Методологічний бюлетень

Серійний номер: МінФін-AML-2025-11

Березень 2025

“Ми - це те, що ми робимо постійно”

Арістотель

Мета

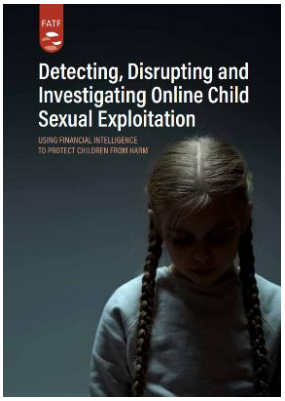
Методологічний Бюлетень видається Міністерством Фінансів України на регулярній основі починаючи з січня 2025 р. та містить інформацію щодо національних та світових тенденцій у сфері протидії відмиванню коштів, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення (ПВК/ФТ/ФР).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

Виявлення, припинення та розслідування випадків сексуальної експлуатації дітей в Інтернеті[1]



Документ, підготовлений FATF, присвячений питанням виявлення, припинення та розслідування сексуальної експлуатації дітей онлайн (OCSE) із застосуванням фінансової розвідки. Головною метою звіту є аналіз механізмів та схем злочинної діяльності, зокрема, двох основних типів OCSE: сексуального насильства над дітьми, що транслюється наживо (LSAC), та фінансового сексуального вимагання від дітей (FSEC).

За глобальними оцінками, приблизно 300 мільйонів дітей, що становить кожну восьму дитину у світі, щорічно зазнають сексуальної експлуатації в Інтернеті, і ця загроза має чітку тенденцію до зростання. Злочинці використовують сучасні інформаційні технології та соціальні мережі для спрощення, прискорення та масштабування своїх операцій.

[1] https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Online%20Child%20Sexual%20Exploitation%20Report.pdf.coredownload.inline.pdf

У випадку сексуального насильства в режимі прямої трансляції (LSAC) процес залучає трьох головних учасників: споживача (consumer), посередника (facilitator) та безпосередньо кривдника (abuser). Зазвичай споживач знаходиться у розвинених країнах (наприклад, Європа, Австралія, Північна Америка), а фактичні насильники й організатори – у країнах із високим рівнем ризику експлуатації (зокрема в Південно-Східній Азії). Платежі за ці злочинні послуги, хоча індивідуально невеликі (від 10 до 200 євро за сеанс), у сукупності складають значні суми. Транзакції здійснюються за допомогою платіжних систем типу PayPal, peer-to-peer переказів (P2P), а також віртуальних активів, які забезпечують додаткову анонімність. Характерно, що ці операції проводяться в незвичні години доби та мають повторюваний характер. Злочинці часто створюють емоційні зв'язки з жертвами, примушуючи їх до багаторазових сеансів експлуатації, збільшуючи тим самим загальні прибутки.

Другий тип злочину – фінансовий сексуальний шантаж дітей (FSEC). Цей злочин, як правило, передбачає контакт злочинця з дитиною через соціальні мережі з використанням фальшивих акаунтів («катфішинг»). Після отримання компрометуючих матеріалів жертви злочинці вимагають гроші, погрожуючи оприлюднити матеріали серед її контактів. Суми викупів варіюються в межах від 50 до 1500 EUR, і найчастіше перші суми становлять не більше 250 EUR. Найбільш поширеними методами передачі коштів є перекази через P2P-платформи, онлайн-платежі, передплачені карти, а також подарункові картки для ігрових платформ. Злочинці часто використовують технології анонімізації (VPN, криптовалюту та шифрування повідомлень), що значно ускладнює їхнє виявлення. Потерпілі в основному – підлітки чоловічої статі, хоча останнім часом збільшується кількість жінок-жертв. Більшість злочинців походять із країн, таких як Нігерія, Філіппіни та Кот-д'Івуар, але жертви знаходяться в усьому світі.

Документ містить практичні рекомендації та методики для ідентифікації фінансових транзакцій, пов'язаних із OCSE. Вказується, що фінансова інформація може суттєво допомогти правоохоронним органам у розкритті цих злочинів, навіть

Висновки:

- **Посилення використання фінансових індикаторів:** Фінансові установи повинні активно впроваджувати запропоновані у звіті індикатори ризику в операційну діяльність, особливо P2P-перекази, перекази через передплачені карти та віртуальні активи, для раннього виявлення підозрілих транзакцій, пов'язаних із сексуальним насильством над дітьми онлайн.
- **Покращення оперативності реагування:** Фінансові установи та підрозділи фінансової розвідки повинні розвивати здатність до виявлення й реагування на транзакції в реальному часі, а також співпрацювати з правоохоронними органами для швидкого захисту потенційних жертв (наприклад, своєчасні welfare checks).
- **Розширення партнерств із приватним сектором:** Слід стимулювати партнерство між правоохоронними органами та компаніями, які надають електронні послуги (соцмережі, онлайн-платформи, VASP), з метою покращення якості інформації, що подається для подальшого розслідування. Особливо слід заохочувати провайдерів соціальних мереж до використання інструментів виявлення матеріалів зі зловживаннями (hash-based detection).
- **Підвищення кваліфікації та обізнаності персоналу фінансових установ та компетентних органів:** Країни повинні проводити спеціалізовані тренінги для персоналу фінансових установ, правоохоронних та регуляторних органів, спрямовані на розпізнавання та ефективне реагування на транзакції, пов'язані з сексуальною експлуатацією дітей, що посилить оперативність та якість втручання.

якщо суми транзакцій незначні. Особлива увага приділена індикаторам ризику, таким як багаторазові перекази невеликих сум, нічні перекази, використання певних платформ чи послуг, незвичні транзакції, а також швидке зняття отриманих коштів.

Документ детально описує важливість взаємодії між приватним та державним секторами для виявлення та боротьби з OCSE. Наведені успішні приклади взаємодії між фінансовими установами, підрозділами фінансової розвідки та правоохоронними органами (зокрема у Канаді, Австралії, Індонезії, Нідерландах). Підкреслено ефективність методів виявлення «в прямому ефірі», коли фінансові установи миттєво повідомляють про підозрілі операції правоохоронні органи, які можуть негайно втрутитись, запобігаючи повторному віктимізуванню дітей.

Наприкінці звіту представлені конкретні рекомендації щодо посилення міжнародної співпраці, використання фінансових індикаторів, підвищення якості звітності, запровадження заходів запобігання та проведення спеціалізованих тренінгів для фінансових установ, що дозволить значно підвищити ефективність виявлення, розслідування та припинення таких злочинів.

Цей звіт є важливим аналітичним ресурсом для державних та приватних установ, спрямованим на посилення їхніх можливостей протидії фінансовим аспектам онлайн-експлуатації дітей.

Штучний інтелект у європейських інвестиційних фондах: можливості, ризики та регуляторні виклики[2]

Звіт Європейського управління з цінних паперів і ринків (ESMA) глибоко аналізує рівень впровадження та вплив штучного інтелекту (ШІ) на діяльність інвестиційних фондів у Європейському Союзі. Основна увага приділяється двом аспектам: операційному використанню ШІ в управлінні фондами та стратегіям інвестування у ШІ-компанії. Важливим контекстом дослідження є зростання популярності великих мовних моделей (LLMs) та генеративного ШІ (GenAI), що стимулює фінансові установи до перегляду своїх бізнес-моделей і технологічних стратегій.

У частині, присвяченій операційному використанню ШІ, автори зазначають, що попри зростання інтересу до ШІ, його застосування в інвестиційних фондах залишається відносно обмеженим. Лише невелика кількість фондів відкрито заявляє про використання алгоритмічних підходів на основі ШІ для ухвалення інвестиційних рішень. Водночас більшість інституцій застосовують інструменти ШІ не як автономні механізми прийняття рішень, а як допоміжні засоби для аналізу ринкових даних, прогнозування та підвищення ефективності бізнес-процесів. Зокрема, використання генеративного ШІ та LLMs зосереджене на автоматизації аналізу даних, вдосконаленні процесів управління ризиками, підготовці аналітичних звітів і комунікації з клієнтами. Важливо, що регулятор не виявив суттєвих доказів того, що фонди, які використовують ШІ, демонструють кращу фінансову ефективність, а деякі з них навіть зазнали відтоку капіталу.

Аналіз маркетингових і регуляторних документів 44 000 європейських інвестиційних фондів виявив, що кількість фондів, які прямо рекламують використання ШІ, досягла піку у 2023 році і

[2] https://www.esma.europa.eu/sites/default/files/2025-02/ESMA50-43599798-9923_TRV_Article_Artificial_intelligence_in_EU_investment_funds.pdf

відтоді знизилася. Лише 145 фондів (менше 0,1% від загальної кількості) офіційно заявляли про використання ШІ у своїх стратегіях, і тільки близько 30% з них використовували ШІ як основний механізм ухвалення рішень. При цьому понад половина таких фондів – це акційні фонди, решта – фонди змішаних активів, альтернативних інвестицій та облігацій. Більшість із них активно управляються, що підтверджує тезу про допоміжний, а не автономний характер ШІ у фінансовому секторі.

Ще одним важливим аспектом є аналіз інвестиційних стратегій, спрямованих на компанії, пов'язані з ШІ. За останні два роки активні інвестиційні фонди в ЄС збільшили частку своїх портфелів у ШІ-компаніях на 50%, підвищивши її з 9% до 14%. Вартість цих інвестицій подвоїлася, що частково пояснюється загальним зростанням ринкової капіталізації таких компаній. Значна частина вкладень припадає на найбільші технологічні компанії, відомі як «Magnificent Seven» (Apple, Microsoft, Amazon, Alphabet, Meta, Nvidia, Tesla). Водночас фонди також почали вкладати у ширше коло компаній, що займаються розробкою ШІ-рішень або інтегрують їх у свої бізнес-моделі. Ця тенденція вказує на високий рівень довіри до ШІ-індустрії, але водночас несе ризики надмірної концентрації інвестицій.

Регулятор звертає увагу на проблеми, що можуть виникнути у зв'язку зі збільшенням ролі ШІ у фінансовій індустрії. Однією з головних загроз є концентрація ризиків, зокрема через високий рівень інвестицій у вузьке коло технологічних компаній. Якщо ці компанії зіштовхнуться з несприятливими ринковими умовами, це може мати суттєвий вплив на весь сектор інвестиційних фондів. Інший аспект – залежність від сторонніх постачальників ШІ-рішень. Використання зовнішніх ШІ-сервісів несе ризики операційної вразливості та потенційної маніпуляції ринком, особливо якщо більшість учасників покладаються на одні й ті ж самі технології. Крім того, у доповіді підкреслюється необхідність ретельного управління алгоритмічними ризиками – автоматизовані системи ухвалення рішень можуть містити приховані упередження, що здатні призвести до системних викривлень на ринку.

Фінансові установи також стикаються із зростаючим регуляторним тиском. У 2024 році в ЄС набув чинності Акт про штучний інтелект (AI Act), який встановлює правові вимоги до використання ШІ в різних сферах, зокрема у фінансовому секторі. Однак на даний момент відсутні чіткі

Висновки:

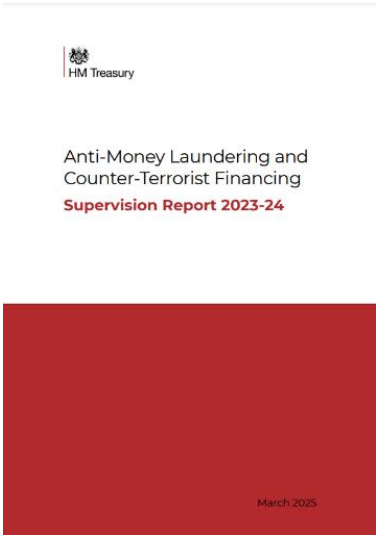
- **Розширене використання ШІ у фондах – більше підтримка, ніж заміна людських рішень.** Генеративний ШІ та великі мовні моделі використовуються переважно для допомоги аналітикам та трейдерам, але автоматичні стратегії ШІ поки що не є домінуючими. Фонди мають бути обережними щодо потенційного «AI-washing» (перебільшеного використання ШІ у маркетингових цілях).
- **Зростаюча концентрація інвестицій у компанії ШІ підвищує ринкові ризики.** Значне збільшення вкладень в компанії ШІ, особливо у «Magnificent Seven», може зробити інвестиційні портфелі більш вразливими до ринкових потрясінь. Інвесторам і регуляторам слід враховувати цей ризик під час оцінки системної стійкості.
- **Розрив у доступі до ШІ між великими та малими фондами.** Великі компанії швидше впроваджують ШІ, що створює ризик домінування впливових учасників у фінансовому секторі. Менші фонди можуть залежати від зовнішніх провайдерів ШІ-рішень, що підвищує ризик концентрації ринку технологічних послуг.
- **Потреба у чітких регуляторних підходах до ШІ у фінансах.** Впровадження ШІ у фінансовий сектор потребує детальнішого регулювання, особливо щодо управління ризиками, прозорості моделей та захисту інвесторів. Регулятори повинні контролювати використання ШІ в інвестиційних процесах для запобігання ринковим маніпуляціям та надмірним ризикам.

