МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ ВАДИМА ГЕТЬМАНА

Факультет міжнародної економіки і менеджменту

Кафедра міжнародних фінансів

Освітньо-професійна програма «Міжнародні фінансові відносини»

Галузь знань: 29 «Міжнародні відносини»

Спеціальність 292 «Міжнародні економічні відносини»

Форма навчання: очна (денна)

КВАЛІФІКАЦІЙНА БАКАЛАВРСЬКА РОБОТА

на тему:

МІЖНАРОДНІ ФІНАНСОВІ ЗЛОЧИНИ: ВИДИ І ЗАСОБИ ЗАПОБІГАННЯ

здобувача Суховєєва Степана Васильовича

(ПІБ, підпис)

Науковий керівник: кандидат економічних наук, доцент кафедри міжнародних фінансів Зінченко Федір Анатолійович

_____

(підпис)

Робота допущена до захисту перед екзаменаційною комісією з атестації здобувачів вищої освіти (ЕК)

Завідувач кафедри: д.е.н., професор Мозговий О.М.

_____

(підпис)

Київ 2025

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ВАДИМА ГЕТЬМАНА

Факультет міжнародної економіки і менеджменту

Кафедра міжнародних фінансів

Освітньо-професійна програма «Міжнародні фінансові відносини»

Галузь знань: 29 «Міжнародні відносини»
Спеціальність 292 «Міжнародні економічні відносини»

ПОГОДЖЕНО	**ЗАТВЕРДЖУЮ**
Керівник проектної групи (гарант) освітньо-професійної програми	Завідувач кафедри
Т.О. Фролова	О.М. Мозговий
(підпис)	*(підпис)*
_____ 20___ р.	_____ 20___ р.

ІНДИВІДУАЛЬНЕ ЗАВДАННЯ

здобувачу вищої освіти Суховєєву Степану Васильовичу
(прізвище, ім'я, по батькові)

очної (денної) форми навчання

на підготовку кваліфікаційної бакалаврської роботи

на тему «Міжнародні фінансові злочини: види і засоби запобігання»

Тему затверджено наказом ректора Університету від " 18 " 12 2024 р. № 2060-ст

Кваліфікаційна бакалаврська робота виконується на матеріалах наукових статтей, аналітичних звітах міжнародних організацій (FATF, ЄС, МВФ, ООН), законодавчих документах, статистиках та цифрових ресурсах з фінансового моніторингу.

План кваліфікаційної бакалаврської роботи

Розділ 1	**Теоретичні аспекти міжнародних фінансових злочинів**
(назва розділу)	
Розділ 2	**Сучасні засоби запобігання та протидії міжнародним фінансовим злочинам**
(назва розділу)	

Об'єкт дослідження:	Міжнародні фінансові злочини як складове явище глобальної економічної та правової системи
Предмет дослідження:	Механізми здійснення міжнародних фінансових злочинів та інституці й технологічні засоби їх запобігання в умовах трансформації світо фінансових ринків
Мета кваліфікаційної бакалаврської роботи:	Аналіз природи міжнародних фінансових злочинів, їх класифікації, механізмів здійснення, а також дослідження сучасних засобів запобігання та протидії цим злочинам на міжнародному рівні в умовах глобалізації фінансових ринків

Конкретні завдання, які здобувач повинен виконати для досягнення поставленої мети:

У розділі 1	Розкрити поняття, ознаки та класифікацію міжнародних фінансових злочинів
Проаналізувати основні схеми та інструменти здійснення фінансових злочинів у міжнародному середовищі	
Дослідити нормативно-правову базу та міжнародні інституції, що здійснюють боротьбу з фінансовими злочинами	

У розділі 2	Оцінити роль інституційного механізму у виявленні та запобіганні фінансовим злочинам
Проаналізувати інноваційні цифрові інструменти (KYC, AML, блокчейн, big data) у сфері протидії злочинам	
Оцінити перспективи підвищення ефективності запобігання міжнародним фінансовим злочинам у контексті сучасних викликів глобалізованого фінансового середовища	

Завдання підготував науковий керівник _____ _____

(підпис) *(ініціали, прізвище)*

«_____» _____ 20___ р.

Завдання одержав здобувач _____

(підпис) *(ініціали, прізвище)*

«_____» _____ 20___ р.

РЕФЕРАТ

Кваліфікаційна бакалаврська робота містить 60 сторінок, 21 таблиця, 5 рисунків, список використаних джерел з 49 найменування.

Тема роботи: «Міжнародні фінансові злочини: види і засоби запобігання»

Об’єктом дослідження є міжнародні фінансові злочини як складове явище глобальної економічної та правової системи.

Предметом дослідження виступають механізми здійснення міжнародних фінансових злочинів та інституційні й технологічні засоби їх запобігання в умовах трансформації світових фінансових ринків.

Метою кваліфікаційної бакалаврської роботи є аналіз природи міжнародних фінансових злочинів, їх класифікації, механізмів здійснення, а також дослідження сучасних засобів запобігання та протидії цим злочинам на міжнародному рівні в умовах глобалізації фінансових ринків.

Для досягнення мети були поставлені такі завдання:

- Розкрити поняття, ознаки та класифікацію міжнародних фінансових злочинів.
- Проаналізувати основні схеми та інструменти здійснення фінансових злочинів у міжнародному середовищі.
- Дослідити нормативно-правову базу та міжнародні інституції, що здійснюють боротьбу з фінансовими злочинами.
- Оцінити роль інституційного механізму у виявленні та запобіганні фінансовим злочинам.
- Проаналізувати інноваційні цифрові інструменти (KYC, AML, blockchain, big data) у сфері протидії злочинам.
- Оцінити перспективи підвищення ефективності запобігання міжнародним фінансовим злочинам у контексті сучасних викликів глобалізованого фінансового середовища.

Актуальність теми зумовлена поширенням фінансових злочинів, що ставлять під загрозу економічну безпеку держав, стабільність ринків та довіру до

фінансових інституцій. Геополітичні конфлікти, зокрема війна в Україні, посилення санкційного тиску, зростання обсягів криптовалютних транзакцій — усе це актуалізує потребу в дослідженні нових механізмів протидії.

Методи дослідження: аналіз наукової літератури, контент-аналіз міжнародних нормативно-правових актів, порівняльний аналіз політик у різних країнах, вивчення статистичних даних та кейсів.

Теоретична значущість роботи полягає в поглибленні розуміння класифікації, регулювання та впливу міжнародних фінансових злочинів на глобальну фінансову безпеку.

Методична значущість – у розробці підходів до аналізу злочинних схем і засобів їх виявлення.

Практична значущість полягає у можливості використання результатів для вдосконалення фінансового моніторингу, антикорупційних стратегій та міждержавної співпраці.

Інформаційною базою дослідження є наукові статті, аналітичні звіти міжнародних організацій (FATF, ЄС, МВФ, ООН), законодавчі документи, статистика та цифрові ресурси з фінансового моніторингу.

Структура роботи: вступ, два розділи (теоретичний та практично-аналітичний), висновки, список використаних джерел, додатки.

В і д г у к

про кваліфікаційну бакалаврську роботу
здобувача освітньо-професійної програми «Міжнародні фінансові відносини»
факультету Міжнародної економіки і менеджменту

Суховєєва С.В.

(прізвище, ініціали)

на тему «Міжнародні фінансові злочини: види і засоби запобігання»

(назва теми)

1. Актуальність теми: у сучасному світі фінансові злочини набувають все складніших форм і масштабів. Відмивання коштів, ухилення від сплати податків, офшорні схеми, використання криптовалют — ці явища суттєво загрожують економічній стабільності та безпеці країн. Особливо важливим є вивчення цієї проблеми на тлі сучасних геополітичних викликів, зокрема санкційної політики та війни в Україні.

2. Позитивні риси кваліфікаційної бакалаврської роботи: робота вирізняється глибоким аналізом, великою кількістю прикладів, актуальною статистикою та системним викладом матеріалу. Автор вдало структурував дослідження: від теоретичних аспектів і класифікації злочинів до аналізу механізмів та міжнародної правової бази.

3. Наявність самостійних розробок автора: у роботі помітна аналітична позиція автора — зокрема, при класифікації злочинів, порівнянні міжнародних практик та оцінці ролі цифрових технологій у злочинних схемах.

4. Цінність теоретичних висновків та практичних рекомендацій: Висновки роботи мають практичну користь, особливо для фахівців у сфері фінансового моніторингу, боротьби з корупцією та банківської справи.

5. Наявність недоліків: до недоліків роботи можна віднести її певну перевантаженість — у деяких місцях занадто багато таблиць, статистики та прикладів, що ускладнює сприйняття. Частині матеріалу бракує узагальнення або коротших підсумків, які допомогли б краще структурувати інформацію. Також можна було б трохи ширше висвітлити роль України у міжнародних ініціативах боротьби з фінансовими злочинами.

6. Загальна оцінка кваліфікаційної бакалаврської роботи та її допущення до захисту перед ЕК: кваліфікаційна бакалаврська робота Суховєєва С.В. виконана якісно, відповідає вимогам до бакалаврських кваліфікаційних робіт даної галузі знань та рекомендується до захисту перед ЕК.

Науковий керівник: доцент кафедри міжнародних фінансів, к.е.н.

(посада, учене звання, науковий ступінь)

_____ **Зінченко Ф.А.**

(підпис) **(прізвище, ініціали)**

“____”_____ 20___ р.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

AML	(Anti-Money Laundering) Протидія відмиванню грошей
AMLD	(Anti-Money Laundering Directive) Директива щодо протидії відмиванню грошей
BEPS	(Base Erosion and Profit Shifting) Розмивання податкової бази та виведення прибутку з-під оподаткування
CFT	(Combating the Financing of Terrorism) Боротьба з фінансуванням тероризму
COSMIC	(Coordinated Oversight of Securities and Markets in the Community) Координований нагляд за цінними паперами та ринками в Співтоваристві (це застаріла абревіатура, яка стосувалася проєкту ЄС)
CRS	(Common Reporting Standard) Загальний стандарт звітності
DAI	(Dai) Дай (стабільна криптовалюта)
DFSA	(Dubai Financial Services Authority) Управління фінансових послуг Дубая
ESMA	(European Securities and Markets Authority) Європейське управління з цінних паперів та ринків
FATF	(Financial Action Task Force) Група розробки фінансових заходів боротьби з відмиванням грошей
FINMA	(Swiss Financial Market Supervisory Authority) Швейцарська служба з нагляду за фінансовими ринками
FIU	(Financial Intelligence Unit) Підрозділ фінансової розвідки
ICIJ	(International Consortium of Investigative Journalists) Міжнародний консорціум журналістів-розслідувачів
IMF	(International Monetary Fund) Міжнародний валютний фонд
IOSCO	(International Organization of Securities Commissions) Міжнародна організація комісій з цінних паперів
IRS	(Internal Revenue Service) Податкова служба США
KYC	(Know Your Customer) Знай свого клієнта
MLA	(Mutual Legal Assistance) Взаємна правова допомога
MROS	(Money Laundering Reporting Office Switzerland) Швейцарське управління з питань звітності про відмивання грошей
OCCRP	(Organized Crime and Corruption Reporting Project) Проєкт з розслідування організованої злочинності та корупції
OECD	(Organisation for Economic Co-operation and Development) Організація економічного співробітництва та розвитку

