іноземні фінансові системи.

1. Банки та платіжні системи:

- П'ять додаткових російських банків (Istina, Zemsky Bank, Commercial Bank Absolut Bank, MTS Bank та Alfa-Bank) були додані до транзакційної заборони, що означає заборону будь-яких прямих чи опосередкованих транзакцій для операторів ЄС.
- Запроваджено заборону на використання російської національної платіжної системи "Mir" (Mir) та Системи швидких платежів (SBP).
- Запроваджено заборону на транзакції щодо восьми банків та нафтотрейдерів з Таджикистану, Киргизстану, ОАЕ та Гонконгу.
- Чотири банки з Білорусі та Казахстану (VTB Bank (Kazakhstan), CJSC Alfa-Bank (Belarus), OJSC Sber Bank (Belarus) та VTB Bank (Belarus)) також підпали під транзакційну заборону через їхній зв'язок з російськими фінансовими та платіжними системами.

2. Санкції проти криптовалют та фінтех-послуг: Вперше введено повноцінні санкції проти стейблкоїну A7A5, який підтримується рублем.

- Санкції накладено на розробника, киргизького емітента (LLC Old Vector) та оператора великої торгової платформи (Grinex), що торгує A7A5.
- Транзакції за участю A7A5 на території ЄС заборонені.

Цей крок має на меті закрити лазівки, оскільки A7A5 був створений за підтримки російської держави (частково належить ПСБ Банку (PSB Bank)). Операторам ЄС заборонено надавати крипто-послуги та певні фінтех-послуги, які дозволяють росії розвивати власну фінансову інфраструктуру та обходити санкції.

III. Військово-промисловий комплекс (ВПК) та торговельні обмеження

Пакет містить посилені заходи, спрямовані на руйнування російського ВПК та припинення постачання критично важливих товарів.

1. Розширення списку суб'єктів ВПК: Додано 45 нових юридичних осіб, які підтримують російський військовий та промисловий комплекс або залучені до обходу експортних обмежень. 17 з цих організацій розташовані у третіх країнах: 12 у Китаї (включно з Гонконгом), 3 в Індії та 2 у Таїланді. Ці суб'єкти сприяють обходу обмежень на експорт верстатів з числовим програмним

керуванням (ЧПК), мікроелектроніки, безпілотних літальних апаратів (БПЛА) та інших передових технологічних виробів.

2. Обмеження на експорт товарів подвійного призначення: Розширено заборону на експорт, включивши додаткові товари, які можуть сприяти військовому та технологічному посиленню росії:

- Додано електронні компоненти та далекоміри.
- Включено додаткові хімічні речовини, що використовуються для виготовлення металевих зарядів, а також додаткові метали, оксиди та сплави.
- Посилені експортні обмеження стосуються також товарів, що підвищують промисловий потенціал, таких як солі та руди, вироби з гуми, труби, шини, жорна та будівельні матеріали.

3. Золотодобувна промисловість: Під санкції потрапив найбільший російський золотодобувний виробник — ПАТ "Полюс" (PJSC Polyus), що обмежує значне джерело доходів для уряду рф.

IV. Заходи щодо протидії обходу санкцій та обмеження на СЕЗ

Пакет включає потужні механізми для боротьби з обходом санкцій, особливо через певні географічні та економічні інструменти, що використовуються росією.

1. Обмеження на Спеціальні економічні зони (СЕЗ): Вводиться заборона на набуття нової участі або продовження існуючої участі у власності чи контролі, створення нових спільних підприємств, фінансування та укладення нових контрактів з підприємствами, зареєстрованими або діючими у певних російських СЕЗ. Особливо суворі обмеження застосовуються до СЕЗ "Алабуга" (Alabuga) та "Технополіс Москва" (Technopolis Moscow), вимагаючи відчуження (divestment) існуючих контрактів та участі до 25 січня 2026 року. Це відображає задокументовану участь цих зон у діяльності, що сприяє військовим зусиллям. На інші СЕЗ (Липецьк, Тольятті, Сколково, Вільний порт Владивосток тощо) поширюється заборона на нову участь та фінансування.

2. Обмеження на порти третіх країн: Розширено заборону на транзакції, включивши будь-які порти та шлюзи в третіх країнах, які використовуються для:

- Передачі БПЛА, ракет або пов'язаних технологій до росії.
- Обходу механізму граничної ціни на нафту через нерегулярні та високоризикові практики судноплавства.

V. Обмеження на послуги та дипломатичну діяльність

Пакет вводить суворі обмеження на надання високотехнологічних та професійних послуг, а також посилює контроль за пересуванням російських дипломатів.

1. Обмеження на цифрові та технологічні послуги: ЄС обмежує доступ російських суб'єктів до передових цифрових можливостей:

- Послуги штучного інтелекту (AI), що включають доступ до моделей або платформ для їхнього навчання та використання.
- Послуги високопродуктивних обчислень та квантових обчислень.
- Комерційні космічні послуги, що включають спостереження Землі або супутникову навігацію.
- Розширено сферу обмежень на інженерно-технічні та наукові консультаційні послуги (наприклад, геологічна розвідка та картографування).

2. Посилений нагляд за послугами (Prior Authorisation): Введено нову вимогу попереднього дозволу компетентного органу для будь-яких послуг, що надаються уряду росії (і які не підпадають під пряму заборону). Це забезпечує суворий контроль та нагляд, щоб запобігти

використанню послуг для підтримки військового, технологічного чи промислового потенціалу рф.

3. Обмеження туристичних та інших послуг: Заборонено європейським операторам надавати послуги, безпосередньо пов'язані з туристичною діяльністю в росії (наприклад, послуги туристичних агентств та туроператорів). Це спрямовано на скорочення доходів росії та стримування несуттєвих поїздок до РФ.

4. Обмеження для російських дипломатів: Для протидії ворожій розвідувальній діяльності та підвищення обізнаності держав-членів ЄС запроваджено:

- Обов'язок попереднього інформування (мінімум за 24 години) для російських дипломатів, консульських працівників та їхніх сімей про намір подорожувати або прямувати транзитом через Шенгенську зону за межами країни своєї акредитації.
- Держави-члени ЄС також можуть запровадити вимогу авторизації для таких поїздок.