правила щодо застосування ШІ у портфельному менеджменті, що залишає простір для зловживань або неналежного управління ризиками.

Щодо майбутніх перспектив, звіт ESMA акцентує увагу на тому, що регулятори повинні ретельніше моніторити роль ШІ у фінансовій сфері, особливо в контексті прозорості використання ШІ у процесах прийняття рішень. Важливо також приділяти увагу можливим випадкам «AI-washing», коли компанії неправдиво заявляють про використання ШІ, вводячи інвесторів в оману. Загалом, дослідження свідчить про те, що ШІ продовжить відігравати зростаючу роль у фінансовому секторі, однак його вплив на прибутковість фондів залишається суперечливим, а підвищення концентрації інвестицій у технологічний сектор може нести значні ризики для стабільності ринку.

У цілому, звіт ESMA пропонує комплексний аналіз ролі ШІ в європейських інвестиційних фондах, окреслюючи як позитивні аспекти його застосування (підвищення ефективності, автоматизація процесів, розширення інвестиційних можливостей), так і потенційні загрози (ризик концентрації, залежність від сторонніх технологій, регуляторні виклики). Він підкреслює необхідність більш чіткої регуляторної політики, щоб забезпечити збалансоване впровадження ШІ у фінансовій сфері та мінімізувати ризики для інвесторів та ринку загалом.

Звіт Королівської Скарбниці Великобританії про нагляд у сфері ПВК/ФТ у 2023-24 роках[3]



Річний звіт Міністерства фінансів Великобританії щодо протидії ВК та ФТ за 2023-2024 роки є детальним аналізом стану, тенденцій та ефективності наглядової діяльності у сфері ПВК/ФТ. Документ охоплює інформацію про роботу 25 спеціалізованих наглядових органів, які контролюють понад 90 тисяч підприємств, що здійснюють діяльність, яка може бути використана для ВК та ФТ. У звіті представлено розгорнуту інформацію щодо процедур реєстрації та верифікації підприємств, а також оцінки ризиків, що притаманні конкретним секторам економіки.

Значна увага приділяється застосуванню ризик-орієнтованого підходу до нагляду, який дозволяє максимально ефективно використовувати ресурси та сфокусуватись на найбільш вразливих до ризиків секторах. Серед таких виділяються сектор роздрібних банківських послуг, послуг електронних грошей, управління активами, криптовалютні компанії та гральний бізнес, особливо дистанційні казино, що демонструють стабільно високі ризики щодо ВК/ФТ.

Документ описує нові впроваджені показники ефективності наглядової діяльності, серед яких кількість та результати проведених перевірок, аналіз поданих повідомлень про підозрілу діяльність (SARs), а також якість цих повідомлень. У звіті зазначається, що рівень відмов у реєстрації для криптовалютних компаній залишається дуже високим (до 86%), що свідчить про недостатню відповідність їхніх внутрішніх систем контролю чинним нормативним вимогам.

Окрім практичних аспектів наглядової діяльності, звіт включає підготовчі роботи до наступного раунду взаємної оцінки Великобританії Групою розробки фінансових заходів боротьби з відмиванням коштів (FATF), що запланована на 2028 рік. Особливістю цієї оцінки є посилений

[3] https://assets.publishing.service.gov.uk/media/67d04713dbe565b4fe307835/AML_Annual__Report.pdf

акцент на ефективності нагляду за фінансовими інституціями та постачальниками послуг з віртуальними активами.

Особлива увага приділена необхідності удосконалення процесів належної перевірки клієнтів (CDD) та посилення заходів з виявлення та контролю підвищених ризиків, зокрема у фінансових установах та казино. Значною мірою увага також сконцентрована на покращенні процедур оцінки ризиків, які мають враховувати специфіку діяльності компаній, їхні клієнтські бази та території обслуговування.

Висновки:

- Необхідність посилення контролю за компаніями, що надають послуги з криптоактивами через високий відсоток відмов у реєстрації (86%), рекомендовано покращити процедури оцінки та внутрішнього контролю цих компаній.
- Посилення застосування процедур належної перевірки клієнтів (CDD), особливо в казино та серед компаній, які надають фінансові послуги, через високу частку виявлених недоліків.
- Підвищення ефективності ризик-орієнтованого підходу, зокрема шляхом активнішого використання інноваційних аналітичних інструментів для раннього виявлення ризиків.
- Збільшення взаємодії та інформаційного обміну між регуляторами, приватним сектором та правоохоронними органами з метою більш оперативного виявлення та реагування на загрози ВК/ФТ.

Звіт окремо наголошує на важливості співпраці та координації між наглядовими органами, правоохоронними структурами та приватним сектором. Така взаємодія необхідна для ефективного обміну інформацією, своєчасного виявлення потенційних загроз та швидкого реагування на них, що є критичним у боротьбі з економічною злочинністю.

Таким чином, звіт надає комплексний огляд стану протидії ВК та ФТ у Великобританії, визначає ключові пріоритети наглядової діяльності та рекомендує заходи, необхідні для посилення ефективності системи AML/CTF в країні.

Етичні принципи нових технологій: посібник від Europol [4]

Документ, розроблений Стратегічною групою з питань технологій та етики у співпраці з Europol Innovation Lab та European Clearing Board (EuCB), є методичним посібником для правоохоронних органів щодо оцінки нових технологій із точки зору етичних принципів і дотримання прав людини. Його основна мета – розробка структурованого підходу до ухвалення рішень щодо застосування технологічних рішень у правоохоронній діяльності з урахуванням ключових моральних, правових та соціальних аспектів. Документ орієнтований на забезпечення балансу між безпекою громадян, ефективністю правоохоронних органів та захистом прав людини.

Технологічний прогрес значно вплинув на діяльність правоохоронних органів у всьому світі. Новітні цифрові інструменти, такі як штучний інтелект, аналітика великих даних, автоматизоване розпізнавання облич та відео-аналітика, дозволяють підвищити ефективність боротьби зі злочинністю. Водночас, їх використання викликає серйозні етичні питання, пов'язані з можливим порушенням конфіденційності, прав людини та ризиком неправомірного використання таких технологій. Для вирішення цих викликів було створено

[4] https://www.europol.europa.eu/cms/sites/default/files/documents/Assessing-Technologies-in-Law-enforcement.pdf

Стратегічну групу з питань технологій та етики, яка спирається на досвід, принципи європейського права та аналіз етичних стандартів у сфері технологій.

Документ розроблено у формі «живого документа», що дозволяє адаптувати його до нових технологічних реалій. Він є не лише практичним посібником для оцінки конкретних технологій, а й інструментом для узгодження спільних етичних підходів між правоохоронними органами різних країн ЄС.

Основою документа є методологія оцінки, яка складається із семи послідовних етапів, що дозволяють системно аналізувати нові технології з урахуванням їхнього впливу на суспільство.

1. Формулювання моральної проблеми – визначення потенційних етичних ризиків, пов'язаних із використанням технології, через аналіз суспільних реакцій, занепокоєнь та можливих конфліктів між цінностями.
2. Встановлення релевантних фактів – збирання ключової інформації про технологію, її можливості, обмеження та правові аспекти.
3. Ідентифікація зацікавлених сторін – визначення всіх груп, які можуть бути безпосередньо або опосередковано зачеплені впровадженням технології (громадяни, підозрювані, жертви злочинів, правоохоронні органи, приватний сектор тощо).
4. Визначення нормативних цінностей – оцінка того, які фундаментальні етичні принципи стосуються конкретного випадку. Основними цінностями є:
    - Прозорість – право громадян знати, як і для чого використовуються технології.
    - Справедливість – недопущення дискримінації та забезпечення рівних умов для всіх.
    - Конфіденційність – захист персональних даних і права на приватність.
    - Підзвітність – встановлення відповідальності за використання технології.
5. Формулювання можливих рішень – розробка варіантів впровадження технології, які максимально враховують визначені цінності.
6. Оцінка варіантів та обґрунтування вибору – аналіз допустимості кожного рішення, оцінка його правомірності, наслідків для суспільства та потенційних ризиків.
7. Підсумковий аналіз та узагальнення висновків – формування обґрунтованого висновку щодо етичної прийнятності технології та її можливого регулювання.

Цей підхід дозволяє уникати одноосібних або політично мотивованих рішень, роблячи процес оцінки технологій прозорим, логічним і науково обґрунтованим.

Висновки:

- **Технології у правоохоронній діяльності повинні відповідати принципам прозорості, справедливості, конфіденційності та підзвітності.** Перед впровадженням необхідно оцінювати їхній вплив на права людини та публічне сприйняття.
- **Нові технології повинні мати механізми контролю та аудитів, щоб уникнути упередженості та зловживань.** Наприклад, AI-алгоритми повинні бути пояснюваними, а автоматизовані рішення – переглядатися людиною перед застосуванням.
- **Ризики порушення конфіденційності та етичні дилеми мають бути ретельно збалансовані із суспільними вигодами.** Наприклад, відео-аналітика та AI-ризик-оцінка можуть покращити безпеку, але водночас можуть бути неправильно використані або викликати супротив суспільства.
- **Залучення громадськості до обговорення технологічних нововведень сприяє їхньому прийняттю та ефективності.** Перед впровадженням інновацій доцільно проводити консультації, тестування та поетапне впровадження з оцінкою впливу.

Крім цього, документ містить аналіз п'яти практичних кейсів, які ілюструють застосування методології до реальних або гіпотетичних технологій.

- Відео-аналітика – використання AI-алгоритмів для автоматичного аналізу записів з камер відеоспостереження. Основний ризик – потенційне порушення конфіденційності громадян та масове спостереження за людьми. Висновок: застосування можливе лише після консультацій із суспільством та з обмеженням на конкретні випадки.
- Прогнозування рецидиву у справах домашнього насильства – система AI аналізує дані щодо нападників для оцінки ризику повторного насильства. Основні виклики: можлива дискримінація, відсутність прозорості алгоритмів. Висновок: впровадження має бути поступовим, з обов'язковим людським контролем.
- Автоматизований скрапінг відкритих даних – використання алгоритмів для пошуку викраденого майна на онлайн-майданчиках. Основні ризики: незаконне втручання у персональні дані, порушення умов використання платформ. Висновок: на поточному етапі неприйнятний метод, необхідно розробити альтернативні підходи.
- Чат-бот для боротьби з сексуальним насильством – алгоритм аналізує чати, виявляючи ознаки експлуатації дітей. Основні ризики: масове стеження, неточність алгоритмів. Висновок: прийнятний у спрощеній формі з віковими обмеженнями для аналізу користувачів.
- Автоматизований аналіз великих масивів даних – ризики неправильного трактування інформації та "функціонального дрейфу" технологій. Висновок: використання можливе за умови чітких процедур контролю.

Кожен кейс демонструє необхідність зваженого підходу до використання технологій у сфері правопорядку. Незважаючи на потенційні переваги, жодна технологія не повинна впроваджуватися без ретельного аналізу її соціального та етичного впливу.

Шахрайство та кіберзлочинність в Сінгапурі: ключові факти [5]

Інформаційна стаття, опублікована 25 лютого 2025 року на вебсайті Сінгапурської поліції (Singapore Police Force, SPF), базується на щорічному звіті про шахрайство та кіберзлочини за 2024 рік і має на меті інформувати громадськість про масштаби проблеми, основні тенденції, профілі жертв, ключові види шахрайства та заходи, які вживає поліція для боротьби з цими злочинами. Основний акцент зроблено на тому, що шахрайство та кіберзлочини залишаються серйозною загрозою, але пильність громадян може значно знизити ризики.