SEPA	(Single Euro Payments Area) Єдина зона платежів у євро
SWIFT	(Society for Worldwide Interbank Financial Telecommunication) Товариство всесвітніх міжбанківських фінансових телекомунікацій
TJN	(Tax Justice Network) Мережа податкової справедливості
UBO	(Ultimate Beneficial Owner) Кінцевий бенефіціарний власник
UNCAC	(United Nations Convention Against Corruption) Конвенція Організації Об'єднаних Націй проти корупції
UNODC	(United Nations Office on Drugs and Crime) Управління Організації Об'єднаних Націй з наркотиків і злочинності
UNSCR	(United Nations Security Council Resolution) Резолюція Ради Безпеки Організації Об'єднаних Націй
USDT	(Tether) Тезер (стабільна криптовалюта)

ВСТУП

Актуальність теми. У сучасному глобалізованому світі фінансові потоки дедалі частіше перетинають державні кордони, що створює не лише можливості для економічного зростання, але й відкриває нові шляхи для злочинних схем. Відмивання коштів, фінансування тероризму, ухилення від оподаткування через офшорні юрисдикції — ці злочини стали невід'ємною частиною світової фінансової екосистеми. Вони загрожують фінансовій стабільності, підривають довіру до банківських інституцій, спотворюють конкуренцію й ускладнюють боротьбу з корупцією. Особливої актуальності тема набуває на тлі сучасних геополітичних викликів, зокрема війни в Україні, посилення санкційної політики та активізації боротьби з фінансуванням агресії через тіньові схеми. Водночас стрімкий розвиток цифрових технологій, зокрема криптовалют, створює як нові інструменти для боротьби з фінансовими злочинами, так і нові ризики.

У зв'язку з цим виникає потреба у глибшому розумінні механізмів міжнародних фінансових злочинів та розробці ефективних засобів їх запобігання. Саме тому дослідження цієї проблематики є надзвичайно актуальним як з наукового, так і з практичного погляду — воно сприяє формуванню більш безпечного й прозорого глобального фінансового середовища.

Аналіз останніх досліджень та публікацій. Постійна актуалізація теми міжнародних фінансових злочинів у контексті глобалізації, фінансової безпеки та транскордонної співпраці підкреслює важливість відповідних наукових досліджень. Ці роботи виконані як вітчизняними, так і зарубіжними науковцями та практиками, серед яких можна назвати В. Д. Базилевича, І. Б. Сохацьку, Л. Лісовську, О. В. Рогач, А. М. Кендзу, М. О. Савлука, А. Ґамбра, М. Пікара, Е. Д'Альє, Л. Грантта, Т. Гілмора, Ф. Муллера, К. Саллівана, М. Буша, Д. Рікардсона, Дж. Зетца, А. Бойла, Е. Хаузера та П. Сандера.

Значна кількість досліджень присвячена аналізу механізмів відмивання коштів, фінансування тероризму, податкових зловживань через офшорні структури, а також розробці політик протидії цим загрозам на рівні міжнародних

інституцій. Слід зауважити, що іноземні дослідження значною мірою зосереджені на міждержавній координації, законодавчих ініціативах та цифрових інноваціях у сфері фінансового контролю. Водночас вітчизняна наука робить акцент на правовому регулюванні та викликах для національної економічної безпеки в умовах міжнародного тиску. Попри значний обсяг наукових праць, усе ще існує потреба у комплексному аналізі ефективності засобів запобігання фінансовим злочинам в умовах сучасної трансформації фінансових ринків.

Метою роботи є аналіз природи міжнародних фінансових злочинів, їх класифікації, механізмів здійснення, а також дослідження сучасних засобів запобігання та протидії цим злочинам на міжнародному рівні в умовах глобалізації фінансових ринків. Для досягнення поставленої мети необхідно виконати такі **завдання**:

- Розкрити поняття, ознаки та класифікацію міжнародних фінансових злочинів.
- Проаналізувати основні схеми та інструменти здійснення фінансових злочинів у міжнародному середовищі.
- Дослідити нормативно-правову базу та міжнародні інституції, що здійснюють боротьбу з фінансовими злочинами.
- Оцінити роль інституційного механізму у виявленні та запобіганні фінансовим злочинам.
- Проаналізувати інноваційні цифрові інструменти (KYC, AML, блокчейн, big data) у сфері протидії злочинам.
- Оцінити перспективи підвищення ефективності запобігання міжнародним фінансовим злочинам у контексті сучасних викликів глобалізованого фінансового середовища.

Об’єкт дослідження - міжнародні фінансові злочини як складове явище глобальної економічної та правової системи.

Предмет дослідження - механізми здійснення міжнародних фінансових злочинів та інституційні й технологічні засоби їх запобігання в умовах трансформації світових фінансових ринків.

Методи дослідження включають аналіз наукової літератури з теми міжнародних фінансових злочинів, контент-аналіз міжнародних нормативно-правових актів, порівняльний аналіз механізмів запобігання фінансовим злочинам у різних країнах, а також вивчення статистичних даних щодо масштабів і тенденцій фінансової злочинності.

Теоретична значущість отриманих результатів полягає у поглибленні наукового розуміння природи, класифікації та міжнародного регулювання фінансових злочинів, а також їх впливу на глобальну фінансову безпеку.

Методична значущість полягає в обґрунтуванні підходів до аналізу схем фінансових правопорушень та оцінки ефективності інституційних та цифрових засобів протидії їм.

Практична значущість полягає у можливості використання результатів дослідження для підвищення ефективності механізмів фінансового контролю, посилення антикорупційних стратегій та вдосконалення міждержавного співробітництва у сфері боротьби з фінансовими злочинами.

Інформаційною базою дослідження є наукові статті, аналітичні звіти міжнародних організацій (FATF, ЄС, МВФ, ООН), законодавчі документи, відкриті статистичні дані, а також ресурси, що висвітлюють сучасні цифрові інструменти у сфері фінансового моніторингу.

Структура роботи. Робота складається зі вступу, двох розділів (теоретичного й аналітико-практичного), загальних висновків, списку використаних джерел та додатків.

РОЗДІЛ 1.
ТЕОРЕТИЧНІ АСПЕКТИ МІЖНАРОДНИХ ФІНАНСОВИХ ЗЛОЧИНІВ

1.1 Поняття та класифікація міжнародних фінансових злочинів

Поняття «фінансовий злочин» має багатовимірний характер і варіюється залежно від контексту — правового, економічного або міждисциплінарного. У науковій літературі та практиці міжнародних організацій не існує єдиного універсального визначення, що зумовлено складністю явища, його мінливістю та широким спектром форм прояву (рис.1.1).

Правовий підхід

передбачає розуміння фінансового злочину як діяння, що прямо порушує фінансове законодавство або положення, що регулюють обіг грошових коштів, кредитування, оподаткування, банківську діяльність тощо. У рамках кримінального права фінансові злочини вважаються окремою категорією злочинів у сфері економіки.

Економічний підхід

визначає фінансові злочини як умисні дії, спрямовані на отримання неправомірної вигоди шляхом використання фінансової системи з порушенням ринкових правил, що призводить до перерозподілу або втрати вартості в економіці. Тут акцент зроблено на наслідки для економічної системи, а не лише на порушення норм.

Інституційний підхід

представлений у документах міжнародних організацій (наприклад, FATF, МВФ, ООН), розглядає фінансові злочини як загрозу міжнародній безпеці, інтеграції ринків і довірі до глобальних фінансових інститутів. У фокусі — відмивання коштів, фінансування тероризму, транснаціональні схеми ухилення від оподаткування.

Рисунок.1.1 Основні підходи до дефініції

Джерело: [1]

Варто чітко розділяти поняття економічного та фінансового злочину (рис.1.2).

Економічні злочини	Фінансові злочини
охоплюють ширше коло правопорушень, пов'язаних з виробництвом, розподілом, обігом товарів і послуг (контрабанда, порушення антимонопольного законодавства, шахрайство у сфері торгівлі тощо).	зосереджені безпосередньо на сфері фінансових відносин: гроші, інвестиції, банки, страхування, оподаткування, фондовий ринок.

Рисунок 1.2. – Розмежування фінансових та економічних злочинів

Джерело: [1]

Ключовою відмінністю є сфера діяльності та інструменти порушення: у фінансових злочинах зазвичай фігурують операції з грошовими активами, тоді як економічні можуть включати матеріальні ресурси, інфраструктуру, логістику тощо (табл.1.1).

Таблиця 1.1 – Порівняння підходів до визначення фінансових злочинів

Джерело / Інституція	Формулювання / Ключові ознаки	Підхід	Приклад/ Орієнтація
FATF (Financial Action Task Force)	Фінансові злочини охоплюють відмивання коштів, фінансування тероризму, ухилення від податків, шахрайство, корупцію. Розглядаються як загроза фінансовій стабільності.	Інституційний, міжнародно-правовий	Міждержавна співпраця, стандарти AML/CFT
Конвенція ООН проти корупції (2003)	Надає правову класифікацію злочинів фінансового характеру: корупція, незаконне збагачення, розтрата, зловживання владою.	Правовий	Превенція та криміналізація
Конвенція ООН проти транснаціональної організованої злочинності (2000)	Фінансові злочини розглядаються в контексті транснаціонального організованого злочинного угруповання.	Правовий, міжнародний	Координація правозастосування
Європейська Комісія	Зосереджується на фінансових злочинах, що завдають шкоди бюджету ЄС: шахрайство, підробка, зловживання грантами, ПДВ-шахрайство.	Інституційний	Захист фінансових інтересів ЄС
МВФ (IMF)	Визначає фінансові злочини як дії, що дестабілізують фінансові ринки та підривають довіру до інституцій.	Економіко-інституційний	Контроль капіталу, ризики систем
Світовий банк (World Bank)	Розглядає фінансові злочини через призму впливу на інвестклімат: корупція, відмивання коштів, шахрайство в держзакупівлях.	Економічний	Реформи управління, аудит
Transparency International	Не дає формального визначення, але акцентує на системній фінансовій корупції як базовому елементі фінансових злочинів.	Громадський, аналітичний	Антикорупційні ініціативи
Науковці (Сохацька, Лісовська, Базилевич)	Визначають фінансові злочини як умисні дії з використанням фінансових інструментів для отримання незаконного прибутку, що викривлює ринки.	Економічний	Академічна економічна теорія
КК України (ст. 209–212)	Закріплює перелік злочинів: відмивання доходів, ухилення від сплати податків, зловживання в банківській сфері, фальсифікація документів.	Національно-правовий	Правозастосування на рівні держави

FSB США (Financial Crimes Enforcement Network)	Фінансові злочини — це будь-які дії, що порушують законодавство у сфері фінансового регулювання: шахрайство, зловживання криптовалютами, нелегальні перекази.	Адміністративно-контрольний	Виявлення підозрілих транзакцій

Джерело: [1-2]

Як свідчить порівняльний аналіз, у міжнародній практиці не існує єдиного, усталеного визначення фінансових злочинів. Різні інституції та наукові школи трактують це поняття відповідно до власних цілей: правове регулювання, економічний контроль, захист інституційної стабільності чи громадський моніторинг. Загальним для всіх підходів є визнання фінансових злочинів як серйозної загрози економічній безпеці, фінансовій прозорості та довірі до ринкових інститутів [2]. Водночас ця багатозначність у трактуваннях ускладнює уніфікацію стандартів боротьби з такими правопорушеннями, що зумовлює потребу в подальшому теоретичному осмисленні та гармонізації правових рамок.