VI. Права людини та заходи щодо Білорусі

Пакет також посилює увагу до порушень прав людини, зокрема депортації дітей, та розширює санкції щодо Білорусі за її співучасть.

1. Відповідальність за злочини проти дітей: Запроваджено новий критерій для включення до санкційного списку осіб, відповідальних за дії або політику, що сприяють депортації, насильницькому переміщенню, насильницькій асиміляції, включаючи індоктринацію, або мілітаризованій освіті українських дітей. До списку додано 11 осіб, причетних до цих дій. Серед них — уповноважені з прав дитини в регіонах рф (наприклад, Світлана Адаменко, Костянтин Домогацький, Надія Болтенко) та посадові особи окупаційних адміністрацій. Також включено особу, відповідальну за нелюдське поводження з українськими військовополоненими (Ілля Сорокін, "Dr Evil").

2. Санкції щодо Білорусі: Введено п'ять нових суб'єктів, пов'язаних з білоруським ВПК та режимом Лукашенка. Це, зокрема, ICT Horizont та Horizont Holding, які розробляють товари подвійного призначення (наприклад, відеопристрої для бронетехніки) та співпрацюють із Міністерством оборони Білорусі. Заходи "віддзеркалюють" (mirrors) положення щодо росії, включаючи:

- Розширення експортних обмежень на товари, що можуть сприяти військовому та технологічному посиленню Білорусі (електронні компоненти, далекоміри, хімічні речовини, метали, руди та будівельні матеріали).
- Заборону на надання послуг у сфері ПЗ для банківського сектора, комерційних космічних послуг, ШІ та квантових обчислень.
- Обмеження на надання крипто- та платіжних послуг білоруським суб'єктам.

Цей пакет, що охоплює 69 індивідуальних санкцій та численні економічні заходи, є рішучим кроком Євросоюзу, спрямованим на подальше зростання економічних витрат росії та Білорусі, ускладнюючи фінансування їхньої агресивної політики.

Санкції США проти російської нафти ⁷

Обмеження були оголошені Управлінням контролю за іноземними активами (OFAC) Міністерства фінансів США 22 жовтня 2025 року, після того, як Президент Дональд Трамп обрав «середній» пакет санкційних заходів, які тривалий час були в готовності. Рішення про запровадження санкцій, згідно з офіційними заявами, було зумовлене відсутністю «серйозної

⁷ <https://home.treasury.gov/news/press-releases/sb0290>

прихильності росії до мирного процесу» та небажанням кремля припинити війну в Україні. Секретар Міністерства фінансів США Скотт Бессент заявив, що це сигнал кремлю з вимогою «припинити вбивства та негайно оголосити про припинення вогню».

Санкції спрямовані на посилення тиску на енергетичний сектор росії та зниження здатності кремля отримувати доходи для фінансування своєї військової машини. «Роснефть» та «Лукойл» були включені до списку санкцій відповідно до Указу Президента № 14024 (Е.О. 14024) за діяльність в енергетичному секторі Російської Федерації. Під обмеження потрапили обидві компанії, які є вертикально інтегрованими енергетичними компаніями, що займаються



видобутком, переробкою, транспортуванням та продажем нафти й газу. Крім того, санкції автоматично поширюються на всі дочірні компанії, зареєстровані в Росії, а також на будь-які організації, які прямо чи опосередковано на 50% або більше належать «Роснефти» чи «Лукойлу», навіть якщо вони не названі окремо OFAC. Серед дочірніх компаній, перелічених в Додатку 1, знаходяться численні нафтопереробні заводи та підприємства з видобутку нафти й газу в росії, включаючи «Лукойл Перм», «Лукойл Калінінградморнафта», а також різні підрозділи «Роснефті», такі як «Башнефть Добыча», «РН Туапсинський НПЗ» та інші.

З точки зору ПВК/ФТ, ключовим аспектом є те, що всі активи та інтереси в активах заблокованих осіб, які перебувають у США або під контролем осіб США, блокуються і про них необхідно повідомляти OFAC. Загалом, американським особам забороняється здійснювати будь-які операції з цими заблокованими активами. Міністерство фінансів США особливо наголосило на ризику вторинних санкцій для іноземних фінансових установ, які свідомо проводять значні операції або надають послуги від імені заблокованих осіб, а також для тих, хто підтримує російську військово-промислову базу. Порушення цих санкцій може призвести до цивільно-правової або кримінальної відповідальності як для осіб США, так і для іноземних осіб.

Для мінімізації негативних наслідків та забезпечення керованого припинення ділових відносин OFAC видало кілька Загальних ліцензій (General Licenses):

1. Загальна ліцензія № 126 дозволяє згортання (wind-down) будь-яких транзакцій із заблокованими «Роснефть» або «Лукойл» та їхніми дочірніми компаніями до 21 листопада 2025 року. При цьому будь-які платежі на користь заблокованої особи мають бути внесені на заблокований рахунок.
2. Загальна ліцензія № 127 дозволяє відчуження або передачу боргових зобов'язань, акцій або похідних фінансових інструментів («Covered Debt or Equity») «Роснефті» або «Лукойлу» на користь осіб, які не є особами США, також до 21 листопада 2025 року.
3. Загальна ліцензія № 128 спеціально дозволяє операції, необхідні для підтримки, експлуатації або згортання діяльності роздрібних автозаправних станцій «Лукойлу», розташованих за межами росії, також до 21 листопада 2025 року.
4. Загальна ліцензія № 124A дозволяє операції, пов'язані з проектами Каспійського трубопровідного консорціуму (КТК) та Тенгізшевройл (Tengizchevroil), навіть якщо в них задіяні заблоковані «Роснефть» або «Лукойл».

Санкції вже спричинили значні ринкові зміни. Для Китаю та Індії, які є найбільшими покупцями російської нафти, виникає ризик втрати доступу до західних банків та участі у ключових проектах на світових товарних ринках, якщо вони продовжать співпрацю із підсанкційними компаніями. Китай, на який припадає близько 20% імпорту нафти з Росії, офіційно виступив проти

односторонніх санкцій, які, на його думку, не мають міжнародно-правової основи. Тим не менш, китайські державні нафтові компанії, такі як PetroChina, Sinopec, CNOOC і Zhenhua Oil, призупинили морські закупівлі російської нафти через занепокоєння щодо санкцій. Запроваджені санкції також безпосередньо зачепили китайські порти Ціндао та Донцзяоу, ключові для імпорту російської та іранської нафти. Хоча китайські державні компанії призупинили морські закупівлі, очікується, що незалежні китайські нафтопереробні заводи («teapots»), які імпортують більшу частину морської нафти, можуть лише тимчасово призупинити закупівлі для оцінки впливу санкцій, але, ймовірно, продовжать фінансування росії через посередників.