Стаття відкривається загальною статистикою, яка демонструє зростання проблеми: у 2024 році загальна кількість випадків шахрайства та кіберзлочинів у Сінгапурі зросла на 10,8% — до 55 810 випадків порівняно з 50 376 у 2023 році. З них 51 501 випадок класифіковано як шахрайство, що на 10,6% більше, ніж 46 563 у попередньому році. Ще більш вражаючим є зростання загальної суми збитків — на 70,6%, до щонайменше 1,1 мільярда сінгапурських доларів (SGD) у 2024 році порівняно з 651,8 мільйона SGD у 2023 році. Автори пояснюють цей стрибок невеликою кількістю справ із надзвичайно високими втратами, наприклад, чотири випадки склали 237,9 мільйона SGD. Антишахрайський підрозділ (ASCom) зміг повернути понад 182 мільйони SGD, що

[5] https://www.police.gov.sg/Media-Room/Police-Life/2025/02/Five-Things-You-Should-Know-about-the-Annual-Scams-and-Cybercrime-Brief-2024

знизило чисті втрати до приблизно 930 мільйонів SGD, а завдяки проактивним діям вдалося запобігти потенційним збиткам на суму 483 мільйони SGD, що свідчить про певну ефективність зусиль поліції.

Далі стаття звертає увагу на профіль жертв шахрайства, зазначаючи, що у 2024 році 70,9% постраждалих були молодше 50 років, тобто молодь та дорослі становили більшість. Однак літні люди (65 років і старше), хоч і складали меншу частку жертв, втрачали найбільші суми в середньому на одного постраждалого. Різні вікові групи виявилися вразливими до різних типів шахрайства: особи до 19 років частіше ставали жертвами шахрайства в електронній комерції, шахрайства з працевлаштуванням і фішингу; ті, кому від 20 до 49 років, мали схожий профіль уразливості; особи віком 50–64 роки частіше потерпали від фішингу, інвестиційних шахрайств і шахрайств типу "дзвінок від фальшивого друга"; а літні люди (65+) найчастіше стикалися з тими ж фішингом, інвестиційними шахрайствами та "фальшивими дзвінками від друзів". Ці дані підкреслюють необхідність адаптованої просвітницької роботи для різних вікових груп.

Значну частину статті присвячено аналізу топ-10 видів шахрайства за кількістю випадків і сумою збитків. Серед них виділяються шахрайства в електронній комерції (9 043 випадки, 156,2 млн SGD збитків, середній збиток 17 281 SGD на випадок), фішинг (8 552 випадки, 59,4 млн SGD, середній збиток 6 955 SGD), інвестиційні шахрайства (6 814 випадків, 320,7 млн SGD, середній збиток 47 077 SGD), а також шахрайство з працевлаштуванням (1 665 випадків, 17,5 млн SGD) і шахрайство типу "дзвінок від друга" (1 504 випадки, 151,3 млн SGD, середній збиток 100 622 SGD). Інші види включають шахрайство від імені урядових осіб, використання шкідливого програмного забезпечення та імперсонацію в соціальних мережах. Примітно, що деякі види шахрайства, такі як "дзвінок від друга", шахрайство з використанням шкідливого ПЗ і соціальних мереж, показали значне зниження як за кількістю випадків, так і за сумами збитків завдяки заходам уряду, банків і телекомунікаційних компаній. Натомість фішинг, інвестиційні шахрайства, шахрайства в електронній комерції та від імені урядових осіб продемонстрували зростання.

Висновки:

- **Зростання збитків від шахрайства вимагає пильності:** Загальні збитки зросли до 1,1 млрд SGD у 2024 році (+70,6% порівняно з 2023), тому громадянам слід перевіряти джерела транзакцій і уникати поспішних переказів, особливо під тиском незнайомців.
- **Молодь — основна ціль, але літні люди втрачають більше:** 70,9% жертв — молодше 50 років, але середні збитки вищі серед осіб 65+. Рекомендується таргетована просвіта: для молоді — про фішинг і електронну комерцію, для літніх — про інвестиційні шахрайства.
- **Інвестиційні шахрайства — найдорожчі:** Збитки від інвестиційних шахрайств склали 320,7 млн SGD (47 077 SGD на випадок). Уникайте неперевірених інвестиційних пропозицій і консультуйтеся з фінансовими експертами перед вкладеннями.
- **Посилення законодавства та операцій працює:** Зменшення деяких видів шахрайства (наприклад, "дзвінок від друга") і повернення 182 млн SGD показують ефективність заходів ASCom. Громадянам слід повідомляти про підозрілі дії для підтримки поліції.

Особливу увагу приділено тенденціям у методах шахрайства: у 82,4% випадків жертви самостійно здійснювали перекази (self-effected transfers), коли шахраї не отримували прямого доступу до їхніх рахунків, а використовували методи соціальної інженерії та обману, щоб переконати жертв переказати кошти. Це вказує на високу залежність шахраїв від психологічних маніпуляцій, а не від технічних зломів. У контексті боротьби з цими злочинами стаття детально описує заходи поліції, які включають як законодавчі, так і оперативні дії. Наприклад, застосовуються закони, такі як

Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act (CDSA) і Computer Misuse Act (CMA). Наводиться випадок, коли особа, яка за 300 SGD надала доступ до свого банківського рахунку, була засуджена до шести місяців ув'язнення після того, як через її рахунок відмили понад 160 000 SGD. З 1 січня 2025 року також набули чинності зміни до Miscellaneous Offences Act, спрямовані на боротьбу зі зловживанням місцевими SIM-картками для шахрайства. На оперативному рівні ASCom разом із командами боротьби з шахрайством у семи поліцейських підрозділах провели 25 загальнонаціональних операцій, розслідуючи понад 8 000 справ "грошових мулів" і шахраїв, а також притягнули до суду понад 660 осіб, із них понад 110 — за новими положеннями CDSA та CMA.

Таким чином, у 2024 році шахрайство та кіберзлочини в Сінгапурі зросли, завдавши збитків на 1,1 мільярда SGD, але пильність громадян і заходи поліції, такі як повернення 182 мільйонів SGD та запобігання втратам на 483 мільйони SGD, демонструють прогрес у боротьбі з цією загрозою. Найуразливішими залишаються особи до 50 років, хоча літні люди втрачають найбільше, а інвестиційні шахрайства лідирують за сумою збитків. Поліція посилює законодавство й операції, закликаючи громадськість бути обачною.

Морські реєстри та фінансування розповсюдження[6]

Документ є фактичним звітом, підготовленим Азіатсько-Тихоокеанською групою з протидії відмиванню коштів (APG) та Управлінням ООН з наркотиків і злочинності (UNODC), присвяченим ризикам фінансування розповсюдження зброї масового знищення (ФР) через зловживання системою реєстрації суден. У ньому розглядається, яким чином морські реєстри можуть бути використані для обходу цільових фінансових санкцій (ЦФС) ООН, а також пропонуються заходи щодо запобігання таким загрозам. Документ пояснює роль, яку відіграють реєстри суден у схемах ФР, та наводить конкретні випадки з міжнародної практики, що демонструють масштаби проблеми.

Основний акцент зроблено на міжнародних зобов'язаннях держав, які виникають із Рекомендацій FATF, резолюцій Ради Безпеки ООН та інших міжнародних стандартів у сфері протидії фінансуванню розповсюдження. Зокрема, FATF вимагає, щоб країни вживали заходів щодо виявлення, пом'якшення та управління ризиками ФР, а також негайно заморожували активи осіб і організацій, внесених до санкційних списків ООН. Згідно з резолюціями 1718 (2006) та 2231 (2015), країни повинні запобігати наданню фінансових ресурсів або інших активів зазначеним особам, зокрема через морські реєстри, страхування суден та видачу ліцензій.

Звіт пояснює механізми, за допомогою яких реєстри суден можуть сприяти ФР, зокрема через використання «зручних прапорів» (Flags of Convenience, FoC). Ця схема передбачає реєстрацію суден в юрисдикціях, які мають слабкий контроль та недостатній нагляд. Це дає змогу зловмисникам приховувати справжню власність судна, а також здійснювати перевезення матеріалів, які можуть бути використані у програмах створення зброї масового знищення. Прикладами зловживань є транзитні перевезення вугілля, операції ship-to-ship (STS) на відкритому морі та фальсифікація реєстраційних документів суден.

[6] https://apgml.org/news/details.aspx?pcPage=1&n=7233

Документ рекомендує державам реалізовувати суворіші заходи контролю на етапі реєстрації суден, зокрема перевіряти власників та керівників судноплавних компаній, здійснювати додаткові процедури належної перевірки та забезпечувати дотримання санкційних вимог. Окрему увагу приділено проблемам, пов'язаним із передачею функцій реєстрації суден приватним компаніям, особливо якщо такі компанії базуються в інших юрисдикціях. Це створює складнощі в забезпеченні відповідності нормам FATF і ООН, адже держава не може передати відповідальність за дотримання санкційних вимог.

Документ містить аналіз низки реальних кейсів, які демонструють ризики використання морських реєстрів для ФР. Наприклад, у звіті APG 2024 розглянуто випадок, коли китайські компанії використовували судна з іноземними прапорами для незаконного постачання нафти суднам Північної Кореї, що перебувають під санкціями ООН. Інший випадок із островів Кука демонструє, як судно, зареєстроване через трастову компанію в одній країні, брало участь у незаконних STS-операціях з північнокорейськими суднами, що призвело до його виключення з реєстру та накладення санкцій.

Також у звіті розглядається звітність Групи експертів ООН, яка регулярно виявляє спроби КНДР використовувати міжнародні судноплавні реєстри для обходу санкцій. Наприклад, було задокументовано випадки, коли північнокорейські судна змінювали прапор у процесі переходу між портами, фальсифікували документацію та відключали системи автоматичної ідентифікації (AIS), щоб уникнути виявлення.

Висновки:

- **Необхідність посилення контролю за реєстрацією суден.** Реєстрація суден у юрисдикціях із низьким рівнем контролю створює значні ризики ФР. Держави повинні запроваджувати суворі перевірки власників суден та кінцевих бенефіціарів, щоб запобігти використанню реєстрів для обходу санкцій.
- **Розширення обов'язків реєстраторів суден у рамках санкцій ООН.** Відповідно до резолюцій ООН, судна, які перебувають під контролем підсанкційних осіб, вважаються їх економічними активами та підлягають замороженню. Реєстраційні органи повинні вживати негайних заходів щодо виключення таких суден із реєстру та обмеження їхньої діяльності.
- **Попередження зловживань схемою "зручних прапорів".** Використання "зручних прапорів" є одним із основних методів обходу санкцій та ФР. Держави повинні переглянути свою політику у сфері реєстрації суден, особливо щодо випадків, коли реєстраційні органи діють через приватні компанії або під юрисдикцією інших держав.
- **Посилення міжвідомчої та міжнародної співпраці.** Для ефективного протистояння схемам ФР необхідна тісна співпраця між державними органами, реєстрами суден, фінансовими установами та міжнародними організаціями. Це включає обмін розвідувальною інформацією, проведення спільних розслідувань та посилення санкційного контролю на рівні держав.

Загалом, звіт наголошує, що реєстри суден є критичною точкою у глобальній системі боротьби з ФР, і рекомендує державам посилити механізми нагляду та перевірки, щоб запобігти їх зловживанню.

Санкції

Шлях обходу санкцій: Як Киргизстан став воротами для люксових автомобілів до Росії [7]

Стаття від Organized Crime and Corruption Reporting Project (OCCRP), опублікована 26 лютого 2025 року, є детальним розслідуванням того, як Киргизстан перетворився на ключовий транзитний центр для постачання санкційних автомобілів до Росії після введення широких економічних санкцій Європейським Союзом, США та Південною Кореєю у відповідь на повномасштабне вторгнення Росії в Україну в лютому 2022 року. Автори розслідування — Болт Теміров (Temirov Live), Екліяр Арикбаєв (OCCRP), Анастасія Короткова (IStories) та Елуаз Лаян (Forbidden Stories) — спираються на статистичні дані, інтерв'ю з інсайдерами, аналіз соціальних мереж і свідчення джерел, щоб розкрити механізми обходу санкцій через Центральну Азію, зокрема через Киргизстан.