Транснаціональний характер

Однією з визначальних рис фінансових злочинів є їх транснаціональність. У багатьох випадках вони виходять за межі однієї юрисдикції, що ускладнює їхнє розслідування та притягнення винних до відповідальності. Наприклад, відмивання коштів може включати декілька етапів переміщення коштів через рахунки в різних країнах — від офшорних зон до цифрових платіжних платформ. Саме ця глобальна логістика обумовлює потребу в міжнародному співробітництві, уніфікації стандартів AML/CFT (боротьби з відмиванням коштів і фінансуванням тероризму) та гармонізації кримінального процесуального законодавства.

Використання фінансової інфраструктури

Фінансові злочини здійснюються в межах або через елементи офіційної фінансової системи. У той час як більшість кримінальних правопорушень пов'язані з насильством, фізичним впливом або матеріальним посяганням, фінансові злочини використовують інструменти законного обігу: банківські рахунки, цінні папери, електронні платіжні системи, криптовалюти, податкові механізми. Це робить їх не лише важкими для виявлення, але й підступними у плані зловживання довірою до фінансових інституцій. Наприклад, фіктивні компанії чи підроблені інвестиційні фонди діють зовні легально, маскуючи злочинну суть.

Високий рівень латентності

Фінансові злочини відзначаються високим ступенем латентності, тобто прихованості від правоохоронних органів. Причинами цього є складність схем, тривала підготовка до їх здійснення, професіоналізм виконавців, а також залучення посередників та використання правових лазівок. Багато таких злочинів залишаються невикритими протягом років, або взагалі не виявляються без глибокого аудиту чи міжнародних розслідувань (наприклад, Panama Papers або Pandora Papers). Відповідно, статистичні дані про фінансову злочинність часто не відображають реального масштабу проблеми.

Рисунок 1.3. – Ознаки, що відрізняють фінансові злочини від інших видів правопорушень

Джерело: [3]

Саме тому вивчення змісту та класифікації міжнародних фінансових злочинів залишається важливим як у науковому, так і в прикладному вимірі. Фінансові злочини становлять особливу категорію правопорушень, які відрізняються від класичних кримінальних діянь не лише за своєю економічною природою, але й за характером виконання, масштабами впливу та складністю виявлення. Їх специфіка зумовлена рядом ознак, що чітко виокремлюють ці злочини в межах загальної структури злочинності (рис.1.3).

Фінансові злочини є прикладом «невидимого» правопорушення — там, де інші види злочинів викликають негайну соціальну реакцію, фінансові злочини можуть роками залишатися поза увагою, при цьому завдаючи колосальної шкоди як державному бюджету, так і фінансовій стабільності в цілому. Саме ці ознаки вимагають створення спеціалізованих механізмів контролю, розслідування та міждержавної координації у боротьбі з таким видом правопорушень.

Класифікація міжнародних фінансових злочинів дозволяє систематизувати їх за видами, механізмами вчинення, об'єктами посягання та правовими наслідками. Такий підхід необхідний для розробки ефективних механізмів їх попередження, криміналізації та міждержавної координації розслідувань (табл.1.2).

Таблиця 1.2 – Класифікація міжнародних фінансових злочинів

Вид злочину	**Суть правопорушення**	**Типові механізми**	**Основні ризики**	**Міжнародні органи/документи**
Відмивання коштів	Легалізація доходів, отриманих злочинним шляхом	Транзит через офшори, фіктивні компанії, нерухомість, криптовалюти	Підрив фінансової системи, втрати бюджету	FATF, UNODC, AMLD (ЄС), Конвенція ООН проти злочинності (2000)
Фінансування тероризму	Фінансова підтримка терористичних дій та організацій	Фіктивні благодійні фонди, мікротранзакції, Hawala-системи	Загроза національній безпеці, міжнародна дестабілізація	FATF, ООН, Директиви ЄС, UNSCR 1373
Ухилення від сплати податків	Намір уникнути податкових зобов’язань	Заниження доходів, офшори, трансфертне ціноутворення	Втрати державного бюджету, недовіра до системи	OECD BEPS, Європейська комісія, G20, Глобальний форум з прозорості
Корупційні схеми	Незаконне збагачення через	«Відкати», підставні	Ерозія державного управління,	UNCAC (2003), Transparency

	зловживання владою	тендери, офшорні перекази	втрати інвестклімату	International, World Bank
Махінації з цінними паперами	Штучне впливання на фінансові ринки задля особистої вигоди	Інсайдерська інформація, "pump & dump", дезінформація	Втрата довіри до ринків, збитки інвесторам	IOSCO, SEC (США), ESMA (ЄС)
Незаконне використання криптовалют	Застосування цифрових активів у злочинних цілях	Анонімні перекази, крипто-гаманці на dark web, нелегальні ICO	Нові виклики для регулювання, фінансування злочинності	FATF Travel Rule, MiCA (ЄС), FinCEN (США), Chainalysis (аналітика)

Джерело: [3]

Ці категорії не є вичерпними, однак охоплюють основні типи злочинів, які найчастіше фігурують у практиці міжнародних розслідувань, фінансової розвідки та законодавства. Їхня класифікація допомагає точніше формувати стратегії запобігання, виявлення та реагування.

Міжнародне правове поле, що регламентує боротьбу з фінансовими злочинами, формується на перетині загальновизнаних конвенцій, рекомендацій міжурядових організацій та наднаціонального законодавства, зокрема Європейського Союзу [4]. На відміну від класичних кримінальних діянь, фінансові злочини часто мають транснаціональний характер і вимагають спільного нормативного реагування.

Одним із ключових міжнародних документів у цій сфері є Конвенція ООН проти транснаціональної організованої злочинності (Палермо, 2000), що окреслює механізми запобігання злочинам, які вчиняються в більш ніж одній державі [4]. Доповненням до неї стала Конвенція ООН проти корупції (UNCAC, 2003), яка надає визначення корупційним злочинам та передбачає обов’язкову криміналізацію фінансової корупції, зловживання владою, відмивання коштів та незаконного збагачення.

У свою чергу, FATF (Група розробки фінансових заходів боротьби з відмиванням коштів) формує гнучку систему рекомендацій (40 основних), які визнаються "золотим стандартом" у сфері протидії фінансовим злочинам. Їх особливість — у практичному характері: вони не є юридично обов’язковими, але

їх невиконання впливає на міжнародну репутацію та доступ до фінансових ринківv[5].

Європейський Союз розробив серію директив з боротьби з відмиванням коштів (AMLD — Anti-Money Laundering Directives), які мають обов'язковий характер для країн-членів. Зокрема, 6-та директива AMLD (2021) вперше прямо визначає перелік фінансових злочинів і встановлює спільні мінімальні санкції.

Однак попри існування глобальних підходів, національні правові системи по-різному трактують фінансові злочини залежно від історичних, інституційних і економічних умов. Це створює проблеми гармонізації, але водночас дає підстави для порівняльного аналізу (табл.1.3).

Таблиця 1.3 – Порівняння правового підходу до фінансових злочинів у різних країнах

Країна / Юрисдикція	Окреме визначення фінансового злочину	Ключові законодавчі акти	Фокус правозастосування	Особливості / Примітки
США	✅ (в рамках фінансового права)	Bank Secrecy Act, USA PATRIOT Act	AML, SEC fraud, фінансування тероризму	Активне використання FinCEN, санкції за недотримання KYC
Німеччина	✅ (в межах податкового та банківського кодексів)	Strafgesetzbuch (StGB), GwG	Податкова злочинність, корпоративна відповідальність	Криміналізація ухилення від податків із 2021 р.
Франція	✅	Code pénal, Code monétaire et financier	Корупція, біржові маніпуляції, AML	Активна участь у регулюванні криптовалют
Україна	✅ (чітко визначено в Кримінальному кодексі)	ККУ (ст. 209–212), Закон про фінансовий моніторинг	Відмивання коштів, ухилення від податків, зловживання у банках	Система фінансового моніторингу через Держфінмон
Швейцарія	✅	Swiss Criminal Code, Anti-Money Laundering Act	Захист банківської таємниці, AML	Високий рівень міжнародної співпраці, прецедентна система
ОАЕ (Дубай)	✅ (особливо у вільних економічних зонах)	Federal Law No. 20 (2018), DIFC Regulatory Law	AML, злочини в банківському секторі	Акцент на репутаційній прозорості, великі штрафи

Китай	🔶 (часткове визначення через економічні злочини)	Criminal Law of PRC, Measures on AML	Фінансова корупція, тіньові банківські операції	Високий рівень державного контролю
ЄС (наднац. рівень)	✅ (уніфіковане через директиви)	4th–6th AML Directives, Regulation (EU) 2015/847	Загальноєвропейський підхід до AML та CFT	Країни зобов'язані гармонізувати внутрішнє законодавство

Джерело: [5]

Як видно з таблиці, попри зусилля міжнародних організацій з гармонізації підходів до боротьби з фінансовими злочинами, нормативно-правові трактування залишаються різними в залежності від національних правових систем. Одні країни акцентують увагу на податкових зловживаннях, інші – на корупції або цифрових фінансових інструментах. Водночас на наднаціональному рівні (зокрема в межах ЄС) активно впроваджуються директиви, спрямовані на уніфікацію базових стандартів у сфері запобігання фінансовим правопорушенням. Така неоднорідність підходів створює як виклики (асиметрія регулювання, складність міжнародного переслідування), так і можливості для зміцнення міжнародної співпраці, правової інтеграції та обміну інформацією між юрисдикціями.

1.2 Механізми здійснення фінансових злочинів у міжнародному середовищі

Офшорні юрисдикції та фіктивні (так звані shell) компанії відіграють ключову роль у глобальній архітектурі фінансових злочинів. Упродовж останніх десятиліть офшорна інфраструктура перетворилася на своєрідну «тіньову паралельну систему», яка дозволяє злочинцям, корумпованим посадовцям, а іноді й транснаціональним корпораціям, приховувати справжнє походження капіталу, уникати податкових зобов'язань та ускладнювати фінансове розслідування [6].

Офшорна юрисдикція — це країна або територія з пільговим податковим режимом і слабкими вимогами до фінансової прозорості. В таких країнах не вимагається публічного розкриття інформації про кінцевих бенефіціарних власників (UBO — Ultimate Beneficial Owner), що дозволяє зловмисникам

створювати багаторівневі корпоративні структури для маскування реального контролю над активами. Згідно з даними Tax Justice Network (2023), через офшорні схеми у світі щороку втрачається понад $480 млрд податкових надходжень, з яких приблизно $312 млрд припадає на транснаціональні компанії, а ще $170 млрд — на приватних осіб, що приховують активи (табл.1.4).