В Європі санкції посилять тиск на наявні активи «Лукойлу». Керівництво Нідерландів та Румунії очікує, що компанія буде змушена продати свої заводи на їхніх територіях, зокрема, НПЗ Petrotel у Румунії та 45% частку в НПЗ Zeeland у Нідерландах. Колишній керівник «Лукойлу» зазначив, що санкції завдадуть компанії значної шкоди, потенційно змушуючи її продати частки в іноземних проектах (від Єгипту до Іраку), що може вплинути на 20% її доходів. Однак прем'єр-міністр Угорщини Віктор Орбан вже шукає шляхи обходу американських санкцій проти «Роснефті» та «Лукойлу». Загалом, запровадження цих заходів є частиною ширших дій США та їхніх союзників, спрямованих на обмеження доходів Москви від енергоресурсів, що допомагають фінансувати війну.

Регулювання

Реформа режиму нагляду з ПВК/ФТ у Сполученому Королівстві ⁸



Reform of the Anti-Money
Laundering and Counter-
Terrorism Financing
Supervision Regime

Consultation Response

Цей документ, «Відповідь на консультації щодо реформи режиму нагляду за ПВК/ФТ», опублікований Казначейством Його Величності (HM Treasury), є не просто звітом про отриманий зворотний зв'язок, а фундаментальною політичною заявою, що анонсує наймасштабнішу реструктуризацію британської системи нагляду у сфері ПВК/ФТ за останнє десятиліття. В основі документа лежить визнання того, що поточна система є "складною та роз'єднаною". Ця фрагментація, коли нагляд здійснюють три державні органи (FCA, Комісія з азартних ігор та HMRC) та 22 окремі професійні органи-наглядачі (PBSs) для юридичного та бухгалтерського секторів, призводить до критичних проблем: "непослідовності у нагляді та правозастосуванні" та суттєвих ускладнень у співпраці з правоохоронними

органами. Реформа покликана вирішити саме ці стратегічні недоліки, які були визнані вразливістю національної безпеки.

У ході консультацій 2023 року уряду було запропоновано чотири моделі реформи: від мінімального втручання (модель OPBAS+, що передбачала лише посилення існуючого органу нагляду за PBSs) до повної централізації (модель SAS, Єдиний наглядач за ПВК для абсолютно всіх секторів). Проміжними варіантами були Консолідація PBS (скорочення кількості наглядачів) та модель SPSS (Єдиний наглядач за професійними послугами). Аналіз 95 отриманих відповідей виявив фундаментальний розкол у поглядах. Юридичний та бухгалтерський сектори,

представлені своїми PBSs, переважною більшістю (89%) підтримали найменш інвазивну модель OPBAS+, аргументуючи це необхідністю збереження спадкоємності та визнанням прогресу, вже досягнутого OPBAS. Натомість фінансовий сектор, державні органи (включно з правоохоронцями) та представники громадянського суспільства так само рішуче виступили за кардинальні структурні зміни, віддавши перевагу моделі SPSS (53% підтримки у цій групі). Їхня позиція ґрунтувалася на тому, що поточна система є неефективною, а модель OPBAS+ не здатна вирішити системні проблеми.

Ключовим рішенням уряду, детально викладеним у цьому документі, стало прийняття моделі 3: створення Єдиного наглядача за професійними послугами (SPSS). Уряд свідомо відхилив позицію юридичної та бухгалтерської спільнот на користь позиції фінансового сектору та силових структур. Виконавцем цієї нової ролі мегарегулятора призначено Financial Conduct Authority (FCA). Це означає повну передачу повноважень: FCA забере функції нагляду за ПВК/ФТ у всіх 22 існуючих PBSs, а також у Податкової та митної служби (HMRC) в частині нагляду за тими постачальниками бухгалтерських послуг (ASPs) та TCSPs, які не є членами PBSs. Таким чином, замість 23+ окремих наглядових інстанцій для професійних послуг з'являється єдиний державний регулятор, що є прямим втіленням тези зі вступу, що нагляд за ПВК/ФТ є, зрештою, "роботою держави".

Обґрунтування цього рішення є багатограним. По-перше, це радикальне спрощення складного регуляторного ландшафту. По-друге, це уніфікація підходу, яка вирівнює професійні послуги з іншими секторами (як-от фінансовий), що вже перебувають під державним наглядом. По-третє, консолідація нагляду за приблизно 60 000 фірмами під егідою FCA дозволить впровадити більш послідовний, керований даними та ризик-орієнтований підхід, концентруючи ресурси на сферах найвищого ризику. Однією з головних очікуваних переваг є значне покращення координації та прямий обмін розвідувальними даними між FCA як єдиним наглядачем та правоохоронними органами.

Наслідком цієї реформи стане те, що існуючий орган OPBAS, який контролював PBSs, більше не буде потрібний. Самі ж PBSs втратять свої статутні повноваження у сфері ПВК/ФТ, але збережуть за собою "ширші регуляторні та представницькі функції (наприклад, нагляд за професійними стандартами)".

Документ чесно визнає головний виклик, який створює ця реформа, — запровадження системи "подвійного регулювання". Наприклад, юридична фірма відтепер буде підзвітна FCA у питаннях ПВК/ФТ, але водночас залишатиметься під наглядом свого традиційного PBS у питаннях професійної поведінки та стандартів. Уряд зобов'язується працювати з

Висновки:

- **Уряд Великої Британії ухвалив рішення про повну ліквідацію поточної фрагментованої моделі нагляду за ПВК/ФТ у секторах професійних послуг.** Функції нагляду будуть відібрані у 22 професійних наглядових органів (PBSs) та частково у Податкової служби (HMRC).
- **Створюється єдиний державний наглядач (модель SPSS), функції якого виконуватиме FCA.** FCA стане мегарегулятором у сфері ПВК/ФТ для всіх постачальників юридичних, бухгалтерських послуг та TCSP (близько 60 000 суб'єктів).
- Це рішення було прийнято всупереч позиції самих юридичних та бухгалтерських секторів (які на 89% підтримували збереження старої моделі OPBAS+), але на користь позиції фінансового сектору та правоохоронних органів, які очікують від FCA більш послідовного ризик-орієнтованого підходу, кращого обміну даними та жорсткіших примусових заходів.
- **Фірми, яких стосується реформа, перейдуть на модель «подвійного регулювання»:** FCA контролюватиме їхню діяльність у сфері ПВК/ФТ, тоді як існуючі професійні органи (PBSs) збережуть нагляд лише за професійними стандартами та етикою. Уряд визнає ризик додаткового навантаження та планує мінімізувати дублювання.