Центральною темою розслідування є діяльність московського автосалону Berg Auto Premium, який, попри санкційні обмеження, пропонує вражаючий асортимент люксових автомобілів, таких як Rolls-Royce Cullinan вартістю майже $1 млн, Tesla Cybertruck і Porsche Cayenne Coupé. Журналісти з'ясували, що ці машини потрапляють до Росії через складні схеми "паралельного імпорту", де Киргизстан виступає посередником. Один із прикладів: репортерка IStories під прикриттям зателефонувала до Berg Auto і запитала про Porsche 911 Turbo, модель, яку важко знайти в Росії через заборону ЄС на експорт автомобілів вартістю понад 50 000 євро. Продавець запевнив, що будь-яку модель із офіційного німецького сайту Porsche можна доставити через Грузію чи Киргизстан — спочатку морем або літаком, а потім до Москви. Він наголосив, що це "складно, але можливо", а автомобіль залишиться європейського виробництва.

Дані UN Comtrade підкріплюють масштабність явища: якщо в 2020–2021 роках Киргизстан імпортував автомобілів із країн ЄС на $8,8 млн, то в наступні два роки цей показник злетів до $730 млн — зростання в понад 80 разів. Економіст Карл Греку, коментуючи це для Forbidden Stories, зауважив, що таке різке збільшення не пов'язане з внутрішнім попитом у Киргизстані, а є очевидним свідченням перенаправлення машин до Росії. Для порівняння, Казахстан за той же період збільшив імпорт із $154 млн до трохи більше $1 млрд, але Киргизстан вирізняється своєю роллю як менш помітного, але ефективного хаба.

Розслідування називає конкретних учасників схеми. Азіз Жиргалбеков, контакт Berg Auto, підтвердив, що автомобілі імпортуються з Європи та Південної Кореї через Киргизстан, причому для уникнення перевірок їх оформлюють на приватних осіб, а не компанії. Він описав Бішкек як тісну спільноту, де "всі знають один одного і співпрацюють", а імпорт не обмежується автомобілями — через "паралельний імпорт" надходить багато інших товарів. Інший фігурант, Сиргакбек Атишов, активно демонструє свою діяльність у TikTok та Instagram: у липні 2023 року він хвалився доставкою Range Rover до Бішкека з подальшим відправленням до Москви, а в квітні 2024 року показав купівлю Audi RS Q8 у Південній Кореї для Berg Auto, обіцяючи доставку за 15 днів. У грудні того ж року він організував авіаперевезення Audi RS6 із Франкфурта до Бішкека для того ж автосалону. Ще одна особа, Адилет Тилдебаєв, асоціюється з імпортом

[7] https://www.occrp.org/en/feature/we-know-no-borders-how-kyrgyzstan-became-a-hub-for-sanctioned-car-exports-to-russia

через Киргизстан, що підтверджується даними телефонних контактів із Getcontact, де його номер пов'язаний із фразами на кшталт "Adilet Brings Cars Kyrgyz" чи "Adilet Cars From Europe".

Berg Auto Premium, заснований Марком Бергом 7 жовтня 2023 року позиціонується як успішний бізнес, що скористався санкційними лазівками. У інтерв'ю російському журналу Берг розповів про використання "паралельного імпорту" і з'явився в образі сучасного підприємця з дорогими аксесуарами. Хоча прямих доказів зв'язку автосалону з киргизькими чиновниками немає, розслідування вказує на тісну співпрацю між киргизькими та російськими посередниками. Зокрема, російські імпортні записи за 2023–2024 роки показують, що третина киргизьких компаній, які виступають посередниками в експорті автомобілів і запчастин до Росії, мають російських акціонерів. Джерело в киргизькій митниці, яке побажало залишитися анонімним, повідомило, що багато машин проходять через країну лише на папері, а реальні власники уникають митних процедур, використовуючи спрощений режим для "особистих" автомобілів.

Ширший контекст розкриває Тимур Умаров із Carnegie Russia Eurasia Center: Киргизстан скористався санкціями, фінансовими обмеженнями та різними податковими режимами, щоб стати хабом, компенсуючи брак природних ресурсів, на відміну від Казахстану. Виробники автомобілів, такі як Mercedes, Rolls-Royce і Porsche, заявили про дотримання санкцій і засудили дії сторонніх продавців, але їхня відповідальність залишається формальною. Водночас розслідування підкреслює небезпеку для журналістів: у січні 2024 року 11 репортерів Temirov Live були заарештовані в Киргизстані, двоє отримали тюремні терміни за "організацію масових заворушень", що ілюструє тиск на тих, хто викриває подібні схеми.

Таким чином, стаття не лише документує механізми обходу санкцій через Киргизстан, але й показує, як глобальні обмеження створюють нові можливості для посередників, водночас ускладнюючи життя розслідувачам у регіоні.

Висновки:

- **Закриття лазівок у санкціях:** Західним країнам (ЄС, США, Південна Корея) необхідно посилити контроль за експортом люксових автомобілів до країн Центральної Азії, зокрема Киргизстану, шляхом запровадження вторинних санкцій або детальнішого моніторингу кінцевих отримувачів, щоб зупинити потік санкційних товарів до Росії.
- **Митна прозорість у Киргизстані:** Киргизьким митним органам слід запровадити суворіший облік імпорту автомобілів, зокрема скасувати спрощену процедуру для "особистих" машин, і розкривати дані про реальних власників, а не лише брокерів, для зменшення ролі країни як транзитного хаба.
- **Розширення розслідувань:** Міжнародним журналістським організаціям варто зосередитися на відстеженні конкретних посередників (наприклад, Атишова, Жиргалбекова, Тилдебаєва) та їхніх зв'язків із російськими дилерами, використовуючи дані соціальних мереж і телефонних контактів для викриття ширшої мережі.
- **Тиск на автовиробників:** Брендам, таким як Porsche і Audi, необхідно активніше співпрацювати з урядами для припинення несанкціонованих поставок через треті країни, включаючи розірвання контрактів із дилерами, які порушують санкційні режими, замість лише формальних заяв про відповідність.

Звіти окремих інституцій та експертів

Глобальні фінансові виклики 2025: як змінюється регуляторне середовище та що це означає для бізнесу[8]

Звіт аналізує основні виклики, які постануть перед фінансовими установами у 2025 році, і окреслює ключові регуляторні пріоритети, що визначатимуть розвиток фінансового сектора. У документі розглядається широкий спектр тем, зокрема зростаюча фрагментація регулювання, стійкість фінансових установ до зовнішніх загроз, захист прав споживачів і управління ризиками. Головний висновок звіту полягає в тому, що глобальна регуляторна система стає дедалі більш складною через політичну напруженість, економічну нестабільність та технологічні зміни, що створює значні виклики для фінансових компаній, особливо тих, що працюють у міжнародному середовищі.

Одним із головних аспектів звіту є зростаюча фрагментація регуляторного середовища. Глобальні фінансові установи стикаються з тим, що єдині стандарти поступово поступаються місцем національним підходам до регулювання. Це особливо помітно у сфері цифрових активів, де в різних країнах запроваджуються абсолютно різні механізми нагляду та контролю. Наприклад, у Дубаї створено окремого регулятора для віртуальних активів (Virtual Assets Regulatory Authority), тоді як у Європейському Союзі стейблкоїни регулюються відповідно до існуючих фінансових норм, а в США спостерігається тенденція до послаблення нагляду за цифровими активами. Важливим фактором є й те, що регуляторні вимоги до банківського капіталу стають менш узгодженими через нерівномірне впровадження Basel 3.1 у різних юрисдикціях, що створює перешкоди для міжнародних банків. Окремо варто зазначити про розвиток регулювання штучного інтелекту: підходи до його нагляду та контролю значно відрізняються в різних регіонах, що може призвести до регуляторного арбітражу.

Другий важливий блок звіту присвячений підвищенню стійкості фінансового сектора до зовнішніх загроз. Регулятори все більше зосереджуються на операційній стійкості фінансових установ, особливо в контексті ризиків, пов’язаних із технологічною залежністю від третіх сторін. Це стало особливо актуальним після масового збою в IT-інфраструктурі у 2024 році, який продемонстрував вразливість фінансової системи до технічних збоїв. У відповідь на це Європейський Союз запроваджує Digital Operational Resilience Act (DORA), який вимагатиме від фінансових установ забезпечення високих стандартів кіберстійкості та ретельного управління ризиками третіх сторін. Аналогічні заходи впроваджуються в Австралії, Великій Британії та Гонконзі. Крім того, у звіті наголошується на зростанні ролі небанківських фінансових установ (тіньових банків), які на сьогодні складають близько 47% глобальних активів. Відсутність чіткої регуляції для цих установ може створити потенційні системні ризики, тому очікується подальше посилення контролю з боку міжнародних органів, зокрема Financial Stability Board (FSB).

Окрема увага приділяється боротьбі з фінансовими злочинами та санкціям. Уряди та регулятори посилюють нагляд за транзакціями, особливо у сфері цифрових активів і небанківських платіжних сервісів, які можуть використовуватися для обходу санкцій. У Європейському Союзі створено новий наднаціональний орган для безпосереднього нагляду за високоризиковими

[8] https://www.ey.com/content/dam/ey-unified-site/ey-com/en-gl/insights/financial-services/documents/ey-gl-global-financial-services-regulatory-outlook-01-2025.pdf?AA.tsrc=ownedsocial&WT.mc_id=18700301&utm_campaign=65c0c43ffa662300012c6ef0&utm_content=67ac3c92404ea800019b7edd&utm_medium=smarpshare&utm_source=linkedin#:~:text=More%20scrutiny%20of%20firms'%20operational,will%20also%20remain%20a%20focus.

фінансовими установами, що свідчить про значне посилення контролю. У США FinCEN та SEC пропонують розширення режиму ПВК/ФТ на інвестиційні компанії, а в Австралії оновлюються закони щодо нагляду за криптоактивами.

Ще одним ключовим питанням є захист прав споживачів та забезпечення їхньої фінансової безпеки. Регулятори розширюють вимоги до фінансових установ щодо забезпечення прозорості продуктів та послуг. У Великій Британії набув чинності новий регуляторний стандарт «Consumer Duty», який встановлює принципи етичного поводження з клієнтами, а в Сінгапурі та Японії впроваджуються схожі ініціативи. Збільшується увага до питань фінансової інклюзії: у США, ЄС та Великій Британії впроваджуються заходи щодо покращення доступу до фінансових послуг для малозабезпечених верств населення. Також зростає увага до боротьби з фінансовим шахрайством, особливо в контексті авторизованих платіжних шахрайств (APP fraud). У Великій Британії впроваджено механізм обов'язкового відшкодування жертвам шахрайських переказів, аналогічні ініціативи розглядаються в Австралії та США.

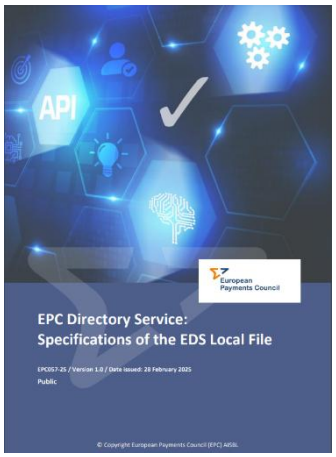
Фінальний блок звіту стосується управління ризиками та корпоративної відповідальності. Події 2023 року, включаючи банкрутства великих банків, показали, що недоліки в управлінні ризиками можуть мати катастрофічні наслідки. Регулятори значно посилюють вимоги до нагляду за корпоративним управлінням, особливо у сфері ризиків, пов'язаних із цифровими активами та змінами клімату. У Великій Британії очікується розширення Senior Managers & Certification Regime (SM&CR) на небанківські фінансові установи, а в Австралії впроваджується Financial Accountability Regime для страхових і пенсійних компаній. Очікується подальше посилення відповідальності керівників фінансових установ, включаючи їхню персональну відповідальність за управління ризиками.