Таблиця 1.4 – Роль офшорів у приховуванні бенефіціарів: статистика, країни та вплив

Показник / Параметр	**Значення / Дані**	**Джерело / Коментар**
Щорічні втрати держав від офшорного приховування активів	$480 млрд	Tax Justice Network (2023)
Частка втрат, спричинених юридичними особами (компаніями)	65% (~$312 млрд)	OECD, TJN
Частка втрат, спричинених приватними особами (олігархи, тощо)	35% (~$168 млрд)	TJN
Кількість shell-компаній, викритих у Panama Papers	214 000+	ICIJ (2016)
Середня кількість офшорних структур на одного бенефіціара	3–7	За даними розслідувань OCCRP, ICIJ
Найпопулярніші юрисдикції для приховування бенефіціарів	Британські Віргінські о-ви, Панама, Беліз, Джерсі, Каймани	ICIJ, Global Witness
Країни, які найбільше втрачають доходів через офшори	США, Франція, Німеччина, Індія, Бразилія	TJN, IMF
Наявність відкритого реєстру бенефіціарів (Україна)	✅ (з 2021 року, частково працює)	Закон України «Про запобігання відмиванню коштів»
Оцінка прихованих активів російських бенефіціарів за кордоном	$800+ млрд	Atlantic Council (2022), Chatham House
Період створення більшості офшорних компаній у схемах (ICIJ)	1990–2015	Довгострокове накопичення через юридичні дірки в законодавстві

Джерело: [6]

Офшори — це не лише “низькі податки”, а насамперед — інструмент анонімності, який масово використовується для приховування власності, відмивання коштів і фінансування тіньових операцій. Така анонімність блокує слідство, фінансовий контроль і міжнародне правосуддя.

Ще одним інструментом для фінансових махінацій є трастові структури, які формально відділяють власника активу від особи, що ним керує, — тим самим

ускладнюючи відстеження кінцевого вигодонабувача. Такі структури часто створюються в юрисдикціях на кшталт Британських Віргінських островів, Белізу, Панами чи Джерсі [7]. Shell-компанії — це юридичні особи без реальної операційної діяльності, офісу чи персоналу, що використовуються виключно для переміщення коштів. Згідно з розслідуванням Panama Papers (2016), понад 214 тис. фіктивних компаній у більш ніж 21 юрисдикції були задіяні в схемах відмивання коштів, фінансування корупції та ухилення від податків.

Таблиця 1.5 – Трастові структури та shell-компанії: роль у фінансових злочинах

Параметр / Категорія	**Трастові структури**	**Shell-компанії (фіктивні компанії)**
Визначення	Юридична угода, за якою активи передаються керуючому (trustee) на користь третьої сторони (beneficiary)	Компанія, що не веде реальної господарської діяльності, але зареєстрована для здійснення фінансових операцій
Основне призначення	Управління активами, спадкове планування, податкове структурування	Анонімне володіння активами, приховування бенефіціарів, відмивання коштів
Переваги для злочинців	Відокремлення юридичного власника від вигодонабувача; важко довести зв'язок із активами	Відсутність прозорості, спрощена реєстрація, низькі вимоги до звітності
Типові юрисдикції	Джерсі, Ліхтенштейн, Сінгапур, Острів Мен, Британські Віргінські острови	Панама, Беліз, Сейшели, Кайманові острови, Вануату
Середня кількість shell-компаній на одного бенефіціара	—	3–7 компаній (ICIJ, 2021)
Кількість трастів, виявлених у Pandora Papers	957 трастів у 15 офшорних юрисдикціях	29 000+ shell-компаній (ICIJ, 2021)
Найвідоміші викриття	Трасти корумпованих еліт Латинської Америки, Африки, Росії	Panama Papers, Pandora Papers, FinCEN Files
Вартість активів, які часто передаються в трасти	$1 млн – $100+ млн (бізнеси, нерухомість, твори мистецтва)	До $10 млрд у формі рухомого капіталу (готівка, перекази, криптовалюта)
Регуляторні ризики	Відсутність централізованих реєстрів бенефіціарів, складність міжнародного аудиту	Мінімальний контроль, масове використання у схемах відмивання коштів
Співвідношення у великих схемах ухилення	Трасти — 20–30% складових схем (у поєднанні з фондами, нерухомістю)	Shell-компанії — понад 60% основних елементів фінансових злочинів

Джерело: [7]

Трастові структури й shell-компанії — це не лише легальні інструменти управління активами, але й ядро багатьох тіньових фінансових операцій, де межа між оптимізацією й злочином надзвичайно тонка.

BEPS (Base Erosion and Profit Shifting) — це схема штучного «переміщення прибутків» до країн з низьким або нульовим оподаткуванням. Компанії використовують трансфертне ціноутворення, внутрішньокорпоративні роялті, позики та «інтелектуальні платежі» для зменшення оподатковуваної бази в країнах, де фактично ведеться діяльність. OECD оцінює щорічні втрати від BEPS для державної фіскальної системи на рівні $100–240 млрд, що становить приблизно 4–10% світових корпоративних податкових надходжень. З цієї причини було розроблено Проєкт BEPS (2013–2015), а з 2021 року активно впроваджується Глобальна мінімальна ставка податку (15%), щоб зменшити привабливість таких схем [8].

Таблиця 1.6 – Типові схеми BEPS: механізми, масштаби та географія

Назва схеми BEPS	**Суть механізму**	**Оцінка щорічних втрат (USD)**	**Країни, що втрачають найбільше**	**Юрисдикції-«реципієнти» прибутку**
Double Irish with a Dutch Sandwich	Прибуток переводиться через Ірландію, потім через Нідерланди до офшорів (наприклад, Бермудів)	$20–30 млрд	США, Німеччина, Франція	Ірландія, Нідерланди, Бермудські острови
Transfer Pricing Manipulation	Завищення/заниження цін між пов’язаними компаніями для переміщення прибутку	$100+ млрд	Бразилія, Індія, Італія	Швейцарія, Сінгапур, Люксембург
Hybrid Mismatch Arrangements	Структури, де витрати визнаються в обох країнах, а доходи — в жодній	$10–20 млрд	Великобританія, Японія, Канада	Ірландія, Австрія, Гонконг
Patent Box / Royalty Schemes	Прибуток з патентів і роялті переводиться в юрисдикції з низьким оподаткуванням	$15–25 млрд	Франція, Південна Корея, Іспанія	Люксембург, Нідерланди, Кіпр
Thin Capitalization	Надмірне кредитування філій, що дозволяє зменшити податки через відсоткові платежі	$5–10 млрд	Аргентина, Польща, ПАР	Маврикій, Панама, Британські Віргінські острови

Commissionaire Arrangements	Компанії працюють як «агенти», а не як «постійні представництва», що знижує податки	$3–7 млрд	Швеція, Італія, Чилі	Ірландія, Швейцарія, Ліхтенштейн

Джерело: [9]

Схеми BEPS — це не порушення закону в класичному сенсі, а скоріше експлуатація прогалин у податкових системах, що дозволяє компаніям «виводити» прибуток з юрисдикцій, де реально ведеться діяльність, до країн з низькими або нульовими податками.

Фінансові злочини на міжбанківському рівні — це одна з найскладніших для виявлення форм порушення, оскільки злочинці часто використовують офіційні платіжні інфраструктури, схвалені регуляторами, для маскування незаконних потоків. Міжбанківські транзакції не тільки прискорюють обіг капіталу, але й створюють умови для транснаціональних маніпуляцій, особливо в умовах асиметричного регулювання фінансових центрів [9].

Кореспондентські рахунки — це банківські рахунки, які один банк відкриває в іншого для здійснення міжнародних платежів. Саме через них проходить переважна більшість глобальних транзакцій. За оцінками FATF (2023) [10]:

- 70–80% випадків відмивання коштів великого масштабу використовують кореспондентські рахунки.
- У 2022 році в середньому 43% банківських установ у країнах, що розвиваються, не могли простежити кінцевого бенефіціара транзакції, здійсненої через третій банк.

Такі рахунки дозволяють злочинцям "вкласти" кошти у легальні фінансові потоки, обійти фінансовий моніторинг і переказати кошти до офшорів чи небанківських структур без порушення внутрішніх процедур.

Переказ грошей через юрисдикції з недостатнім рівнем фінансового нагляду — класичний етап схем відмивання або ухилення. До таких центрів належать, наприклад, Латвія (до 2020 року), Кіпр, Люксембург, Мальта, ОАЕ. У 2021 році Глобальний індекс фінансової секретності (Financial Secrecy Index) вказав, що [10]:

- 20 з 30 найбільших фінансових центрів мають недостатній рівень прозорості щодо міжнародних переказів.
- Щонайменше 12 трлн доларів США обертається щорічно в юрисдикціях із "низьким контролем".

Фінансові потоки розгалужуються: зазвичай один переказ проходить через 3–5 банків у різних країнах, кожен з яких виконує обмежений контроль.

Попри те, що системи SWIFT (глобальні банківські повідомлення) та SEPA (єврозона) були створені для забезпечення безпечних і прозорих розрахунків, вони також використовуються у схемах фінансових злочинів:

- У звітах Europol та FinCEN за 2022 рік зазначається, що 40% складних схем відмивання коштів включають SWIFT-перекази через кореспондентські банки.
- SEPA, хоч і має високий рівень контролю, допускає виконання термінових платежів без миттєвої перевірки бенефіціара, що використовується у шахрайських схемах.

Окреме місце займає Hawala — неформальна система трансферу коштів, поширена в Азії, Близькому Сході та Африці. Вона базується на довірі та обходить офіційну банківську систему [11]. За оцінками Interpol, обсяги операцій через Hawala щороку становлять $100–150 млрд, із них до 20% можуть бути пов’язані з нелегальними операціями (контрабанда, тероризм, наркобізнес).

Таблиця 1.7 – Порівняння платіжних систем за прозорістю та ризиком

Платіжна система	**Юридичний статус**	**Рівень прозорості**	**Основні ризики**	**Поширеність використання у злочинах**
SWIFT	Офіційна глобальна міжбанківська система повідомлень	Високий (але залежить від банку-кореспондента)	Відмивання коштів через транзитні рахунки, складність верифікації бенефіціара	Висока (особливо у складних схемах)
SEPA	Офіційна система переказів у межах ЄС	Дуже високий (внутрішній контроль ЄС)	Використання термінових платежів без достатньої перевірки	Середня (у дрібних або шахрайських схемах)
Hawala	Неформальна, традиційна система довірчих переказів	Дуже низький (анонімність, без документів)	Фінансування тероризму, нелегальний трансфер готівки	Висока (особливо у регіонах Азії та Африки)

Джерело: [11]

Таким чином, міжбанківські платіжні системи — це двосічний інструмент: вони формують основу світової фінансової інфраструктури, але при цьому залишають вразливості, якими системно користуються злочинці. У контексті міжнародної боротьби з фінансовими правопорушеннями важливо не лише виявляти окремі порушення, а й будувати мережі регуляторної співпраці та автоматичного обміну фінансовими даними.