PBSs, щоб "мінімізувати дублювання" в адміністративних процесах, проте саме цей аспект, ймовірно, стане найбільшим джерелом напруги для фірм. Впровадження реформи не буде миттєвим: воно потребує ухвалення нового первинного законодавства. Окремо Казначейство анонсує найближчим часом (на початку листопада) нові консультації щодо конкретних повноважень (включно з примусовими), які необхідно надати FCA для виконання цієї безпрецедентної ролі.

Звіти окремих інституцій та експертів

Майбутнє платежів: цифровий суверенітет Європи, інноваційна інфраструктура та нова архітектура фінансової стійкості⁹



Документ є аналітичним збірником, присвяченим глибокому дослідженню сучасного та майбутнього стану платіжної індустрії у світі, з акцентом на Європу та Велику Британію. Це перше видання нового журналу, який об'єднує провідних міжнародних експертів — представників центральних банків, європейських фінансових регуляторів, комерційних банків, наукових кіл і фінтех-компаній — задля обговорення стратегічних напрямів трансформації платіжних систем у контексті цифровізації, регуляторної гармонізації, кіберстійкості та штучного інтелекту.

Загальний зміст документа вибудований навколо ідеї, що платежі перестали бути другорядною функцією фінансової інфраструктури — вони перетворилися на стратегічний центр інновацій, конкуренції та регулювання. У вступному слові засновника Projective Group, Стефана Діркса, наголошується, що останні роки стали періодом «ідеального шторму» для галузі, коли поєднання цифровізації, нових технологій, зростання ризиків фінансових злочинів і підвищеної регуляторної уваги створило безпрецедентний тиск на традиційних учасників ринку, водночас відкривши шлях новим інституціям, фінтехам та платформним рішенням.

Однією з центральних статей видання є матеріал Вікторії Келанд, Головного уповноваженого з емісії та платежів та виконавчого директора з питань платежів Банку Англії, присвячений оновленню системи RTGS (Real-Time Gross Settlement) у Великій Британії. У документі RTGS постає як «осердя фінансової стабільності» та одночасно «пусковий майданчик для інновацій». Оновлена система RT2, запущена у квітні 2025 року, дозволяє здійснювати розрахунки у режимі реального часу в центральнобанківських грошах, обробляючи щодня близько 800 мільярдів фунтів стерлінгів. Новий інтерфейс BERT1, інтеграція ISO 20022, модульна архітектура та API-орієнтований підхід зробили систему відкритою для небанківських постачальників платіжних послуг і майбутніх моделей цифрових розрахунків. Келанд описує RT2 як технологічну «орбіту», що, подібно до запуску першого супутника, закладає основу для подальшого розвитку — зокрема для впровадження синхронізованих транзакцій на основі DLT, токенизованих активів і навіть wholesale-CBDC. Автор підкреслює, що успіх RT2 став можливим завдяки тісній співпраці з приватним сектором, майже 250 учасниками, та має стати прикладом спільного державного і ринкового управління інноваціями у сфері платежів.

Наступна ключова стаття, підготовлена Карлосом Нашером та Робертом-Яном Веккінгом, — присвячена глобальним трендам у платіжному секторі. Автори визначають сучасну фінансову

⁹ <https://www.projectivegroup.com/wp-content/uploads/Journal-of-Financial-Services-The-Future-of-Payments.pdf>

екосистему як «VUCA-світ» — волатильний, невизначений, складний і неоднозначний. Вони стверджують, що три головні сили — цифровізація, регулювання та кібербезпека — радикально змінюють поведінку споживачів, бізнес-моделі банків і баланс між державними та приватними платіжними інфраструктурами. Згідно з даними за 2023–2024 роки, обсяг безготівкових транзакцій сягнув 1,4 трильйона, а частка готівкових операцій у Європі стрімко знижується. Автори вказують, що штучний інтелект стає ключовим фактором персоналізації платіжних сервісів, прогнозного виявлення шахрайства та автоматизації регуляторної звітності.

Окрему увагу документ приділяє появі цифрового євро — центральнобанківської цифрової валюти ЄЦБ, яка пройшла етап дослідження й підготовки у 2023–2025 роках і може бути поступово впроваджена після 2028 року. Вона позиціонується не як заміна готівки, а як її доповнення — «цифрова банкнота» для всієї єврозони. На відміну від комерційних систем Visa чи Mastercard, цифровий євро матиме правовий статус законного платіжного засобу, з регульованими тарифами та відкритими інтерфейсами для банків і гаманців. Однак документ звертає увагу на потенційні конфлікти між учасниками (центробанк, емітенти, постачальники гаманців, торговці), а також на потребу в бездоганному користувацькому досвіді, без якого прийняття нової валюти може бути обмеженим.

Інша важлива ініціатива — Wero (European Payments Initiative), приватний проєкт, що має на меті створити європейську альтернативу PayPal і BigTech-платежам. Його амбіція полягає у забезпеченні фінансового суверенітету ЄС, однак автори визнають, що на момент публікації Wero мала обмежену функціональність і низьке сприйняття серед споживачів. Попри це, вона розглядається як критичний елемент у формуванні незалежної європейської платіжної інфраструктури.