Загалом звіт підкреслює, що у 2025 році фінансові установи працюватимуть у складному регуляторному середовищі, яке характеризується високим рівнем фрагментації, посиленими вимогами до кіберстійкості, боротьби з фінансовими злочинами, а також розширенням обов'язків перед споживачами. Фінансові компанії повинні адаптувати

Висновки:

- Глобальна фрагментація регулювання ускладнює діяльність фінансових установ:
  - Фінансові компанії повинні адаптувати операційні моделі до локальних вимог, уникаючи високих витрат.
  - Потрібно розробити стратегії для роботи в умовах нестабільності, використовуючи сценарне планування.
- Регулятори посилюють контроль за фінансовою та операційною стійкістю установ:
  - Компаніям варто оцінити ризики, пов'язані із залежністю від ключових постачальників технологічних рішень, та переглянути плани забезпечення безперервності бізнесу.
  - Очікується посилення стрес-тестування, зокрема на випадок масштабних кіберінцидентів.
- Пріоритетність споживачів у фінансових послугах:
  - Фінансові установи повинні забезпечити високу прозорість продуктів, зменшити складність тарифів та уникати дискримінаційних бар'єрів для малозабезпечених клієнтів.
  - Очікується посилення відповідальності фінансових установ за шахрайські транзакції.
- Управління ризиками та відповідальність керівників – під пильним наглядом регуляторів:
  - Необхідно переглянути внутрішню систему управління ризиками, зокрема щодо криптоактивів, кіберзагроз і змін кліматичних ризиків.
  - Важливо формалізувати відповідальність топменеджерів, щоб уникнути регуляторних санкцій.

Специфікації EDS Local File: Ключовий компонент схеми Verification of Payee (VOP) у європейських платежах[9]



Документ є комплексним технічним керівництвом, що визначає структуру, формат та специфікації локального файлу, який використовується в рамках схеми Verification of Payee (VOP) Європейської платіжної ради (EPC). У документі детально описано, як дані, отримані з EPC Directory Service (EDS), мають зберігатися та використовуватися місцево учасниками схеми для забезпечення безперебійного та безпечного функціонування сервісів, зокрема IBAN-name check, що є вимогою Instant Payment Regulation (IPR). Текст розкриває сутність EDS як ключового елементу, який забезпечує не лише ідентифікацію платіжних сервіс-провайдерів (PSP) за допомогою BIC11 та PSD2 National Authorisation Number (NAN), але й підтримує збереження інформації про ролі, опції та API-ендпоінти (Uniform Resource Identifier, URI), що є необхідними для встановлення довірених зв'язків між учасниками схеми.

Документ підкреслює, що EDS не містить персональних даних або IBAN, оскільки його використання обмежується маршрутизацією інформації між бізнес-суб'єктами, зокрема між платниками та отримувачами платежів, а також між Routing and Verification Mechanisms (RVM), які діють від імені PSP. У тексті описано, що дані, що містяться у файлі, можуть бути представлені у різних форматах, зокрема CSV, XML та JSON, що дозволяє забезпечити максимальну сумісність із різноманітними інформаційними системами та технологічними середовищами учасників схеми. Всі формати використовують кодування UTF-8 та стандартизовану систему іменування файлів, яка включає інформацію про версію, частоту публікації (щоденний оновлений повний файл), тип файлу та дату публікації.

У документі надається детальний опис структурних елементів файлу, що включає інформацію про ідентифікаційні дані PSP (назва, BIC11, країна), а також про специфічні параметри, як-от PSD2 NAN, операційні контакти, ролі та опції учасників, що визначають їхню позицію у схемі VOP. Особлива увага приділяється опису API-ендпоінтів, що є критично важливими для взаємодії між «запитуючими» та «відповідаючими» PSP. Документ пояснює, як за допомогою цих інтерфейсів здійснюється обмін повідомленнями між учасниками, забезпечується авторизація

Висновки:

- **EDS є критичним компонентом для VOP та інших схем EPC.** EDS забезпечує централізоване зберігання інформації про учасників, їхні ролі та інтерфейси API, необхідні для дотримання регламенту SEPA та IPR.
- **Форматування та структура файлів EDS стандартизовані.** Файли підтримують формати CSV, XML та JSON, що дозволяє гнучко інтегрувати дані у різних IT-системах PSP.
- **EDS гарантує перевірку учасників VOP.** Учасники можуть перевірити, чи є їхні контрагенти зареєстрованими PSP, чи підтримують вони певні опції схеми та чи належать до схвалених EPC суб'єктів.
- **Інтерфейс API відіграє ключову роль у взаємодії PSP.** Використання уніфікованих API та стандартизованої авторизації через PSD2 NAN/QWAC підвищує безпеку та ефективність перевірки одержувачів платежів.

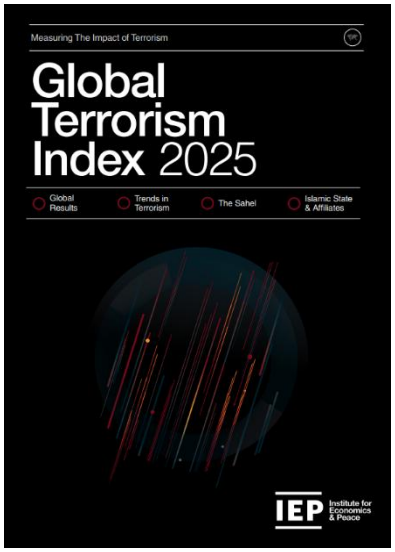
[9] https://www.europeanpaymentscouncil.eu/sites/default/files/kb/file/2025-02/EPC057-25%20v1.0%20EDS_Local_File_specifications_0.pdf

запитів, а також встановлюється пріоритетність використання основних та резервних URL, що гарантує безперебійну роботу системи навіть у випадку змін чи оновлень.

Крім того, у додатках до документа подано роз'яснення щодо абревіатур, що використовуються у специфікаціях (наприклад, API, BIC, NAN, QWAC), а також наведено коди, які використовуються для позначення ролей (наприклад, Requesting PSP, Responding PSP) та опцій (як-от підтримка додаткових ідентифікаційних кодів, таких як LEI, BIC, CBID тощо) у рамках схеми VOP. Окремо розглядаються поняття URI, NAN та QWAC, що дозволяють забезпечити надійну ідентифікацію та авторизацію учасників, підкріплюючи вимоги до безпеки та відповідності регуляторним нормам PSD2.

Таким чином, документ є фундаментальним посібником для розробників, адміністраторів та регуляторів, які впроваджують та експлуатують схеми, пов'язані з перевіркою одержувача платежу та іншими суміжними сервісами, що сприяють підвищенню рівня безпеки та ефективності платіжних операцій у Європейському платіжному просторі.

Глобальний індекс тероризму 2025: Тренди, загрози та нові виклики глобальній безпеці[10]



Звіт, підготовлений Інститутом економіки та миру (IEP), є дванадцятим щорічним аналізом тенденцій у сфері тероризму та його впливу на глобальну безпеку. Основою для цього дослідження є дані з TerrorismTracker, що містять структуровану інформацію про всі зареєстровані терористичні атаки з 2007 року. GTI 2025 оцінює рівень терористичної загрози у світі, аналізуючи динаміку атак, регіональні відмінності, роль ключових терористичних угруповань та геополітичні чинники, які впливають на поширення тероризму.

Звіт демонструє, що, попри загальне зниження кількості смертей унаслідок тероризму у 2024 році, проблема продовжує загострюватися через зміни в регіональних осередках активності та адаптивність терористичних груп. Число країн, у яких було зафіксовано хоча б одну атаку, зросло з 58 до 66, що є найвищим показником з 2018 року. Кількість загиблих знизилася на 13%, до 7 555 осіб, але це скорочення здебільшого пов'язане зі спадом терористичної активності в М'янмі. Без цього впливу загальна кількість атак у світі збільшилася б на 8%, що свідчить про продовження тенденції до поширення тероризму. Особливе занепокоєння викликає той факт, що вперше за сім років більше країн погіршили свої показники боротьби з тероризмом (45), ніж покращили (34).

Сахель став головним регіоном терористичної активності у світі, на нього припадає 51% усіх смертей унаслідок терактів. Буркіна-Фасо знову залишається країною, яка найбільше постраждала від тероризму, хоча кількість атак і смертей там скоротилася відповідно на 57% та 21%. Водночас Нігер зафіксував найбільший приріст смертей від терористичних атак – на 94% (до 930 жертв), що демонструє, наскільки нестабільним може бути прогрес у боротьбі з тероризмом. Поширення насильства в цьому регіоні пов'язане не лише з діяльністю традиційних угруповань, таких як Jamaat Nusrat Al-Islam wal Muslimeen (JNIM) та Ісламська держава (IS), а й із геополітичними змінами. Альянс держав Сахелю (Малі, Буркіна-Фасо, Нігер) зміцнює співпрацю з Росією та Китаєм, дистанціюючись від Заходу, що створює нові виклики для контртерористичних зусиль у регіоні.

[10] https://www.economicsandpeace.org/wp-content/uploads/2025/03/Global-Terrorism-Index-2025.pdf

Західні країни також зазнали суттєвого впливу від змін у тактиці терористів. У 2024 році кількість атак у Західному світі зросла з 32 до 52, причому більшість з них здійснювали одиночні учасники, які стали екстремістами через онлайн-пропаганду. Залучення молоді до екстремістських ідей через соціальні мережі, ігрові платформи та зашифровані месенджери стає дедалі помітнішою загрозою. У Європі кількість терактів подвоїлася, досягнувши 67 атак, що включають напади, організовані Ісламською державою та ХАМАС. Найбільше атак зазнали Німеччина, Швеція, Австралія, Фінляндія, Нідерланди, Данія та Швейцарія. Паралельно зафіксовано різке зростання антисемітських і ісламофобських злочинів на тлі війни у Газі – у США кількість зареєстрованих нападів на єврейську громаду зросла на 270% усього за два місяці.

Ісламська держава та її афілійовані групи залишаються найсмертоноснішою терористичною мережею у світі, відповідальною за 1 805 смертей у 22 країнах. Найактивніші її осередки діють у Сирії, де зафіксовано 369 атак, що спричинили 708 смертей. Також Ісламська держава – Хорасан (IS-K) продовжує своє розширення, діючи не лише в Афганістані, а й у Пакистані, Ірані, Росії та Центральній Азії. Вона здійснює вербування через мультимовний онлайн-контент та інструкції з тактики нападів і виготовлення вибухових пристроїв. Примітно, що IS-K взяла на себе відповідальність за дві з найбільших атак 2024 року – вибух у Ірані, що забрав 95 життів, та масове вбивство в Crocus City Hall у Москві, де загинуло 144 людини.

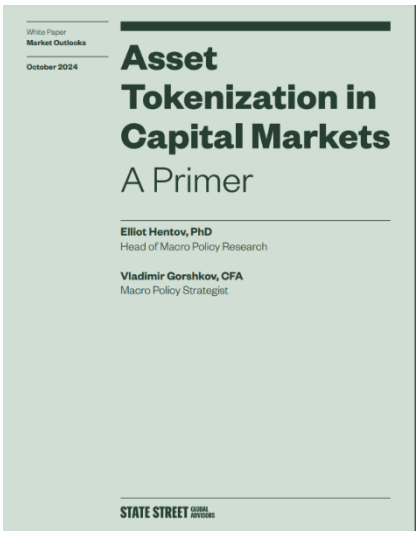
Сучасні терористичні організації дедалі активніше використовують штучний інтелект для створення пропаганди, поширення дезінформації та управління атаками. ШІ та технології дипфейків дозволяють екстремістським групам ефективніше радикалізувати прихильників та поширювати маніпулятивний контент, що створює значні виклики для контррозвідки. Водночас ті ж самі технології можуть бути використані державами для моніторингу поширення екстремістських ідей в онлайн-просторі, ідентифікації загроз у реальному часі та розробки ефективних контрнаративів.