Однією з найвишуканіших форм фінансових злочинів у міжнародному середовищі є маскування нелегального походження коштів через нібито легітимні інвестиційні канали (табл.1.8). Злочинці, політично вразливі особи (PEP), корумповані чиновники та організовані угруповання активно використовують ринок нерухомості, цінного мистецтва, дорогоцінних металів, цінних паперів і новітніх цифрових активів для "відбілювання" капіталу (Додаток В).

Таблиця 1.8 – Маскування незаконного капіталу через інвестиційні інструменти

Інструмент / Сектор	**Схема / Метод**	**Оцінка щорічних обсягів**	**Основні ризики**	**Типові юрисдикції / регіони**
Елітна нерухомість	Купівля за кеш або через shell-компанії, перепродаж за вищою ціною	$1.6 трлн глобальний ринок; ~10% під ризиком	Приховування бенефіціарів, завищення вартості	Лондон, Дубай, Нью-Йорк, Ванкувер, Київ
Мистецтво та антикваріат	Покупка/продаж без оцінки справжньої вартості, зберігання в "freeports"	$65 млрд (з них 5–10% — сірі кошти)	Відсутність публічної реєстрації, низька прозорість	Швейцарія, Люксембург, Гонконг
Золото та дорогоцінні метали	Обмін готівки на золото, переправка через митницю без банківських слідів	$200+ млрд в глобальному обігу	Легкість перевезення, складність відстеження	ОАЕ, Індія, Туреччина, Західна Африка
Цінні папери / деривативи	Маніпуляції з ф’ючерсами, інсайдерська торгівля, фіктивні інвестиційні фонди	$50–70 млрд потенційного обсягу схем	Біржові шахрайства, відсутність контролю за фондами	США, ЄС, Сінгапур, офшори фондових ліцензій
ICO / криптоінвестиції	Створення фіктивного токена, залучення інвесторів, обмін на "чисті" криптовалюти	$24.2 млрд (нелегальні транзакції у 2023)	Відсутність регулювання, децентралізований обмін	Росія, Кіпр, Близький Схід, офшорні криптохаби

Джерело: [12]

Сучасна фінансова злочинність еволюціонує — від тіньових операцій до маскування в легальних ринках, де злочинна активність змішується з легітимною. Водночас посилення міжнародної фінансової розвідки та цифрового моніторингу відкриває нові шляхи протидії цим схемам.

Стрімкий розвиток цифрових технологій, включаючи криптовалюти, децентралізовані фінанси (DeFi), анонімні мережі доступу та смарт-контракти, суттєво змінив ландшафт сучасної фінансової злочинності [12]. З одного боку, ці інновації відкрили нові можливості для розвитку фінансових послуг, однак, з іншого — створили нові, значно менш контрольовані канали для маскування, переміщення та конвертації нелегальних коштів.

Криптовалюти, особливо ті, що не прив’язані до регульованих бірж (наприклад, Monero, Dash, Zcash), широко використовуються в схемах відмивання коштів, зокрема через так звані mixer-wallets або "тумблери", які перемішують транзакції багатьох користувачів, розмиваючи сліди їх походження. За даними Chainalysis (2024) [13]: У 2023 році загальний обсяг криптовалют, пов’язаних із незаконною діяльністю, сягнув $24.2 млрд. 66% всіх транзакцій через біткойн-міксери були пов’язані з даркнетом, шахрайством або хакерськими атаками.

DeFi-платформи, як-от Uniswap, Curve, Tornado Cash, функціонують без централізованого контролю і без процедури KYC (Know Your Customer), що робить їх зручними для злочинців, особливо при конвертації виведених коштів у стейблкоїни (USDT, DAI) або при виведенні за допомогою P2P-обміну [13].

Поряд із криптовалютними сервісами, злочинці активно використовують VPN-сервіси, мережі TOR і darknet-маркети для уникнення нагляду, проведення нелегальних транзакцій і обміну даними щодо фінансових злочинів. Ці інструменти дозволяють приховати IP-адреси, обійти географічні обмеження та забезпечити повну конфіденційність обміну [14]. Europol (2023) повідомляє, що понад 80% нелегальних товарів у даркнеті продаються з оплатою в криптовалюті, і більшість транзакцій здійснюється через приховані браузери TOR.

Новим і складним для регуляторів явищем стали смарт-контракти — алгоритмічні угоди, які автоматично виконують транзакції без участі людини.

Через ці контракти можна здійснювати "псевдозаконні" платежі, наприклад, вид зворотного фінансування, фіктивного обміну послуг або "гарантійного депозиту", що фактично маскує трансфер незаконних коштів. За оцінками CipherTrace (2023), понад $3.1 млрд було втрачено через шахрайство, експлойти або зловживання в DeFi-протоколах, із них близько 1/3 припадає на автоматизовані контракти без верифікації коду [15]. Такі схеми часто мають вигляд легальних угод, але в реальності є частиною складних ланцюжків для відмивання коштів, зокрема в кіберзлочинності, шантажі, хакерських атаках або ухиленні від санкцій (табл.1.9).

Таблиця 1.9 – Цифрові інструменти та їх використання у фінансових злочинах

Інструмент / Технологія	**Принцип дії**	**Типові злочини**	**Обсяг / Статистика**	**Рівень анонімності**
Криптовалюти (BTC, Monero)	Транзакції в децентралізованій мережі	Відмивання коштів, шантаж, даркнет-торгівля	$24.2 млрд злочинних транзакцій у 2023 (Chainalysis)	Середній – дуже високий
DeFi-платформи	Обмін активами без контролю бірж або банків	Конвертація доходів, відхід від KYC	$2.8 млрд незаконних переказів через DeFi	Високий (повна децентралізація)
Mixer-гаманці (Tornado Cash)	Перемішування транзакцій з десятків адрес	Маскування слідів, відмивання хакерських доходів	66% всіх mixer-переказів — злочинні кошти	Дуже високий
VPN / TOR	Приховування IP-адрес і активності користувача	Даркнет-операції, ухилення від геоконтролю	80% торгівлі у даркнеті — криптовалютна	Високий
Смарт-контракти	Автоматизовані угоди, що не потребують втручання людини	Симуляція послуг, фіктивні контракти, схеми DeFi	$3.1 млрд втрат у 2023 від експлойтів	Залежить від платформи

Джерело: [15]

Таким чином, цифрові технології — це не лише інструмент інновацій, але й високоризикова зона, яка активно використовується для обходу фінансових правил і маскування походження коштів. Їхня швидкість, децентралізований характер і глобальний доступ створюють виклик навіть для найрозвиненіших регуляторних

систем, які часто не встигають адаптуватися до технологічної динаміки злочинного середовища.

Корупційні практики у вигляді підкупу, змов і "відкатів" становлять одну з найстійкіших форм тіньової економіки, особливо у сфері міжнародних фінансових операцій. У глобалізованому середовищі, де багатомільйонні транскордонні контракти укладаються між урядами, корпораціями та інституціями, ризик зловживань службовим становищем зростає в геометричній прогресії. Корупційна складова в таких угодах часто є не лише побічною загрозою, а центральним механізмом для виведення та легалізації незаконно отриманих коштів.

Міжнародні контракти — особливо в сферах інфраструктури, оборони, енергетики або медичних закупівель — нерідко супроводжуються прихованими домовленостями між посадовцями та приватними структурами. Зловживання службовим становищем може проявлятися у навмисному завищенні вартості контракту, наданні переваги "своїм" компаніям або формальному дотриманні тендерних процедур з наперед визначеним переможцем [16]. За даними Transparency International (2022), до 25% великих інфраструктурних контрактів у країнах, що розвиваються, мають ознаки корупційної змови або конфлікту інтересів. У звіті World Bank (2020) зазначено, що втрати держав унаслідок корупційних зловживань при реалізації міжнародних проєктів сягають від 10% до 30% їхньої загальної вартості.

Так звані "неформальні альянси" в міжнародних тендерах — це попередні домовленості між учасниками ринку та організаторами торгів, що забезпечують одному з учасників перевагу в обмін на комерційні або політичні поступки. У таких випадках тендер є лише формальністю, а справжнє рішення ухвалюється кулуарно, часто за винагороду у формі відкату.

Окремі схеми передбачають створення штучної конкуренції, де кілька компаній належать до однієї групи, або "зливання" умов участі в торгах наперед визначеному підряднику. У міжнародній практиці такі явища трапляються навіть на рівні міжурядових домовленостей, особливо в галузях, де відсутній або мінімальний нагляд міжнародних аудиторів [16].

Ще одним вишуканим механізмом легалізації коштів є використання псевдоблагодійних або квазігуманітарних організацій, через які оформлюється фінансування на нібито соціальні, освітні або медичні проєкти. У багатьох випадках значна частина коштів не доходить до кінцевого бенефіціара, а осідає на рахунках підставних осіб або йде на оплату фіктивних послуг. За даними OECD Anti-Bribery Working Group (2021), у понад 12% випадків міжнародної корупції кошти проходять через благодійні організації, які формально не підпадають під жорсткі норми фінансового моніторингу.

Особливо часто такі схеми спостерігаються в постконфліктних регіонах, де велика кількість зовнішньої допомоги та низький інституційний контроль створюють сприятливі умови для непрозорого розподілу ресурсів. Крім того, міжнародний статус гуманітарних організацій ускладнює проведення незалежного розслідування чи перевірки їхніх фінансових потоків [17].

Таким чином, підкуп, змова та "відкати" є не просто наслідками недосконалого управління, а структурованими схемами, що інтегровані у міжнародну фінансову взаємодію. Їх транснаціональний характер, гнучкість форм та високий ступінь латентності ускладнюють виявлення та переслідування, водночас підриваючи довіру до механізмів міжнародної фінансової співпраці. Боротися з цими практиками можливо лише через зміцнення інституційної відповідальності, впровадження антикорупційного аудиту на кожному етапі транскордонних проєктів та обов’язкову прозорість усіх транзакцій у межах публічних контрактів.

1.3. Нормативно-правове регулювання боротьби з міжнародними фінансовими злочинами

Міжнародно-правова база відіграє фундаментальну роль у формуванні глобальних стандартів боротьби з фінансовими злочинами. Через конвенції, директиви та рекомендації міжнародні інституції встановлюють правові орієнтири, що зобов’язують держави-учасниці до криміналізації певних діянь, впровадження

систем фінансового моніторингу та забезпечення міждержавної правової допомоги.

Конвенція ООН проти транснаціональної організованої злочинності (2000) - прийнята у Палермо, ця Конвенція стала першим комплексним документом, який регламентує боротьбу з організованою злочинністю, у тому числі в її фінансових проявах. Вона передбачає обов'язкову криміналізацію відмивання доходів, корупції, перешкоджання правосуддю та участі в організованих злочинних угрупованнях [18]. Крім того, документ визначає механізми міжнародної співпраці: екстрадиції, взаємної правової допомоги, передачі кримінального переслідування та захисту свідків. Конвенція зобов'язує держави створити фінансову розвідку (FIU) та запровадити системи для ідентифікації підозрілих транзакцій, що значно посилило роль банківського сектора у протидії злочинам.