Особливо докладно аналізуються регуляторні зміни, які разом формують нову правову архітектуру платіжного простору ЄС. Документ підкреслює, що PSD3 і PSR продовжують лінію PSD2, але з набагато ширшим охопленням — вони встановлюють обов'язкову верифікацію IBAN, заборону додаткових комісій, посилюють вимоги до автентифікації клієнтів і перекладають відповідальність за шахрайські операції з користувачів на банки. Регламент DORA, який набув чинності у січні 2025 року, вводить єдину рамку цифрової операційної стійкості для всіх фінансових установ і постачальників ІКТ, у тому числі зобов'язання до тестування кіберстійкості та моніторингу ланцюгів постачання. FIDA (Financial Data

Висновки:

- **Платіжна інфраструктура стає платформою для інновацій.** Оновлена система RTGS у Великій Британії (RT2) і майбутній цифровий євро демонструють перехід від традиційних розрахунків до відкритих, модульних платформ, що підтримують DLT, API та синхронізовані платежі — фундамент майбутньої фінансової екосистеми.
- **Європейський платіжний суверенітет і конкуренція з глобальними учасниками.** Ініціативи EPI/Wero, цифровий євро та EUDIW спрямовані на створення автономної європейської екосистеми, зменшення залежності від Visa, Mastercard і PayPal, забезпечення правового статусу цифрових грошей та уніфікованої ідентифікації користувачів.
- **Регуляторна конвергенція формує нову архітектуру контролю.** Введення PSD3, PSR, DORA та FIDA у 2025–2027 рр. створює єдину нормативну систему для кіберстійкості, відкритого фінансування та захисту споживачів, підвищуючи відповідальність банків і прозорість даних.
- **Штучний інтелект і дані стають основою персоналізованих фінпослуг.** Інтеграція AI, аналітики транзакцій і відкритих API трансформує боротьбу з шахрайством, дозволяє автоматизувати звітність і створює передумови для індивідуальних платіжних сервісів нового покоління.

Access Regulation), попри невизначений статус, потенційно стане основою для відкритого фінансування, забезпечуючи стандартизований обмін даними між банками, страховиками та фінтехами. Нарешті, EUDIW (European Digital Identity Wallet) — нова цифрова ідентичність ЄС, що має стати універсальним засобом автентифікації до 2026 року, — закладає технічну та юридичну основу для уніфікованого користувацького доступу до фінансових послуг.

Підсумовуючи, автори видання роблять висновок, що найближчі роки визначать структуру світового ринку платежів на десятиліття вперед. Центробанки стають технологічними платформами, а банки — сервісними інтеграторами у ширшій цифровій екосистемі. Головна тенденція — конвергенція інфраструктури, регулювання та технологій у межах єдиного цифрового простору, де ключову роль відіграватимуть довіра, кіберстійкість і персоналізація. Штучний інтелект, розширені API, токенизація активів та відкриті стандарти формують нову фінансову архітектуру, у якій платежі стають не лише механізмом передачі вартості, а й каналом економічної трансформації, прозорості та зростання.

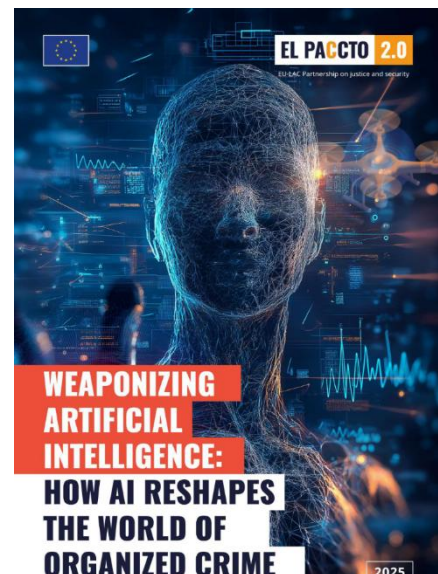
Таким чином, документ не просто описує технологічні інновації, а фактично окреслює стратегічну дорожню карту переходу Європи до цифрової монетарної ери, де фінансова стабільність, інновації, регуляторна єдність і клієнтоцентричність взаємодоповнюють одна одну.

Від генеративних моделей до кіберзлочинів: як AI стає зброєю організованих груп¹⁰

Документ є одним із найповніших міжнародних аналітичних досліджень про те, як штучний інтелект радикально змінює природу організованої злочинності у Європі, Латинській Америці та Карибському басейні. Він був підготовлений у рамках програми EL PACCTO 2.0 — спільної ініціативи ЄС і країн ЛАК, спрямованої на зміцнення безпеки, правосуддя та боротьбу з транснаціональними злочинами. Звіт висвітлює феномен «озброєння AI», показуючи, як технології, створені для суспільного розвитку, перетворюються на інструменти масштабних кримінальних операцій — від кібератак до фінансового шахрайства, торгівлі людьми й дезінформаційних кампаній.

Автори описують безпрецедентну еволюцію штучного інтелекту після запуску ChatGPT у 2022 році. Генеративний AI став «множником сили» для злочинців, дозволяючи автоматизувати, персоналізувати й масштабувати атаки. Виник феномен Crime-as-a-Service (CaaS) — модель, за якої навіть особи без технічних навичок можуть придбати або замовити злочинні послуги в даркнеті. Сучасні великі мовні моделі (LLMs) і системи генеративного AI використовуються для створення шкідливого коду, фішингових кампаній, фальшивих документів, діпфейків та імітації людських осіб. Технології, що колись вимагали спеціальних знань, стали масово доступними й перетворили кіберзлочинність на індустрію.

У першій аналітичній частині звіт описує загальний контекст: злочинні групи використовують AI для модернізації класичних схем — від прання грошей і шахрайства до дезінформаційних кампаній. Europol, Interpol і ENISA констатують, що штучний інтелект радикально ускладнив процес атрибуції, виявлення і доведення злочинів. Зловмисники застосовують алгоритмічні



¹⁰ <https://zenodo.org/records/17206874>

атаки на самі AI-системи — через отруєння даних, викривлення моделей або використання вразливостей у постачальників LLM. Таким чином, AI стає не лише інструментом, а й ціллю злочину, створюючи подвійний виклик для правоохоронців.