Висновки:

- Необхідність посилення міжнародної співпраці у боротьбі з тероризмом.
  - Оскільки терористичні мережі розширюють свою діяльність на нові регіони, потрібно покращити механізми міжнародного обміну розвідувальною інформацією.
  - Пріоритетом має стати боротьба з фінансуванням тероризму, особливо в Сахелі, де незаконний видобуток золота є ключовим джерелом фінансування бойовиків.
- Загроза залучення молоді до екстремістських ідей через онлайн-контент.
  - Різке зростання кількості одиночних терористів серед молоді потребує впровадження нових механізмів контролю за поширенням екстремістських ідей в онлайн-просторі.
  - Рекомендація: посилення співпраці з соціальними мережами для моніторингу потенційних загроз, блокування екстремістського контенту та розробки контрнаративів.
- Зростання впливу ШІ у тероризмі та контртероризмі.
  - Терористи активно використовують ШІ для створення дезінформації та пропаганди. У відповідь спецслужби мають впроваджувати алгоритми раннього виявлення загроз.
  - Рекомендація: посилення досліджень у сфері застосування ШІ для аналізу даних терористичних атак та прогнозування ризиків.
- Розширення терористичних угруповань у нестабільних регіонах.
  - Тенденції свідчать про експансію терористичних груп за межі традиційних зон активності, особливо в Західну Африку та Центральну Азію.
  - Рекомендація: стратегічний перегляд підходів до стабілізації регіонів, схильних до тероризму, шляхом посилення міжнародної допомоги у сфері безпеки та розвитку.

Загалом, GTI 2025 засвідчує, що тероризм залишається серйозною загрозою глобальній безпеці, адаптуючись до нових умов і технологій. Хоча кількість смертей зменшилася, цей показник приховує зміни в патернах терористичної активності: дедалі більше атак відбувається у нестабільних регіонах Африки та Центральної Азії, а також у Західному світі, де залучення молоді до екстремістських ідей через інтернет стає новим ключовим викликом. Протидія цим тенденціям вимагає нових підходів, зокрема міжнародної співпраці у сфері моніторингу фінансування тероризму, посилення контролю за інформаційним простором і створення інноваційних механізмів раннього виявлення загроз.

Токенізація активів: Революція у фінансових ринках чи еволюційний перехід?[11]



Документ досліджує феномен токенізації активів та її потенційний вплив на ринки капіталу, висвітлюючи ключові технологічні, економічні та регуляторні аспекти. Автори визначають токенізацію як черговий великий технологічний прорив у фінансовій сфері, подібний до переходу від паперових цінних паперів до цифрових записів. Основною рушійною силою цього процесу є технологія розподіленого реєстру (DLT), що дозволяє створювати цифрові активи з можливістю програмованих функцій, миттєвих розрахунків і знижених операційних витрат.

Документ підкреслює, що токенізація відкриває нові можливості для фінансових ринків, зокрема шляхом зменшення ролі посередників, скорочення часу розрахунків до миттєвого виконання (T+0), автоматизації рутинних процесів через смарт-контракти та забезпечення більшої прозорості угод. Найбільші вигоди очікуються у ринках облігацій, альтернативних фондів і комерційної нерухомості, тоді як у сегменті публічних акцій ефект буде менш вираженим через високу ефективність існуючих ринкових механізмів.

Розгляд основних класів активів у документі демонструє, що найбільшу трансформацію відчують облігаційні ринки. Тут токенізація дозволить спростити випуск цінних паперів, знизити витрати на обслуговування та значно покращити ліквідність. Завдяки можливості програмування виплат та автоматизації сервісних функцій, такі інструменти стануть більш привабливими для інвесторів. У секторі альтернативних фондів ключовою зміною стане «демократизація» доступу до раніше ексклюзивних активів, таких як приватний капітал та венчурні фонди. Це стане можливим завдяки зниженню мінімальних порогів входу для інвесторів та полегшенню процесів реєстрації, володіння та передачі часток.

Щодо ринку товарів, документ зазначає, що токенізація вже застосовується у золоті та дорогоцінних металах, а також має потенціал для сільськогосподарської продукції. У випадку металів токенізація забезпечує можливість дроблення активів та спрощує доступ інвесторів до ринку. Проте у сільськогосподарському секторі основний вплив буде зосереджений на покращенні механізмів заставного фінансування та інтеграції виробників у глобальні фінансові ринки.

Публічні акції є найменш перспективним сегментом для масштабної токенізації, оскільки сучасні ринки вже досить ефективні. Основний вплив спостерігається у створенні цифрових аналогів акцій для криптовалютного середовища (наприклад, токенізовані ETF або акції великих

[11] https://www.ssga.com/library-content/assets/pdf/global/digital-assets/2024/asset-tokenization-in-capital-markets.pdf

компаній), що дозволяє криптоінвесторам отримати доступ до традиційних ринків без використання фіатних грошей.

У сфері нерухомості токенізація проявляється насамперед у сегменті фондів та комерційних активів. Завдяки цифровим технологіям інвестори можуть брати участь у реальних проєктах через токенізовані REITs (Real Estate Investment Trusts). Проте масова токенізація індивідуальних активів стикається з численними юридичними та регуляторними викликами, зокрема питаннями прав власності, управління та ліквідності.

Документ також акцентує увагу на ризиках та регуляторних викликах. Оскільки токенізовані активи стають доступнішими, виникає загроза зростання фінансових маніпуляцій та шахрайських схем. Крім того, існує ризик фрагментації інфраструктури, оскільки наразі різні компанії створюють власні блокчейн-платформи, що можуть не бути сумісними між собою. Щоб вирішити ці проблеми, потрібна глобальна гармонізація регулювання та стандартизація процесів.

На завершення документ наголошує, що токенізація є невідворотним процесом, який значно змінить фінансовий ландшафт. Вона відкриває нові можливості для ефективнішого розподілу капіталу, підвищує ліквідність ринків та зменшує вартість фінансових послуг. Однак її повний потенціал буде реалізований лише у разі розробки чітких регуляторних рамок та інтеграції з традиційними ринковими структурами.

Висновки:

- Облігаційний ринок — головний бенефіціар токенізації
  - **Практичний результат:** Емітенти можуть зменшити витрати на випуск та обслуговування облігацій, забезпечивши миттєве врегулювання угод (T+0) і автоматизацію виплат через смарт-контракти.
  - **Рекомендація:** Фінансовим установам варто інтегрувати блокчейн-рішення для обслуговування боргових інструментів та експериментувати з токенізованими облігаціями.
- Альтернативні фонди отримають новий клас інвесторів
  - **Практичний результат:** Зниження мінімального порогу входу та спрощення процесів KYC/AML через автоматизовані смарт-контракти відкриють доступ до приватного капіталу ширшому колу інвесторів.
  - **Рекомендація:** Фондам варто розглянути випуск токенізованих часток для залучення капіталу від кваліфікованих інвесторів малого та середнього рівня.
- Фрагментація блокчейн-інфраструктури загрожує ліквідності ринку
  - **Практичний результат:** Відсутність взаємодії між різними платформами обмежує можливості вторинного ринку токенізованих активів, що може стримувати їх поширення.
  - **Рекомендація:** Учасникам ринку слід підтримувати розвиток єдиних стандартів для токенізованих активів і співпрацювати над інтеграцією існуючих систем.
- Регуляторна невизначеність може загальмувати впровадження токенізації
  - **Практичний результат:** Без узгоджених міжнародних норм виникає ризик юридичних колізій та неоднозначного трактування цифрових активів.
  - **Рекомендація:** Фінансовим регуляторам необхідно активізувати роботу над адаптацією нормативно-правової бази для токенізованих активів, зокрема у сфері прав власності та ринкової прозорості.

Західноафриканська криза синтетичних наркотиків – причини і наслідки [12]

Звіт, підготовлений Clingendael Institute та Global Initiative Against Transnational Organized Crime (GI-TOC) у лютому 2025 року авторами Лусією Берд Руїс Бенітес де Луго та доктором Карсом де Брюйне, є ґрунтовним дослідженням, присвяченим синтетичному наркотику "куш", який став значною загрозою для Сьєрра-Леоне та ширшого західноафриканського регіону. Дослідження спирається на широкий спектр методів, включаючи хімічне тестування зразків наркотику, понад 120 інтерв'ю з ключовими інформаторами (дилерами, "кухарями", правоохоронцями, людьми, що вживають наркотики), опитування 94 споживачів у Фрітауні, а також етнографічні спостереження, відомі як "deep hanging out", проведені у 2024 році. Воно має на меті заповнити прогалини в знаннях про хімічний склад кушу, еволюцію його ринку, ланцюги постачання, організацію торгівлі, а також політичні та соціальні аспекти, що сприяють його поширенню, надаючи доказову базу для скоординованої відповіді на цю кризу.

Куш вперше з'явився на роздрібних ринках Сьєрра-Леоне близько 2017 року, а до 2020 року став найпоширенішим наркотиком у країні завдяки своїй дешевизні, надзвичайній залежності та дедалі більшій смертоносності. У квітні 2024 року президент Сьєрра-Леоне Джуліус Маада Біо оголосив надзвичайний стан через руйнівний вплив кушу на громадське здоров'я, включаючи значну кількість смертей, що перевантажили морги, призвівши до групових кремацій у 2022 році та залишення тіл на вулицях Фрітауна. З 2021 року куш почав поширюватися за межі Сьєрра-Леоне, охопивши Ліберію, Гвінею, Гамбію, Гвінею-Бісау та Сенегал, що свідчить про його перетворення на регіональну проблему. Автори наголошують, що куш є лише частиною ширшої тенденції проникнення синтетичних наркотиків на західноафриканські ринки, що змінює демографію споживачів, створює нові ринки споживання та ставить серйозні виклики для погано підготовлених систем охорони здоров'я, особливо серед молоді.

Хімічне тестування, проведене у Фрітауні (39 зразків) та Бісау (9 зразків) між травнем і червнем 2024 року з використанням FTIR-спектрометрів та лабораторного аналізу в Іспанії, розкрило склад кушу: він містить нітазени (синтетичні опіоїди, такі як протонітазен, метонітазен і протонітазепін) та синтетичні канабіноїди (зокрема MDMB-4en-PINACA). Нітазени є надзвичайно потужними — наприклад, протонітазепін у 25 разів сильніший за фентаніл, тоді як MDMB-4en-PINACA у 7,5–9 разів перевищує рівень THC у звичайному канабісі. Тестування спростувало поширені міфи про вміст фентанілу, трамадолу, формальдегіду чи людських кісток, показавши високу консистентність складу кушу. Локальний процес синтезу, відомий як "варіння", передбачає використання ацетону та формаліну для розчинення активних інгредієнтів і нанесення їх на листя, часто імпортоване як чай із м'яти, що вказує на зв'язок із глобальними ринками синтетичних наркотиків.

Ринок кушу в Сьєрра-Леоне еволюціонував стрімко: до 2022 року він контролювався кількома організованими групами, які імпортували готовий продукт, але згодом синтез локалізувався, що знизило бар'єри входу, фрагментувало ринок і сприяло його швидкому розширенню. Куш витіснив канабіс і трамадол завдяки доступності та низькій ціні (одна доза коштує 5–10 нових леоне), а його поширення в регіоні різниться за інтенсивністю: у Ліберії та Гвінеї-Бісау зафіксовано зростання смертності, тоді як у Сенегалі та Гамбії проникнення повільніше через

[12] https://globalinitiative.net/wp-content/uploads/2025/02/Lucia-Bird-Ruiz-Benitez-de-Lugo-and-Dr-Kars-de-Bruijne-Kush-in-Sierra-Leone-%E2%80%93-West-Africas-growing-synthetic-drugs-challenge-GI-TOC-and-Clingendael-Institute-February-2025.final_.pdf

менші ринки та соціальні фактори. Активні інгредієнти імпортуються переважно з Китаю через поштові кур'єрські служби, а також морськими шляхами через порт Queen Elizabeth II Quay у Фрітауні та аеропорт. Великобританія та Нідерланди також згадуються як можливі експортери, хоча їхня роль потребує додаткових доказів.

Організація ринку кушу в Сьєрра-Леоне структурована навколо шести ключових ролей: власники, посередники ("locks"), "кухарі", дистриб'ютори, роздрібні продавці та споживачі. Найбільший прибуток отримують власники та "кухарі", тоді як ціна на дозу залишається стабільною, а конкуренція зосереджена на якості продукту. Банди, які раніше вели насильницькі територіальні війни, відіграють важливу роль як дистриб'ютори та продавці, але політична маргіналізація та фокус на якості знизили рівень насильства, оскільки воно вважається "поганим для бізнесу". Торгівля підтримується децентралізованими структурами захисту, включаючи хабарі на пунктах входу та в правоохоронних органах, а також можливі зв'язки з високопоставленими політичними фігурами через сімейні контакти, хоча ці зв'язки не повністю підтверджені.