UNCAC — перша універсальна антикорупційна конвенція, яка охоплює як запобігання, так і криміналізацію корупційних діянь, включно з підкупом, незаконним збагаченням, розтратами державних коштів та відмиванням корупційних активів. Конвенція також закликає держави встановити прозорість у публічних фінансах, запровадити декларування активів чиновників і створити незалежні антикорупційні органи. Особливістю UNCAC є положення про повернення викрадених активів (asset recovery) — безпрецедентна правова новація, яка дозволяє жертвам міжнародної корупції претендувати на реституцію незаконно виведених коштів.

ЄС створив одну з найрозвиненіших правових систем протидії фінансовим злочинам. Особливо важливу роль відіграють 4-та, 5-та та 6-та директиви про боротьбу з відмиванням грошей (AMLD) [18]:

- 4-та AMLD (2015) — ввела обов'язкову ідентифікацію бенефіціарних власників, підвищила стандарти KYC і встановила вимоги до фінансових установ, юристів, аудиторів та нерухомості.
- 5-та AMLD (2018) — поширила регулювання на криптовалютні платформи та електронні гаманці, зобов'язала створити публічні реєстри бенефіціарів.

•6-та AMLD (2021) — вперше встановила єдиний перелік фінансових злочинів (22 категорії), ввела поняття "співучасті юридичних осіб" та зобов’язала держави встановити мінімальні санкції.

Ці директиви не лише уніфікують підходи в межах ЄС, а й суттєво впливають на країни-кандидати та держави-сусіди, змушуючи їх адаптувати своє законодавство до європейських стандартів (табл.1.10).

Таблиця 1.10 – Порівняльна характеристика ключових міжнародно-правових актів у сфері фінансових злочинів

Критерій	**Конвенція ООН проти транснаціональної організованої злочинності (2000)**	**Конвенція ООН проти корупції (UNCAC, 2003)**	**4–6-та AML-директиви ЄС (2015–2021)**
Тип правового інструменту	Міжнародна конвенція	Універсальна антикорупційна конвенція	Наднаціональні регуляторні директиви ЄС
Сфера охоплення	Організована злочинність, відмивання, фінансова змова	Корупція, незаконне збагачення, активи	Відмивання коштів, фінмоніторинг, криптоактиви
Обов'язкова імплементація	Так (ратифікація)	Так (ратифікація)	Так (для країн ЄС), добровільна гармонізація для третіх країн
Фокус на юридичних особах	Обмежений (через участь у злочинних угрупованнях)	Помірний (контроль за посадовцями)	Високий (вперше введено обов’язкову відповідальність компаній)
Визначення злочинів	Широке, без чіткого переліку	Стандартизоване, але гнучке	Вперше чітко визначено 22 види злочинів
Регуляція криптовалют і DeFi	Відсутня	Відсутня	Так (починаючи з 5-ї директиви AMLD)
Наявність механізму повернення активів	Обмежений (через конфіскацію)	Чітко прописаний (asset recovery)	Не передбачено
Обмін фінансовою інформацією	Механізми міждержавної допомоги (MLA)	Так, через координацію з антикорупційними органами	Так — фінансові розвідки, банківські реєстри
Гнучкість щодо адаптації до нових викликів	Низька — фіксований текст Конвенції	Помірна — можливі інтерпретації	Висока — оновлювані директиви кожні кілька років
Країни-учасниці / охоплення	190+ країн	180+ країн	27 країн ЄС + країни-кандидати та асоційовані

Джерело: [19]

У глобальному середовищі, де фінансові потоки виходять далеко за межі національних юрисдикцій, ефективна протидія фінансовим злочинам неможлива без участі міжурядових організацій. Саме вони виступають творцями стандартів, координаторами політик та платформами обміну даними, завдяки яким держави можуть забезпечувати синхронізовану відповідь на виклики, пов’язані з відмиванням коштів, ухиленням від податків та фінансуванням тероризму.

FATF (Financial Action Task Force) — міжурядовий орган, створений у 1989 році за ініціативи G7, який на сьогодні включає 39 учасників. Його головний інструмент — 40 Рекомендацій, які охоплюють ключові сфери фінансової безпеки: ідентифікація клієнтів, фінансовий моніторинг, прозорість бенефіціарів, криміналізація фінансових злочинів, санкційні режими, ризик-орієнтований підхід [20]. Особливістю FATF є механізм взаємної оцінки (Mutual Evaluation Reports), який визначає відповідність держав міжнародним стандартам і може призводити до включення в "сірі" або "чорні списки". Це стимулює країни не лише ухвалювати закони, а й забезпечувати їх практичну реалізацію.

Організація економічного співробітництва та розвитку (OECD) виступає лідером у сфері боротьби з агресивним податковим плануванням, яке лежить в основі багатьох транснаціональних схем фінансових зловживань. Її флагманська ініціатива BEPS (Base Erosion and Profit Shifting) спрямована на запобігання штучному виведенню прибутків у низькоподаткові юрисдикції. OECD також запустила Common Reporting Standard (CRS) — глобальний стандарт автоматичного обміну податковою інформацією, який до 2024 року запровадили понад 110 юрисдикцій [21]. Ці інструменти створюють правову основу для прозорості у транскордонних капітальних потоках, зменшуючи можливості для маніпуляцій із трансфертним ціноутворенням, роялті, ліцензійними платежами тощо.

На додачу до глобальних структур, дедалі більшого значення набувають регіональні мережі, які забезпечують оперативну реалізацію стандартів FATF та створюють середовище для обміну кращими практиками (табл.1.11).

•MONEYVAL — орган Ради Європи, що здійснює моніторинг виконання стандартів FATF у Східній Європі, Кавказі та частині Центральної Азії.

•GAFILAT — регіональна структура FATF для Латинської Америки, яка враховує локальні виклики, пов'язані з наркобізнесом і готівковими економіками.

•Egmont Group — мережа з понад 160 фінансових розвідувальних підрозділів (FIUs), яка забезпечує оперативний транскордонний обмін розвідувальною інформацією, зокрема щодо підозрілих транзакцій, цифрових активів, фінансування терористичних мереж.

Завдяки таким організаціям формується інфраструктура фінансової безпеки нового типу — гнучка, модульна і зорієнтована на ризики, а не формальні індикатори [21].

Таблиця 1.11 – Порівняльний аналіз ролі ключових міжурядових ініціатив

Організація / Ініціатива	**Головна мета**	**Основний інструмент впливу**	**Охоплення / Формат участі**	**Особливі функції**
FATF	Протидія відмиванню коштів і фінансуванню тероризму	40 Рекомендацій + список ризикованих юрисдикцій	39 членів + 9 регіональних груп	Взаємна оцінка, рекомендації, тиск через фінансову ізоляцію
OECD / BEPS	Боротьба з податковими схемами великих компаній	BEPS-інструменти (15 дій) + Common Reporting Standard	140+ країн у BEPS Inclusive Framework	Обмін податковою інформацією, мінімальний глобальний податок
MONEYVAL (РЄ)	Оцінка ризиків і впровадження AML/CFT стандартів у Європі	Візити, звіти, технічна допомога	34 країни (Рада Європи + сусіди)	Сприяння імплементації FATF у постсоціалістичних державах
GAFILAT	Регіональна координація боротьби з фінансовими злочинами	Технічні звіти, керівні принципи, моніторинг	17 країн Латинської Америки	Адаптація FATF до локальних реалій, зокрема готівкових схем
Egmont Group	Обмін розвідданими між фінансовими розвідками (FIUs)	Платформа обміну + конфіденційна співпраця	160+ FIUs по всьому світу	Реальний обмін файлами підозрілих транзакцій і кіберрозвідка

Джерело: [21]

У підсумку, міжнародні організації не просто формулюють політику, а створюють нормативну екосистему, в якій взаємодіють держава, бізнес, банки, фінтех і правоохоронні органи. Їх роль полягає не лише у розробці стандартів, а у формуванні глобального фінансового мислення, де боротьба з фінансовими злочинами — спільна і безперервна стратегія, а не суто національне завдання.

Адаптація національного законодавства до міжнародних стандартів боротьби з фінансовими злочинами — це ключовий етап трансформації правових систем у глобалізованому фінансовому середовищі. Попри наявність загальновизнаних орієнтирів (FATF, UNCAC, AMLD), імплементація цих норм у різних країнах відбувається нерівномірно через відмінності правових традицій, рівня інституційного розвитку, політичної волі та економічних інтересів.

У США основна увага приділяється жорсткому регулюванню фінансового сектора та посиленій відповідальності юридичних осіб, що закріплено в Patriot Act, Bank Secrecy Act та положеннях FinCEN. ЄС фокусується на регламентованій уніфікації через директиви AMLD, що зобов'язують країни-члени вводити системи розкриття бенефіціарів, автоматичного обміну даними та криміналізації 22 типів фінансових злочинів. В Україні поступово впроваджуються вимоги FATF та ЄС, зокрема через Закон "Про фінансовий моніторинг", однак практичне виконання часто гальмується інституційними слабкостями й низькою якістю правозастосування [22].

Серед ключових викликів гармонізації — різні правові сім'ї (англосаксонська, континентальна, пострадянська), обмежений технічний потенціал, а також неповний доступ до глобальних механізмів автоматичного обміну інформацією (табл.1.12).

Таблиця 1.12 – Адаптація міжнародних стандартів у США, ЄС та Україні

Країна	**Ключові регулятори**	**Відповідність стандартам FATF / ЄС**	**Особливості фінансового моніторингу**	**Статус розкриття бенефіціарів**	**Основні виклики імплементації**
США	FinCEN, SEC, IRS	FATF-compliant	Жорстке KYC, SAR-звіти, банківський моніторинг	Єдиний нац. реєстр (2021)	Висока складність законодавства, кіберризики

ЄС	Єврокомісія, EBA, нац. FIUs	AMLD 4–6	Гармонізоване AML-регулювання, санкційні списки, реєстри PEP	Публічні реєстри у 20+ країнах	Різна якість реалізації в нових/старих членах ЄС
Німеччина	BaFin, Zentralstelle für Finanztransaktio-nsuntersuchungen	AMLD + FATF	Посилена перевірка в нерухомості, адвокатурі, криптообміні	Реєстр з 2019 року	Недостатня цифровізація реєстрів
Франція	TRACFIN, AMF	Повна відповідність	Централізоване виявлення PEP, обов'язкове повідомлення про великі транзакції	Прямий доступ банків до реєстрів	Вразливість до складних офшорних схем
Україна	Держфінмоніторинг, НБУ, БЕБ	Часткова відповідність	KYC, реєстр бенефіціарів, криміналізація фінзлочинів, регулювання крипто	Реєстр працює з 2021 р.	Нерівномірна імплементація, низька спроможність FIU
ОАЕ (Дубай)	UAE FIU, DFSA (DIFC)	Частково відповідає FATF	Обмежене розкриття в free zones, контроль вимагає посилення	Обмежений доступ до даних	Високий ризик готівкових та офшорних схем
Швейцарія	MROS, FINMA	Висока відповідність	Високий рівень перевірки в банках, фокус на ПЕП	Частковий доступ, не завжди публічний	Банківська таємниця vs міжнародні вимоги

Джерело: [22]

Ця таблиця дозволяє побачити реальний стан адаптації: хоча формальна відповідність міжнародним стандартам декларується багатьма державами, глибина реалізації норм та ефективність фінансового контролю суттєво різниться, особливо щодо цифрових активів, корпоративної прозорості й міжнародної координації розслідувань.