Далі документ переходить до розгорнутого аналізу конкретних видів злочинів, що здійснюються або підсилюються AI. Одним із найнебезпечніших є інтелектуальне шкідливе ПЗ, яке самонавчається, змінює власний код і уникає антивірусного виявлення. Кампанії на зразок ShadowRay (2024) показали, як AI-моделі можуть бути викрадені й перетворені на платформи криптомайнінгу та викрадення даних. У сфері вимагачів (ransomware) AI використовується для масштабних атак на енергетику й транспорт, а фішинг, згенерований за допомогою LLM, досяг рівня, коли повідомлення майже неможливо відрізнити від легітимних. Штучний інтелект також змінив природу DDoS-атак — так звані «автономні рої» самостійно змінюють протоколи та інтенсивність, обходячи захист у реальному часі.

Окремий блок присвячено фінансовим злочинам, що за допомогою AI набули небаченого масштабу. Платформи на зразок OnlyFake дають змогу за хвилини генерувати фальшиві паспорти та посвідчення, обходити системи KYC і відкривати рахунки на біржах, таких як OKX, Bybit чи PayPal. У даркнеті з'явилися сервіси KYC-bypass-as-a-Service, де AI створює повністю синтетичні особистості з реалістичними відео, підписами та біометричними даними. Ці технології використовуються не лише для викрадення коштів, а й для відмивання коштів та ухилення від санкцій. AI також використовується у маніпулюванні ринками — боти створюють

штучну ліквідність («wash trading») або розповсюджують фейкові новини для керування ціновими коливаннями. Прикладом є операція ФБР «Token Mirrors» (2024), яка розкрила мережу AI-трейдингових ботів із 25 млн USD прибутку.

Одним із найтривожніших аспектів є соціальна інженерія та дїпфейк-атаки. Зображення згенеровані за допомогою AI та голоси використовуються для імітації керівників компаній або держслужбовців, що призводить до фінансових збитків на десятки мільйонів доларів (випадок з Гонконгу — 25,6 млн USD переказано на основі підробленої відеоконференції з «керівництвом»). Група Lazarus використовує дїпфейки для отримання доступу до криптобірж та здійснення масштабних крадіжок. У Латинській Америці картелі використовують відео згенеровані за допомогою AI для вимагання викупів. Таким чином, AI перетворюється на інструмент психологічного терору та інформаційної дестабілізації.

На законодавчому рівні Європейський Союз у 2024 році прийняв Регламент (ЄС) 2024/1689 — AI Act, що встановлює ризик-орієнтований підхід до

Висновки:

- **Необхідна адаптація кримінального права до «машинних агентів».** Потрібно юридично визначити відповідальність за дії, згенеровані AI (автономне програмне рішення, код, навчена модель), включно з процедурою доказування і збереження цифрових артефактів.
- **Публічно-приватна співпраця — критичний чинник стримування.** AI-провайдери, хмарні сервіси та соцмережі мають бути зобов'язані повідомляти про зловживання, зберігати лог-дані, співпрацювати з правоохоронцями на транскордонному рівні (зразок — модель Europol EC3).
- **Потрібне створення спеціалізованих «AI Task Forces».** Слід розвивати у правоохоронних органах підрозділи з цифрової криміналістики AI (розпізнавання дїпфейків, атрибуція генеративного контенту, відстеження ботнетів, аналітика криптовалют).
- **Превенція через освіту й етичне регулювання.** Звіт наголошує: підготовка суддів, прокурорів і поліції у сфері AI має бути системною. Водночас важливо стимулювати «етичний дизайн» технологій (Safety by Design) та підвищувати обізнаність суспільства про ризики AI-маніпуляцій.

використання AI та забороняє високоризикові практики, такі як біометричний моніторинг у публічних просторах або соціальне скорингування. Водночас питання відповідальності залишаються неврегульованими після відкликання AI Liability Directive. У результаті правоохоронці вимушені працювати в умовах правового вакууму, де частина дій штучних агентів не підпадає під існуючі норми кримінального права.

У заключній частині автори наголошують, що боротьба зі злочинністю в епоху AI потребує нової архітектури міжнародної координації. ЄС, країни Латинської Америки та Карибів мають інтегрувати AI-інструменти у системи розслідувань, створити спільні бази даних і розробити єдині протоколи зберігання цифрових доказів. Звіт рекомендує зміцнення спеціалізованих підрозділів поліції та судових експертів з цифрової криміналістики, запровадження обов'язкових механізмів звітності AI-провайдерів та програм навчання для суддів, прокурорів і регуляторів. Наголошується також на важливості етичного дизайну технологій та суспільної просвіти, щоб запобігти маніпуляціям і зберегти демократичні інститути.

Отже, дослідження EL PACSTO 2.0 викриває нову реальність, у якій штучний інтелект стає не просто засобом злочину, а й його архітектором. Автори підкреслюють, що протидія вимагає превентивного підходу — від оновлення законодавства та побудови стійких технологічних систем до міжнародної кооперації та постійного моніторингу з боку держав і приватного сектору. Без цього розрив між швидкістю інновацій і реакцією правосуддя лише зростатиме, створюючи середовище, де злочинний інтелект може працювати автономно і безкарно.

Інші новини

Викриття кіберзлочинності як послуги: 7 заарештованих ¹¹



Стаття повідомляє, що в результаті міжнародної правоохоронної операції, під кодовою назвою "SIMCARTEL", було затримано сім осіб, які забезпечували злочинний механізм «кіберзлочин-як-послуга» (cybercrime-as-a-service). Ця операція була спільною між кількома державами Європи (у тому числі Латвія, Австрія, Естонія, Фінляндія) та агентствами, зокрема Europol та Eurojust.

У своїй суті мережа, що була ліквідована, працювала як інфраструктурний сервіс: вона надавала іншим злочинним акторам (клієнтам) ефективні інструменти для проведення низки тяжких правопорушень, зокрема шахрайства, вимагання, розповсюдження матеріалів сексуального насильства над дітьми, та переміщення людей (migrant smuggling) — тобто вона не діяла лише як кінцевий виконавець, а виступала як «постачальник послуги» для інших.

Операція передбачала суттєві арешти та вилучення: правоохоронці знищили п'ять серверів, вилучили близько 1 200 «SIM-box» пристроїв і приблизно 40 000 активних SIM-карт. У двох країнах — тільки в Австрії та Латвії — число зафіксованих випадків шахрайства досягло 1 700 та 1 500 відповідно. Загальна сума збитків, яку вони завдали жертвам, оцінюється близько €5 млн — з чого приблизно €4.5 млн були в Австрії і €420 000 — в Латвії.