Вплив кушу на здоров'я є катастрофічним: він спричиняє опіоїдні передозування, психози та соціальну деградацію, особливо серед молоді, а відсутність налоксону та програм зменшення шкоди ускладнює ситуацію. У 2022 році в Фрітауні тіла жертв залишали на вулицях через перевантаження моргів, а в інших країнах регіону також зростає смертність. Документ критикує недостатню доказову базу для відповіді на кризу через брак даних про склад кушу та його ринки до цього дослідження, що дозволяло міфам ускладнювати розробку ефективних заходів.

Висновки:

- **Хімічний склад і загроза:** Куш містить нітазени (потужні опіоїди) та MDMB-4en-PINACA (синтетичний канабіноїд), що вказує на зв'язок із глобальними ринками та початок опіоїдної кризи в Західній Африці.
- **Локальний синтез:** Перехід до місцевого виробництва кушу знизив бар'єри входу, ускладнивши контроль за фрагментованим ринком.
- **Смертельні наслідки:** Висока активність нітазенів спричиняє значну смертність; брак догляду та лікування посилює кризу.
- **Міжнародна роль:** Китай, Великобританія та Нідерланди є ключовими постачальниками інгредієнтів, що вимагає їхньої участі в перериванні ланцюгів постачання.

Автори пропонують три напрями відповіді на кризу. По-перше, побудова доказової бази через посилення регіонального моніторингу, обміну інформацією та технічних спроможностей для виявлення синтетичних речовин. По-друге, переривання ланцюга постачання шляхом посилення контролю за експортом із Китаю, Великобританії та Нідерландів, а також на пунктах входу в Сьєрра-Леоне, разом із оновленням законодавства. По-третє, зменшення шкоди через розширення доступу до лікування, зокрема налоксону та опіоїдно-замісної терапії, а також альтернативи в'язниці для споживачів. Дослідження підкреслює міжнародну відповідальність країн-експортерів та необхідність термінових дій для запобігання подальшій ескалації кризи, яка, ймовірно, є лише початком ширшої проблеми синтетичних наркотиків у Західній Африці.

Рекомендовані матеріали та події

Цифрове рабство: Як жертв перетворюють на шахраїв [13]

Наукова публікація, опублікована 25 лютого 2025 року в журналі Deviant Behavior авторами Suleman Lazarus, Mina Chiang та Mark Button, являє собою детальне дослідження того, як кіберзлочинці використовують оманливі тактики вербування та цифрові платформи для того, щоб заманити жертв у торгівлю людьми. Автори застосовують перспективи міграції та транснаціоналізму, щоб пояснити складний зв'язок між цими двома формами злочинності, спираючись на тематичний аналіз свідчень жертв, отриманих із відкритих джерел, зокрема від Humanity Research Consultancy. Документ підкреслює еволюцію торгівлі людьми в цифрову епоху, коли традиційні форми експлуатації, такі як примусова проституція чи рабство, доповнюються новим явищем — "примусовою злочинністю" (forced criminality), де жертв обманом змушують брати участь у кібершахрайствах під виглядом легальної роботи. Пандемія COVID-19, за словами авторів, посилила цю проблему, спричинивши сплеск таких операцій у Південно-Східній Азії, де сотні тисяч людей, за оцінками OHCHR (2023), утримуються в "шахрайських центрах" у Камбоджі, М'янмі та Лаосі, генеруючи мільярди доларів (зокрема, 43,8 мільярда доларів у країнах Меконгу) для злочинних синдикатів.

Дослідження базується на аналізі одного кейсу — свідчення жертви, випускника комп'ютерних наук і інженерії, що додає унікальний вимір до роботи, оскільки демонструє, як особи з технічними навичками стають мішенню для підвищення ефективності шахрайських схем. У вступі автори зазначають, що торгівля людьми, визнана міжнародним злочином, адаптувалася до цифрових технологій, дозволяючи злочинцям залучати жертв через фальшиві пропозиції роботи, які видаються законними. Ці операції часто розміщуються в спеціальних економічних зонах або перепрофільованих об'єктах, таких як казино та готелі, і управляються синдикатами з міцними зв'язками в кримінальних мережах та політичним захистом. Жертви, які походять із понад 60 країн Азії, Африки, Америки та Європи, зазнають обману, маніпуляцій і примусу до участі в шахрайських операціях, таких як онлайн-казино чи "pig-butchering scams".

Теоретична основа дослідження спирається на теорії міграції та транснаціоналізму, які пояснюють, як глобальні економічні нерівності, обмежувальні міграційні політики та транснаціональні злочинні мережі створюють умови для експлуатації. Ці теорії, розроблені такими вченими, як Faist (транснаціональні соціальні простори), Portes (глобальні зв'язки) і Schiller (багатошарові відносини), детально описані в таблиці, що включає такі елементи, як фактори "push and pull" (економічні труднощі та обіцянки кращого життя), структурні бар'єри (обмежені легальні шляхи міграції) та роль діаспор у підтримці чи експлуатації жертв. Цей підхід дозволяє авторам розглядати торгівлю людьми як транснаціональний феномен, що підсилюється цифровими платформами.

Методологічно стаття використовує підхід одиничного кейс-стаді, аналізуючи свідчення однієї жертви з Камбоджі, опубліковані Humanity Research Consultancy (2024). Тематичний аналіз, проведений за методом Braun і Clarke, виявив шість ключових тем, які детально розкривають досвід жертви: обман і вербування, маніпуляція та контроль, експлуатація та примусова праця, торгівля та переміщення, методи шахрайства, а також втеча та порятунок. Обмеження вибірки одним випадком пояснюється складністю доступу до жертв через їхню вразливість, страх

[13] https://www.tandfonline.com/doi/full/10.1080/01639625.2025.2470402#abstract

помсти від злочинних груп і етичні міркування, що робить великомасштабні дослідження в цій сфері проблематичними. Автори зазначають, що навіть один випадок може дати глибоке розуміння через деталізацію досвіду, що підтверджується порівняннями з іншими дослідженнями.

Результати дослідження розкривають систематичну природу експлуатації. Жертви залучалися через фальшиві обіцянки високооплачуваної роботи, наприклад, посади оператора комп'ютера в онлайн-казино з зарплатою 800–1200 доларів США на місяць, бонусами та квитками додому. Після вербування їхні паспорти конфісковували, а візи оформляли обманним шляхом (наприклад, туристичні замість робочих), часто за підтримки корумпованих імміграційних чиновників, які брали хабарі (наприклад, 500 доларів США). Умови праці були суворими: жертви працювали в шумних офісах із гучною музикою, виконуючи нереальні цілі, такі як залучення трьох клієнтів щодня через WhatsApp чи Telegram, а за невиконання отримували додаткові години роботи чи фізичні покарання. Їх продавали між компаніями та утримували в комплексах із чотирма рівнями безпеки, включаючи озброєних охоронців, що ускладнювало втечу. Жертв навчали створювати фальшиві профілі в соціальних мережах (наприклад, 10 акаунтів Twitter на людину), використовуючи фотографії молодих дівчат для обману клієнтів, а також застосовувати інструменти, такі як Google Voice, для масового розсилання повідомлень. Деяким вдавалося втекти завдяки допомозі НУО, таких як Global Anti-Scam Organization (GASO), яка врятувала жертву свідчень 4 вересня 2022 року після двох місяців спроб.

Унікальність цього дослідження полягає в акценті на примусовій праці в кіберзлочинності, а не лише на романтичних шахрайствах, і в аналізі через призму транснаціоналізму, що підкреслює роль глобальних мереж і структурних вразливостей. Автори зазначають, що жертви часто помилково ідентифікуються як злочинці, що вимагає перегляду юридичних рамок і розробки цільових інтервенцій.

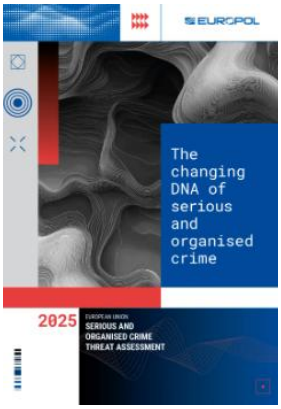
У висновках стаття закликає до подальших досліджень еволюціонуючих тактик кіберзлочинців і торгівців людьми, наголошуючи на необхідності міждисциплінарного підходу, який враховує соціальні, культурні та економічні фактори. Вона підкреслює ключову роль НУО та приватного сектору в боротьбі з експлуатацією, пропонуючи міжнародну співпрацю для розірвання злочинних мереж. Обмеженнями визнано можливі спотворення в свідченнях через травму чи самозахист і залежність від одного випадку, що зменшує узагальнення, але водночас дозволяє

Висновки:

- **Розробка цільових рятувальних операцій:** Необхідно створювати скоординовані програми порятунку жертв примусової кіберзлочинності в Південно-Східній Азії, спираючись на співпрацю з НУО, такими як GASO, які довели свою ефективність (наприклад, порятунок 4 вересня 2022 року).
- **Посилення міграційного законодавства:** Урядам слід переглянути міграційні політики, усуваючи прогалини, які дозволяють обман із візами та корупцію на імміграційних пунктах, щоб зменшити вразливість потенційних жертв до обманних пропозицій роботи.
- **Технологічні та юридичні заходи проти кібершахрайства:** Платформи соціальних мереж (Twitter, Red Book) повинні впроваджувати суворіші механізми виявлення фальшивих акаунтів, а правоохоронні органи — адаптувати юридичні рамки для розрізнення жертв і злочинців у примусовій кіберзлочинності.
- **Підтримка жертв із спеціалізованими навичками:** Потрібні програми реабілітації та реінтеграції, орієнтовані на жертв із технічною освітою (наприклад, випускників комп'ютерних наук), яких дедалі частіше експлуатують для підвищення ефективності шахрайських операцій.

глибше зануритися в індивідуальний досвід. Загалом, дослідження розширює розуміння перетину торгівлі людьми та кіберзлочинності, пропонуючи практичні ідеї для правоохоронних органів, розробки політики та підтримки жертв.

Європол представить новий звіт щодо загроз серйозної та організованої злочинності в ЄС (#SOCTA25)[14]



Європол проведе прес-конференцію, на якій відбудеться презентація унікального, інтелектуально-аналітичного звіту EU Serious and Organised Crime Threat Assessment 2025 (#SOCTA25).

У звіті йтиметься про те, як змінюється природа серйозної та організованої злочинності у світі, що стрімко трансформується. Представники Європолу та керівництво правоохоронних органів ЄС озвучать ключові висновки дослідження та обговорять їхній вплив на безпекову ситуацію в Європі.

Коли: 18 березня 2025 року. Презентація проходитиме у форматі онлайн-прес-конференції.

Спікери заходу:

- Виконавчий директор Європолу Катрін Де Болль
- Єврокомісар із питань внутрішніх справ та міграції Магнус Бруннер
- Заступник державного секретаря Польщі Мацей Душчик
- Голова поліції Польщі Марек Боронь

Під час заходу ви дізнаєтесь про ключові висновки нового звіту Європолу, про те, як правоохоронні органи можуть адаптувати свої підходи для протидії новим кримінальним трендам та які практичні рекомендації пропонуються державам Європи для зміцнення безпеки в регіоні.

Долучитись до перегляду можна онлайн – 18 березня. Щоб отримати доступ до трансляції та одним із перших ознайомитись із ключовими висновками звіту, відвідайте сайт Європолу.

Інші новини

Наслідки кіберінциденту Fintrac: як хакерська атака спричинила кризу у фінансовому моніторингу Канади [15]

Стаття аналізує наслідки масштабного кіберінциденту, що стався в Fintrac (Фінансовий центр аналізу транзакцій та звітності Канади). У березні 2024 року Financial Transactions and Reports Analysis Centre of Canada (Fintrac), канадське агентство з протидії відмиванню коштів (AML) і фінансуванню тероризму (CFT), зазнало масштабного кіберінциденту, який спричинив одну з найсерйозніших криз у сфері фінансового моніторингу країни. Внаслідок атаки, яку агентство офіційно назвало "некласифікованим втручанням", система Fintrac була вимкнена

[14] https://www.europol.europa.eu/media-press/newsroom/news/launch-of-eu-serious-and-organised-crime-threat-assessment-2025
[15] https://thelogic.co/news/the-big-read/fintrac-hack-businesses-fallout/

для забезпечення її безпеки. Однак, попри запевнення регулятора, що дані не були скомпрометовані, наслідки цього інциденту виявилися набагато серйознішими, ніж здавалося на перший погляд.