У глобалізованому світі, де фінансові транзакції за долі секунди перетинають кілька юрисдикцій, а злочинці можуть керувати капіталом з будь-якого куточка планети, жодна країна не здатна самостійно протидіяти фінансовим злочинам. Саме тому особливу роль у сучасній фінансовій безпеці відіграють

механізми міжнародної співпраці у сфері правозастосування, які дозволяють країнам діяти скоординовано, оперативно і без зайвих бар'єрів [23].

Базовим інструментом міжнародного кримінального співробітництва є екстрадиція осіб, підозрюваних у вчиненні фінансових злочинів. Сучасні угоди про взаємну правову допомогу (MLA — Mutual Legal Assistance) дозволяють не лише передавати осіб, а й спільно розслідувати справи, допитувати свідків через кордон, здійснювати арешт активів та документів.

Ключовими вузлами такого обміну є фінансові розвідувальні підрозділи (FIU), які існують у більшості країн. Через мережу Egmont Group ці підрозділи можуть швидко обмінюватися підозрілою інформацією про трансакції, що є вирішальним у боротьбі з кіберфінансовими злочинами, криптошахрайством і фіктивними фондами.

Наднаціональні правоохоронні структури забезпечують логістику, аналітику та цифрову взаємодію між державами. Інтерпол розміщує "червоні повідомлення" щодо розшуку підозрюваних у фінансових злочинах і забезпечує комунікацію між нацполіціями. Європол має спеціалізований центр EC3 (European Cybercrime Centre), який розслідує фінансові злочини в ЄС, зокрема біржові маніпуляції, криптоафери, шахрайство з банківськими даними. Офіс ООН з наркотиків і злочинності (UNODC) забезпечує нормативну підтримку, технічну допомогу та координує глобальні тренінги з розслідування та судового переслідування фінансових злочинів, особливо в країнах, що розвиваються [23].

Сучасні фінансові злочини не можна ефективно розслідувати без автоматизованого обміну даними. Саме тому країни дедалі частіше приєднуються до багатосторонніх платформ, які уникають бюрократії та діють у режимі реального часу [23].

- CRS (Common Reporting Standard) — ініціатива OECP, яка передбачає щорічний автоматичний обмін податковою інформацією між понад 110 країнами.
- AMLA (Anti-Money Laundering Authority) — новий орган ЄС, запуск якого запланований на 2025 рік, координуватиме нагляд за великими банками та централізуватиме AML-регулювання на рівні блоку.

- CARIN (Camden Asset Recovery Inter-Agency Network) — глобальна платформа для співпраці між митними, судовими та антикорупційними структурами з фокусом на виявлення, арешт і конфіскацію активів, що були отримані незаконно.

У сукупності, ці механізми формують транскордонну інфраструктуру правозастосування нового покоління — цифрову, скоординовану й проактивну. Вони не лише дозволяють обмінюватися даними, але й встановлюють нові стандарти оперативності, юридичної взаємодії та спільної відповідальності у сфері фінансової безпеки.

РОЗДІЛ 2.
СУЧАСНІ ЗАСОБИ ЗАПОБІГАННЯ ТА ПРОТИДІЇ МІЖНАРОДНИМ ФІНАНСОВИМ ЗЛОЧИНАМ

2.1. Інституційний механізм протидії міжнародним фінансовим злочинам

У системі протидії міжнародним фінансовим злочинам ключову роль відіграє інституційний механізм, який представляє собою сукупність взаємопов'язаних організацій, органів влади, нормативних структур та технологічних інструментів, що координовано забезпечують виявлення, запобігання та розслідування фінансових правопорушень. У контексті фінансової безпеки інституційний механізм є опорним компонентом економічної та правової архітектури, спрямованої на захист як національних, так і міжнародних фінансових систем.

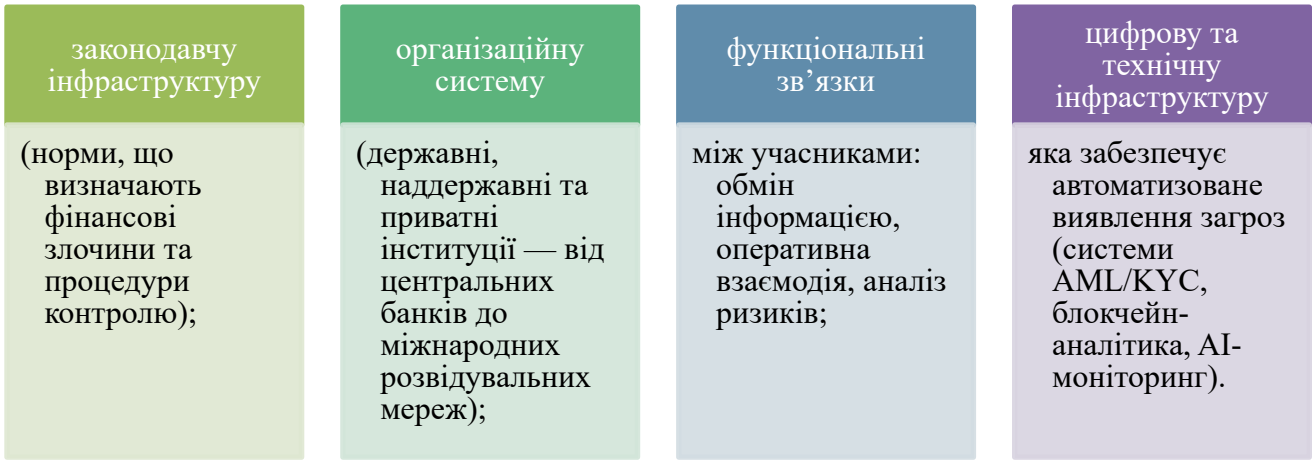

Рисунок 2.1 – Інституційний механізм охоплює
Джерело: [24]

Інституції, що входять до цього механізму, реалізують комплекс функцій, які можна класифікувати за такими напрямами [24]:

- Нормативно-регуляторна функція — розробка та оновлення законодавства відповідно до міжнародних стандартів (FATF, AMLD, BEPS), визначення переліку фінансових злочинів, встановлення санкцій і процедур контролю.

- Аналітично-моніторингова функція — збір, обробка та аналіз фінансових даних для виявлення підозрілих транзакцій або нетипової поведінки учасників ринку. Тут ключову роль відіграють фінансові розвідувальні підрозділи (FIU), аналітичні центри центральних банків, автоматизовані AML-системи.
- Правозастосовна та слідча функція — здійснення кримінального переслідування, взаємодія з міжнародними правоохоронними структурами (Інтерпол, Європол), екстрадиція, арешт активів, реалізація санкцій.
- Координаційна функція — забезпечення зв'язку між національними та міжнародними структурами, включаючи обмін фінансовою інформацією, спільні розслідування та участь у глобальних ініціативах (Egmont Group, CARIN).
- Превентивна функція — просування стандартів прозорості, етичної поведінки та фінансової грамотності серед суб'єктів ринку, включаючи підвищення корпоративної відповідальності та контроль за бенефіціарною власністю.

Таким чином, інституційний механізм протидії фінансовим злочинам — це не лише сукупність окремих органів, а складна динамічна система, яка функціонує на стику права, фінансів, технологій і міжнародної політики [25]. Її ефективність визначається не лише якістю інституцій, а й здатністю забезпечити цілісну, адаптивну та ризик-орієнтовану модель безпеки, яка відповідає новим загрозам — зокрема, у цифровому та транскордонному вимірі.

На практичному рівні, боротьба з міжнародними фінансовими злочинами є неможливою без участі наднаціональних структур, які не лише встановлюють правила гри, а й координують розслідування, обмін інформацією, розробку індикаторів ризику, а іноді — навіть оперативні втручання. Такі інституції не мають виключно політичного або нормотворчого характеру: вони функціонують як мережі з оперативною логікою, часто інтегровані у щоденну роботу фінансової розвідки, слідчих органів та банківського сектора (табл.2.1).

Міжнародна співпраця між цими структурами охоплює п'ять ключових форм [26]:

•Спільні розслідування та task forces — тимчасові робочі групи з обмеженим мандатом (напр., FATF–Interpol–Europol task force проти фінансування тероризму).

•Оцінки ризиків та трендові огляди — регулярні публікації Egmont/FATF (наприклад, типології злочинів у DeFi).

•Оперативний обмін файлами через захищені платформи — FIU.net, goAML, EFECC.

•Пілотні технологічні проєкти — проєкти з блокчейн-аналітики, спільні хаби з AML-алгоритмами (наприклад, LATAM Risk Radar).

•Технічна допомога та інституційне навчання — UNODC та Європол проводять регулярні курси для аналітиків з крипторизиків, кіберфінансових схем тощо.

Таблиця 2.1 Міжнародні інституції та їхні прикладні функції

Інституція	Сфера впливу	Унікальна функція	Формат координації	Орієнтація на майбутнє
FATF	Глобальні стандарти AML/CFT	Рейтинговий тиск через "сірі списки"	Моніторинг, оцінка юрисдикцій, тематичні звіти	Цифрові ризики, нові форми капіталу
Egmont Group	Обмін між FIU	Автоматизовані запити по підозрілих транзакціях	Платформа FIU.net, тренінги, оперативні форуми	Розширення аналітичних повноважень FIU
UNODC	Технічна підтримка країн	Нарощування спроможності в країнах з "регуляторними прогалинами"	Регіональні програми, інституційна допомога	Інтеграція з цифровими AML-рішеннями
Європол	Розслідування в ЄС	Аналіз великих масивів даних, цифрові профілі фінансових схем	Центри AP SIRIUS, AP FININT, спільні рейди	Інтеграція із фінтех, партнерство з банками
Інтерпол	Міжнародна розвідка і арешти	Фінансовий розшук, розслідування злочинних груп із доступом до SWIFT-даних	Міждержавні task forces, червоні повідомлення	Оперативна реакція на глобальні схеми шахрайства

Джерело: [26]

У підсумку, міжнародні інституції перетворюються з "центрів консенсусу" на оперативні гравці, здатні не лише формулювати стандарти, а й забезпечувати реальну міждержавну дію у сфері розслідування, моніторингу і конфіскації активів. Їх майбутнє — це інституційна інтеграція, цифрова взаємодія та реактивність, яка не відстає від злочинця, а випереджає його.

Одним із найбільш резонансних прикладів міжнародної співпраці у боротьбі з фінансовими злочинами є справа Danske Bank, пов’язана з відмиванням понад 230 млрд євро через естонське відділення банку у 2007–2015 роках. Справа продемонструвала не лише вразливість фінансової системи Європи, але й ефективність скоординованої взаємодії між міжнародними інституціями у межах інституційного механізму правозастосування [27].

1. Ініціювання справи та виявлення системних порушень (2017–2018)

У 2017 році FSA Естонії та Данії розпочали перевірку внутрішніх контролів Danske Bank на основі низки підозрілих транзакцій, виявлених фінансовими розвідувальними підрозділами (FIU) Латвії, Великої Британії та Нідерландів.