З точки зору ризиків ПВК/ФТ/ФР важливо підкреслити такі аспекти.

По-перше, функціонування моделі «кіберзлочин-як-послуга» означає, що інфраструктура злочинної діяльності відокремлена від кінцевих виконавців, що створює значну вразливість до

¹¹ <https://www.europol.europa.eu/media-press/newsroom/news/cybercrime-service-takedown-7-arrested>

санкційних ризиків. Тобто організація, що надає послугу (наприклад, SIM-box чи масові SIM-картки) — хоча й може не бути безпосередньо задокументована як виконавець шахрайства — виступає важливим проміжним ланцюгом і може бути притягнута до відповідальності або потрапити під санкції.

По-друге, види шахрайства, які було здійснено з використанням цієї інфраструктури, мають серйозний компонент ВК/ФТ: створення великої кількості фальшивих акаунтів на комунікаційних платформах дозволяє злочинцям приховувати сліди фінансових операцій, використовувати їх у схемах легалізації коштів та переміщення активів.

По-третє, географічний масштаб та мультиюрисдикційність мережі підкреслюють, що ризики не обмежуються однією країною, а є транскордонними — це важливо з точки зору виконання вимог регуляцій щодо клієнтської перевірки, співробітництва між юрисдикціями та обміну інформацією між відповідальними суб'єктами.

По-четверте, цей випадок демонструє, як інфраструктура, що на перший погляд може здаватися «телефонною (SIM-box) або «телекомунікаційною», фактично стає важливим ланцюгом у схемах відмивання коштів чи переміщення коштів/активів, оскільки масова кількість SIM-карт дозволяє здійснювати анонімні транзакції, створювати множинні акаунти, здійснювати соціальну інженерію, фішинг і т.д. Це означає, що регулятори та органи фінансового моніторингу повинні звертати увагу не лише на класичні фінансові транзакції, але й на телеком-інфраструктуру та її потенціал для зловживань.

З точки зору регуляторної політики та практики, є кілька ключових висновків: перше — необхідність розширення співробітництва між телеком-операторами, провайдерами SIM-послуг, фінансовими установами та правоохоронцями; друге — необхідність впровадження систем виявлення масових заходів з анонімізації телеком-зв'язків (наприклад, прив'язка SIM-карт до персоналізованих ідентифікаційних даних, виявлення «SIM-box» як індикатора ризику); третє — забезпечення механізмів обміну інформацією між країнами щодо подібних інфраструктурних схем злочинців; четверте — в контексті тренінгів і підготовки фахівців з ПВК/ФТ/ФР підкреслюється, що знання про телеком-інфраструктуру та її зловживання має бути включено до навчальних модулів.

Операція, здійснена з використанням координації між країнами ЄС, також підкреслює важливість публічно-приватного партнерства (PPP): провайдери телекомунікацій, банківські установи, інші фінансові установи та державні органи повинні працювати разом для виявлення та реагування на подібні інфраструктурні загрози. База знань, типологічні дослідження, також мають охоплювати такі інфраструктурні послуги «для зловмисників».

Також важливо зазначити, що таке розгортання послуг (SIM-box, масові SIM, сервери) дає зловмисникам можливість працювати в тіні, а тому для регуляторів і слідчих органів важливо володіти інформацією про технічні характеристики таких послуг, методи їх виявлення, ідентифікацію користувачів, а також їх можливу роль у схемах легалізації коштів (наприклад, через фальшиві акаунти, соцмережі, маніпуляції з телеком-послугами, які надалі використовуються для фінансових транзакцій).

У підсумку можна сказати, що ця операція є суттєвим ударом по моделі «кіберзлочин як сервіс» в Європі, демонструючи, що навіть інфраструктурні провайдери для кримінальних схем не є недосяжними. Для практиків ПВК/ФТ/ФР це означає: увага до телеком-інфраструктури як ризикового вузла, посилення координації між відомствами, регулярне оновлення типологій із урахуванням інфраструктурних схем злочинців, а також інтеграція таких сценаріїв в навчальні курси та тренінги.

Для загального розвитку

EDD для клієнтів з високим рівнем ризику: покроковий підхід для ВНУП¹²

 RapidAML

**EDD for
High-Risk Customers:**
A Step-by-Step Approach
for DNFBPs

Документ, підготовлений компанією RapidAML, є практичним методичним посібником для визначених нефінансових установ і професій (ВНУП) в Об'єднаних Арабських Еміратах (ОАЕ) щодо впровадження посиленних заходів належної перевірки (EDD) у відповідності до вимог національного законодавства та стандартів FATF. Текст має чітку освітню та методологічну спрямованість, деталізуючи послідовність дій, типові виклики, автоматизацію процесів і правові наслідки недотримання вимог.

Документ розпочинається поясненням співвідношення між CDD та EDD. CDD описується як базовий процес ідентифікації клієнтів, перевірки їх особи та оцінки ризику відмивання коштів, тоді як EDD застосовується для клієнтів, що становлять підвищений ризик, і передбачає глибше дослідження джерел коштів, цілей транзакцій і характеру бізнесу. Для ВНУП, які працюють в ОАЕ, EDD є обов'язковим елементом комплексної програми ПБК/ФТ, яка має відповідати ризик-орієнтованому підходу (РОП) FATF. Особлива увага приділяється обов'язку ВНУП документувати політики й процедури EDD, визначати умови та частоту перевірок, а також підтримувати оновленість клієнтських даних.

Далі наведено розгорнуту характеристику високоризикових клієнтів, до яких належать політично значущі особи (PEP), клієнти з непрозорими структурами власності, нерезиденти без належних ідентифікаційних документів, підприємства з інтенсивними готівковими операціями, а також суб'єкти, пов'язані з юрисдикціями, що перебувають у санкційних списках, під ембарго чи у переліках FATF (чорний або сірий списки). Високий ризик також може бути зумовлений природою бізнес-відносин або асоціацією з третіми сторонами невідомого походження. Таким чином, EDD застосовується не лише з огляду на тип клієнта, але й на характер транзакцій, бізнес-модель і географічну прив'язку.