Після кібератаки Fintrac припинив приймати та обробляти звіти про підозрілі транзакції (Suspicious Transaction Reports, STRs) та великі грошові перекази (Large Cash Transaction Reports, LCTs). Це означало, що тисячі фінансових компаній, зокрема банки, фінтех-компанії, обмінні пункти, рієлторські агентства, ломбарди, дилери дорогоцінних металів і казино, втратили можливість виконувати свої зобов'язання перед регулятором.

Згідно з законодавством Канади, компанії, що обробляють фінансові транзакції, зобов'язані звітувати перед Fintrac, якщо вони ідентифікують операції, які можуть мати ознаки відмивання коштів або фінансування тероризму. Втрата цього механізму контролю фактично означала, що великі обсяги потенційно сумнівних фінансових операцій залишалися непоміченими.

Одна з найсерйозніших проблем виникла у малих та середніх фінансових установ (MSBs – Money Services Businesses), які не мають власних потужних аналітичних систем і повністю залежать від взаємодії з Fintrac. Відключення реєстру MSBs призвело до того, що багато банків відмовилися працювати з цими компаніями, оскільки не могли перевірити їхню відповідність законодавчим вимогам. Деякі компанії взагалі не змогли продовжити свою діяльність, інші – були змушені терміново шукати нових банківських партнерів, що значно ускладнило їхній фінансовий стан.

Після тривалого простою регулятор почав поступово відновлювати роботу своїх систем. Однак він вирішив не просто повернути стару платформу, а запровадити нову систему для подачі звітів. Це створило додаткові труднощі для бізнесу: багато компаній не були підготовлені до змін у процесі подання звітності, новий інтерфейс виявився складним і нестабільним, а помилки при заповненні форм змушували перездавати звіти, що призводило до подальших затримок.

Зокрема, компанії скаржилися на такі проблеми:

- Недостатня комунікація з боку Fintrac – компанії отримували мінімальну інформацію про те, як подавати звіти в перехідний період.
- Технічні несправності системи – деякі компанії були змушені перезаповнювати сотні звітів через неправильне трактування оновлених вимог.
- Адміністративне перевантаження – фінансові установи, що накопичили місяці невідправлених звітів, змушені були витрачати сотні годин на їхнє оформлення та подачу.

Окремо слід зазначити проблему, пов'язану з терміновими звітами щодо фінансування тероризму та сексуальної експлуатації дітей. У період, коли основна система Fintrac не працювала, компанії мали подавати такі звіти через поштову систему Epost, що значно ускладнювало оперативну реакцію правоохоронних органів на потенційно небезпечні транзакції.

Через проблеми у роботі Fintrac деякі компанії почали розглядати можливість виходу з канадського ринку через надмірне регуляторне навантаження та складність взаємодії з державним агентством. Крім того, цей інцидент ще більше загострив питання ефективності системи протидії відмиванню коштів у Канаді.

Інцидент стався у критичний момент, коли канадський уряд, зокрема прем'єр-міністр Джастін Трюдо, обіцяв активізувати боротьбу з відмиванням коштів у співпраці зі США. Це питання набуло ще більшої гостроти після скандалу з TD Bank, який визнав порушення вимог щодо AML у США, а також напередодні майбутньої оцінки Financial Action Task Force (FATF).

Якщо FATF визнає канадську систему фінансового моніторингу недостатньо ефективною, це може мати серйозні наслідки:

- Підвищений рівень ризику для міжнародних транзакцій – іноземні банки можуть запровадити жорсткіші процедури перевірки транзакцій, пов'язаних з Канадою.
- Зниження довіри до канадського фінансового сектору – це може ускладнити залучення інвестицій та сприяти відтоку капіталу.
- Посилення регуляторного тиску на фінансові установи – якщо Канада отримає негативні висновки FATF, уряд буде змушений запроваджувати нові жорсткіші заходи, що створить додаткове навантаження на бізнес.

Наразі компанії, що працюють у фінансовому секторі Канади, опинилися у складному становищі. З одного боку, їм необхідно виконати всі вимоги Fintrac, включно з подачею накопичених звітів до 31 березня 2025 року. З іншого – існує значна невизначеність щодо того, чи зможе регулятор ефективно обробити цей масив інформації та запобігти можливим злочинним схемам, які могли залишитися поза увагою через збій у системі.

Крім того, фінансовий сектор Канади стикається з необхідністю перегляду своєї стратегії кібербезпеки. Інцидент з Fintrac став черговим нагадуванням про ризики, пов'язані з кібератаками, і продемонстрував необхідність створення більш стійких і гнучких механізмів фінансового моніторингу.

Загалом, ситуація з кіберінцидентом у Fintrac показала вразливість фінансового сектора Канади до технологічних загроз, виявила проблеми у регуляторній комунікації та створила нові виклики для бізнесу, який змушений адаптуватися до нових реалій фінансового моніторингу в умовах глобальної нестабільності.

Висновки:

- **Критична залежність фінансового сектору від регулятора -** Безперебійна робота Fintrac є життєво важливою для фінансових установ. Будь-який серйозний збій не лише порушує звітність, але й може створити прогалини в моніторингу фінансових потоків.
- **Недостатня комунікація та підтримка для бізнесу -** Відсутність чітких вказівок під час кризи призвела до значної плутанини, особливо серед малих та середніх фінансових компаній, які не мали доступу до резервних каналів подачі звітів.
- **Необхідність перегляду стратегії кібербезпеки та управління ризиками -** Інцидент продемонстрував потребу у посиленні заходів кіберзахисту в державних установах, а також розробці кризових протоколів для швидкого відновлення їхньої роботи.
- **Ризик втрати довіри до регулятора -** Невизначеність щодо ефективності Fintrac у обробці величезного обсягу відкладених звітів може негативно вплинути на довіру до фінансової системи Канади та поставити країну під загрозу негативних висновків міжнародних організацій, таких як FATF.

Припинення роботи криптовалютної біржі Garantex в ході міжнародної операції[16]

У результаті міжнародної операції, проведеної Міністерством юстиції США спільно з правоохоронними органами Німеччини та Фінляндії, було припинено діяльність криптовалютної біржі Garantex, яка, за даними слідства, сприяла відмиванню коштів транснаціональними злочинними організаціями, включаючи терористичні угруповання, та порушувала санкційні режими.

[16] https://www.justice.gov/opa/pr/garantex-cryptocurrency-exchange-disrupted-international-operation

3 квітня 2019 року Garantex обробила щонайменше $96 мільярдів у криптовалютних транзакціях. Ця платформа була популярною серед російських хакерських угруповань, що займаються програмами-вимагачами, а також серед користувачів даркнет-ринків та інших кіберзлочинців, які потребували відмивання криптовалют, отриманих незаконним шляхом.

У рамках цієї операції були розсекречені обвинувачення проти двох адміністраторів Garantex:

- Алексей Бесцьоков, 46-річний громадянин Литви, який проживає в Росії.
- Александр Міра Серда (раніше відомий як Александр Нтіфо-Ciay), 40-річний громадянин Росії, який проживає в Об'єднаних Арабських Еміратах.

Їм пред'явлені звинувачення у змові з метою відмивання грошей, причому Бесцьокову також інкримінується змова задля порушення санкцій та змова з ведення незареєстрованого бізнесу з грошових переказів.

Варто зазначити, що обидва обвинувачені проживають у країнах, які малоймовірно видадуть їх до США для притягнення до відповідальності.

Ця операція є значним ударом по російській кіберзлочинній екосистемі та демонструє рішучість США у боротьбі з кіберзлочинністю на міжнародному рівні.

Китайський порт Дон'їн став ключовою точкою для обходу санкцій США проти Росії та Ірану[17]

Нещодавно порт Дон'їн (Dongying) у китайській провінції Шаньдун привернув увагу світової спільноти через зростаючу кількість випадків обходу міжнародних санкцій. Танкерні судна, що перебувають під санкціями США за перевезення нафти з Росії та Ірану, активно використовують цей порт для вивантаження нафти та подальшого її перепродажу на міжнародні ринки.

Яскравим прикладом стала ситуація з танкером «Amil», який після довготривалого переховування від систем відстеження доставив до Дон'їна понад 252 тисячі барелів іранської нафти, вивантаживши її на терміналі, що належить приватній компанії, пов'язаній з місцевою державною корпорацією Shandong Wantong Petrochemical Group.

Не менш показовим є випадок із танкером «SI HE», який доставив до того ж порту близько 709 тисяч барелів російської нафти. Цей танкер також перебуває під санкціями США з січня 2025 року, що демонструє систематичне порушення міжнародних санкцій.

Такі випадки підкреслюють серйозні прогалини у глобальному санкційному режимі та вказують на ключову роль китайських портових терміналів у схемах постачання санкційних товарів з Росії та Ірану на світовий ринок.

[17] https://regtechtimes.com/dongying-port-a-hidden-sanctions-bypass-for-oil/

Міжнародні регулятори та правоохоронні органи мають посилити моніторинг та контроль за подібними схемами, оскільки без ефективних заходів реагування санкції втрачають свій вплив, дозволяючи країнам-агресорам уникати економічних наслідків.

Для загального розвитку

Кейс: одна з найбільших справ про відмивання коштів в історії Великобританії – операція Фаулера Олдфілда та її механізми[18]

У цьому тематичному дослідженні розглядається операція Fowler Oldfield (ювелірний магазин) з відмивання коштів, одна з найбільших, коли-небудь виявлених у Великій Британії, яка включає приблизно 266 мільйонів фунтів стерлінгів незаконних коштів. Схему, яка маскувала злочинні доходи під законні доходи від бізнесу, було викрито під час поглибленого розслідування відділом боротьби з економічною злочинністю поліції Західного Йоркшира, що зрештою призвело до засудження ключових осіб.

Механізм відмивання грошей

1. Збирання та транспортування готівки: Великі суми готівки, що походять від організованої злочинності, наприклад торгівлі наркотиками, були зібрані в різних місцях по всій Великобританії, включаючи Глазго, Манчестер і Мерсісайд. Щоб уникнути підозр, гроші транспортували в анонімних контейнерах — спортивних сумках, сумках для покупок або навіть коробках для їжі на винос. Кур'єри використовували спеціальні методи ідентифікації, такі як секретні паролі або мічені банкноти, щоб забезпечити безпечну доставку.

2. Внесення коштів на банківські рахунки: готівка доставлялася в приміщення Fowler Oldfield в Бредфорді, де її перераховували за допомогою професійних машин для обчислення банкнот. Після перевірки та сортування гроші були перераховані на банківські рахунки компанії за допомогою офіційних послуг з інкасації. Цей крок був вирішальним для інтеграції незаконних доходів у фінансову систему, щоб вони виглядали як законні доходи. З роками обсяг готівки зріс експоненціально, досягнувши 1,7 мільйона фунтів стерлінгів на день — надзвичайно висока цифра для ювелірного бізнесу.

3. Конвертація в золото: щоб ще більше приховати грошовий слід, незаконні кошти конвертували в золото, переважно в гранульованому вигляді, яке важче відстежити, ніж зливки. Цей тип золота легко транспортувався, і його можна було переробити, не залишаючи помітних слідів. Значна частина золота була вивезена за межі Великобританії, що ще більше ускладнило відстеження незаконних коштів.

4. Безпечне спілкування та запобіжні заходи: члени організації для спілкування використовували зашифровані платформи для обміну повідомленнями, запобігаючи перехопленню їхніх розмов представниками влади. Крім того, відео з камер спостереження показало, що гроші регулярно перевірялися на наявність пристроїв відстеження перед обробкою, що підкреслює високий рівень обережності, який застосовувався під час операції.

[18] https://www.thetelegraphandargus.co.uk/news/24980520.fowler-oldfield-four-guilty-266m-money-laundering-plot/

Навіть сьогодні золото залишається наріжним каменем схем відмивання грошей через його високу ліквідність, складність відстеження та здатність зберігати цінність за кордоном, що робить його ідеальним активом для приховування та переказу незаконних коштів.

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-2025-11

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].