У розділі "When should DNFBPs take EDD measures" описано конкретні обставини, за яких ВНУП зобов'язані впроваджувати EDD. Серед них: виявлення високоризикового клієнта; сумніви щодо коректності або релевантності поточного рівня ризику; спостереження підозрілих активностей; нелогічність структури володіння чи відсутність прозорості КБВ; а також невідповідність між задекларованим бізнесом клієнта та пропонуваними відносинами з ВНУП. У всіх випадках ВНУП повинні забезпечити збір достатньої інформації, пропорційної рівню ризику.

Центральне місце у документі займає покроковий підхід до проведення EDD, що охоплює сім ключових етапів.

1. Збір додаткової інформації для ідентифікації особи — ВНУП повинні отримати розширені відомості про діяльність клієнта, основних партнерів, постачальників і причини можливих відхилень від типових операцій.
2. Перевірка джерел коштів і походження статків — збір документів, що підтверджують походження коштів (зарплата, банківські виписки, прибутки, кредити, заощадження) та формування активів (статутні документи, фінансова звітність, дарування, спадщина).
3. Використання лише власних банківських рахунків клієнта для запобігання відмиванню коштів через посередників.

¹² <https://rapidaml.com/wp-content/uploads/2024/06/EDD-for-High-Risk-Customers-A-Step-by-Step-Approach-for-DNFBPs.pdf>

4. Схвалення вищим керівництвом — обов'язкова вимога для встановлення ділових відносин із високоризиковими клієнтами, щоб врахувати ризик-апетит організації.
5. Підвищений моніторинг — регулярна перевірка санкційних списків, аналіз репутації та моніторинг транзакцій, зокрема тих, що пов'язані з віртуальними активами чи переказами коштів.
6. Періодичний перегляд і оновлення КУС — своєчасне оновлення клієнтських профілів для підтримання актуальності ризикової оцінки.
7. Звітування про підозрілі транзакції — у разі виявлення відхилень ВНУП зобов'язаний подати повідомлення до ПФР через портал goAML. Невиконання цього обов'язку розглядається як порушення федерального законодавства з відповідними санкціями, включно зі штрафами та позбавленням права на діяльність.

Подальший розділ присвячено викликам у впровадженні EDD. Серед них виділено:

- Міжюрисдикційні відмінності регулювання, які створюють труднощі для компаній, що працюють у кількох країнах, через різні вимоги до КУС/EDD;
- Постійні оновлення нормативних актів, що вимагають регулярного перегляду політик;
- Складність встановлення КБВ через багаторівневі корпоративні структури, компанії оболонки й офшори;
- Питання захисту даних, де ВНУП мають отримувати чітку згоду клієнтів на зберігання персональних даних і дотримуватися вимог Закону про захист персональних даних;
- Недоліки ручних процесів, які спричиняють затримки, помилки, дублювання перевірок і неефективність використання ресурсів.

Автори роблять акцент на автоматизації EDD як ключовому рішенні для ВНУП. Використання технологій, зокрема штучного інтелекту (AI), машинного навчання (ML), роботизованої автоматизації процесів (RPA) та аналітики даних, значно підвищує якість, швидкість і точність виконання перевірок. AI і ML здатні адаптивно виконувати скринінг санкцій, PEP і негативних медіа, а також допомагають у ризик-скорингу. RPA автоматизує рутинні дії (розсилку запитів, введення даних, верифікацію ID через NFC-чипи чи 2FA-перевірки), що мінімізує людський фактор. Аналітика даних дозволяє виявляти закономірності у складних корпоративних структурах і розкривати приховані зв'язки, включно з КБВ.

Переваги автоматизації включають підвищення точності оцінки ризику, скорочення часу перевірок, покращення звітності та дотримання вимог законодавства. Інтеграція EDD-рішень з іншими програмами — CRM, платіжними системами, AML-звітуванням — створює єдине середовище для виконання вимог відповідності.

Документ завершують розділи про наслідки недотримання EDD, які варіюються від штрафів та кримінальної відповідальності до втрати репутації, а також висновок про стратегічну важливість EDD для ВНУП. Автори підкреслюють, що лише використання сучасних технологій, у поєднанні з чітко побудованим ризик-орієнтованим підходом, дозволяє ВНУП мінімізувати ризики відмивання коштів, фінансування тероризму та розповсюдження ЗМЗ, а також ефективно виконувати вимоги FATF.

Отже, цей документ є комплексним методичним орієнтиром для ВНУП щодо організації системи EDD, її технологічної трансформації та інтеграції в загальну систему управління ризиками ПВК/ФТ/ФР. Він не лише відображає сучасні вимоги до контролю за високоризиковими клієнтами, а й демонструє тенденцію до цифровізації комплаєнс-процесів, що є ключовою передумовою ефективності системи фінансового моніторингу в умовах зростання складності фінансових злочинів.

Ваша думка важлива!

1. Як оптимально зрівноважити свободу діяльності НПО із запобіжниками, що зменшують ризики їхнього зловживання для фінансування тероризму?
2. Які стимули (знижки, безкоштовні транзакції тощо) можуть стати ефективними драйверами впровадження CBDC в Україні?
3. Чи здатна українська модель CBDC (наприклад, е-гривня) забезпечити баланс між прозорістю для держави та збереженням фінансової приватності громадян, і де має проходити межа між контролем і довірою у цифровій фінансовій екосистемі?
4. Як інтегрувати принципи CSF 2.0 у систему управління кіберризиками в українських СПФМ?
5. Яку роль може відігравати модель спільної відповідальності між державою, бізнесом і громадянським суспільством у формуванні національної системи реагування на кіберінциденти в Україні, та які організаційні чи правові зміни необхідні для її ефективного функціонування?
6. Чи може Україна, яка має потужний IT-сектор і досвід у кібербезпеці, стати регіональним центром протидії злочинному використанню AI, і які законодавчі або інституційні зміни для цього необхідні?
7. Які ознаки або «red flags» можуть допомогти СПФМ виявляти автоматизовані схеми відмивання коштів, створені ботами або AI? Які технологічні рішення (виявлення дідфейків, AI-аналітика) можна інтегрувати у систему фінансового моніторингу для зменшення цих ризиків?
8. Які моделі співпраці між державою, приватним сектором і розробниками AI-систем можуть забезпечити ефективне виявлення та запобігання використанню AI у відмиванні коштів, фінансуванні тероризму та кіберзлочинності в Україні?

Контакуйте 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-2025-43

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

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