Водночас Egmont Group активувала канали захищеного обміну даними між FIU відповідних країн, що дозволило побудувати початкову карту переміщення коштів.

2. Аналітична обробка та координація розслідування (2018–2019)

Після оприлюднення внутрішнього звіту Danske Bank у вересні 2018 року, Європол ініціював створення Joint Intelligence Cell за участі Національного бюро Нідерландів, прокуратури Франції та митної служби Німеччини.

Паралельно, FATF включив Естонію до списку країн з "значним ризиком виведення капіталу через банківські філії", а Єврокомісія почала підготовку до створення AMLA — централізованого органу для моніторингу банків.

3. Виявлення іноземних активів та транскордонна координація (2019–2020)

Завдяки співпраці з UNODC, виявлено зв'язки між коштами, що пройшли через Danske Bank, та офшорними фондами у Великобританії, ОАЕ та Швейцарії. Інтерпол, на підставі запиту з боку правоохоронних органів Естонії, видає "червоні

повідомлення" на кількох ключових фігурантів справи — зокрема, колишніх директорів естонського підрозділу.

У грудні 2019 року CARIN (Camden Asset Recovery Inter-Agency Network) починає процедури міжнародної конфіскації активів, арештованих у Німеччині, Литві та Чехії.

4. Судові дії та міжнародна реакція (2021–2023) [28]

- У 2021 році Міністерство юстиції США відкриває справу щодо Danske Bank відповідно до Закону про банківську таємницю (BSA).
- У грудні 2022 року банк погоджується на штраф у розмірі $2,06 млрд за роль у схемах відмивання коштів.
- Водночас Європейський центральний банк (ЄЦБ) та Європейський банківський орган (EBA) розробляють нові вимоги щодо due diligence для філій іноземних банків.

Справа Danske Bank стала ключовим прецедентом координації між FATF, Egmont Group, Європолом, Інтерполом та UNODC, яка охоплювала всі етапи — від обміну інформацією до судових рішень і конфіскації активів. Вона чітко демонструє, що інституційний механізм боротьби з фінансовими злочинами у XXI столітті — це динамічна, міжвідомча і транснаціональна система, де ефективність залежить від якості комунікації, інтеграції цифрових рішень і політичної волі до прозорості.

Незважаючи на глобалізацію механізмів протидії фінансовим злочинам, саме національні органи залишаються першою лінією захисту, оскільки саме вони ініціюють перевірки, реагують на підозрілі транзакції та забезпечують юридичне оформлення кримінальних проваджень [28]. Водночас їхня ефективність значною мірою залежить від рівня інституційної зрілості, доступу до інформації, технічного оснащення та політичної незалежності. В ідеалі, кожна країна повинна не лише мати власну фінансову розвідку (FIU), а й інтегрувати її у глобальну систему швидкого обміну та аналітичної взаємодії.

FinCEN — Financial Crimes Enforcement Network — є однією з найвпливовіших структур світу у сфері AML/CFT. Її функції виходять далеко за

межі внутрішньої розвідки: FinCEN формує міжнародні сигнали, координує глобальні розслідування (наприклад, FinCEN Files) та фактично встановлює стандарти аналітики транзакцій [29]. Щомісяця ця служба опрацьовує понад 2 млн SAR-звітів про підозрілі операції, генерує автоматичні алерти та координує з іншими FIU через Egmont Group. Її вплив є репутаційно значущим: згадки у звітах FinCEN призводять до миттєвої реакції ринків.

TRACFIN функціонує під Міністерством економіки Франції та спеціалізується на відслідковуванні нетипових транзакцій, особливо пов'язаних із ПЕП (політично значущими особами) та публічними тендерами. Завдяки прямому доступу до банківських, митних та податкових реєстрів, TRACFIN володіє високим рівнем автономії. У 2023 році служба передала до прокуратури понад 1 200 обґрунтованих досьє, з яких 70% — у справах великої корупції та офшорних схем. Особливістю французької моделі є активна співпраця з журналістами-розслідувачами (наприклад, Mediapart), що формує прозору екосистему антикорупційного тиску [30].

В Україні Державна служба фінансового моніторингу має офіційний статус FIU і є учасником Egmont Group. Вона здійснює верифікацію фінансових транзакцій, аналізує ризики та надсилає аналітичні матеріали до БЕБ, СБУ та НАБУ (табл.2.2). Але на практиці її ефективність обмежується кількома критичними чинниками:

- Низька оперативна автономія — будь-яке аналітичне повідомлення стає "залежним" від рішення силових органів.
- Недостатній доступ до міжнародних фінансових даних — попри формальну участь в Egmont Group, швидкість обміну нижча за середню по Європі.
- Політична вразливість — керівництво служби неодноразово змінювалось за кулуарними домовленостями, що підриває довіру партнерів.

У 2022 році, за офіційною статистикою, Держфінмоніторинг передав 934 аналітичних повідомлення, однак менше 20% з них стали підставою для відкриття проваджень.

Таблиця 2.2 Національні FIU і їх спроможність до взаємодії

Параметр	FinCEN (США)	TRACFIN (Франція)	Держфінмоніторинг (Україна)
Організаційна автономія	Висока (незалежна у межах Мінфіну)	Висока (економічний блок уряду)	Часткова (підпорядкування уряду)
Кількість SAR/заявок на рік	2+ млн звітів	~110 000 транзакцій перевіряється щороку	~180 000 повідомлень про фіноперації
Кількість справ, переданих до слідства	>15 000 на рік	1 200+ (2023)	934 (2022)
Процент успішних кримінальних справ	~50% справ призводять до суду	~60–70%	~18–20% (оціночні дані, відсутність офіційної публікації)
Інтеграція з Egmont Group	Активна участь, обмін у реальному часі	Стабільна інтеграція	Формальна участь, повільна взаємодія
Доступ до податкових/реєстрових даних	Повний	Повний	Частковий, з міжвідомчими бар'єрами
Наявність цифрової аналітики (AI/ML)	Системи прогнозування ризику	Аналітика на базі банківських API	Відсутня або в зародковому стані

Джерело: [31]

У той час як США та Франція демонструють приклад аналітично автономних і структурно захищених FIU, український механізм перебуває на перехресті декларативної відповідності та реальної інституційної обмеженості. Реформа Держфінмоніторингу повинна включати не лише технічне оновлення, а й гарантії незалежності, прямого доступу до ключових баз даних та право ініціації проваджень, інакше Україна залишатиметься слабкою ланкою в глобальній фінансовій безпеці.

Попри існування багаторівневої архітектури міжнародного контролю, ефективність інституційної взаємодії часто підривається системними бар'єрами. Одним із ключових викликів залишається недостатня синхронізація юрисдикцій, зумовлена різними правовими системами, підходами до визначення злочинів і процедурами розслідування. Навіть у межах ЄС спостерігається фрагментація підходів до AML/CFT. Ще гострішою є проблема повільного або обмеженого обміну фінансовою інформацією [31]. Навіть членство в Egmont Group не гарантує швидкості: на практиці передача файлів часто вимагає бюрократичних погоджень

або зупиняється через відсутність двосторонніх угод. Також слід визнати роль політичних бар'єрів — втручання у роботу FIU, блокування справ проти політично значущих осіб (PEP), конфлікти інтересів між правоохоронними й урядовими структурами. У таких умовах навіть найкращі аналітичні системи втрачають ефективність (табл.2.3).

Таблиця 2.3 Системні обмеження інституційної взаємодії у сфері протидії фінансовим злочинам

Тип обмеження	Опис проблеми	Типові прояви	Країни, де спостерігається	Наслідки для системи	Тип обмеження
Недостатня синхронізація юрисдикцій	Різні визначення злочинів, процедури доказування, строки зберігання даних	Неможливість екстрадиції, розсинхронення доказової бази	США–ЄС, Франція–Африка, Україна–офшори	Втрата доказів, подвоєння розслідувань	Недостатня синхронізація юрисдикцій
Відсутність оперативного обміну	Повільні відповіді на запити, обмежений доступ до фінансових реєстрів	Запити FIU розглядаються тижнями, а не годинами	Італія, Румунія, більшість країн СНД	Зрив розслідувань, переміщення активів поза юрисдикцію	Відсутність оперативного обміну
Політичне втручання та конфлікти	Залежність керівництва FIU, втручання у справи, що зачіпають політичну еліту	Зміна керівників антикорупційних органів, блокування підозрілих справ	Угорщина, Туреччина, Україна, Ліван	Низька довіра міжнародних партнерів, втеча фігурантів	Політичне втручання та конфлікти
Нестача аналітичних потужностей	Відсутність технологій на базі AI, слабка кібербезпека, неінтегровані реєстри	Звітність в Excel, затримки у верифікації транзакцій	Киргизстан, Болгарія, Молдова	Неможливість ідентифікації складних схем	Нестача аналітичних потужностей

Джерело: [32]

Технічна інтеграція — лише пів справи: без незалежності, оперативності та міжнародного правового узгодження інституційна архітектура залишається крихкою, особливо в країнах із гібридними режимами та політичним тиском на антикорупційні органи.

2.2. Інноваційні засоби виявлення і запобігання фінансовим злочинам

У XXI столітті фінансова безпека вже не обмежується контролем за готівкою, банками чи митними операціями. У цифрову епоху зростання криптоактивів, алгоритмічних транзакцій і транскордонної віртуалізації капіталу інновації стали ключовим захисним щитом проти нових форм злочинності. Протидія сучасним фінансовим злочинам більше не можлива лише завдяки нормативним приписам — вона потребує технологічної переваги, адаптивності та аналітичного мислення в реальному часі.

Інновації у сфері фінансової безпеки — це не просто технологічні новації, а глибокі трансформації в способі виявлення, оцінювання та реагування на фінансові загрози. У контексті протидії фінансовим злочинам інновації означають нові, цифрово орієнтовані та аналітично підкріплені рішення, здатні замінити традиційні бюрократичні процедури високоточними, масштабованими і швидкодійними механізмами [33].

Такі рішення охоплюють автоматизоване виявлення ризиків у потоках фінансової інформації, прогнозування складних злочинних схем ще до їх фактичної реалізації, підвищення прозорості транзакцій на основі блокчейн-технологій, а також миттєву реакцію на загрози без необхідності ручного втручання людини. Тобто йдеться не лише про програмне забезпечення, а про системну зміну парадигми фінансового контролю.

У сучасному розумінні інновації — це інтеграція машинного навчання (AI/ML), блокчейн-аналітики, цифрових ідентифікаторів, верифікації даних та біометричних рішень, які формують нову інфраструктуру превентивного впливу. Такі технології дають змогу не лише реагувати на злочини, а й випереджати їх, формуючи своєрідний "цифровий імунітет" фінансової системи. Вони стають новою формою юридичного тиску, де право реалізується не через затримку і санкцію, а через швидке виявлення й автоматичне блокування аномальних дій (рис.2.2). Таким чином, інновації у фінансовій безпеці — це не майбутнє, а вже

поточна необхідність, яка визначає успішність держав у боротьбі з фінансовими загрозами глобального масштабу.

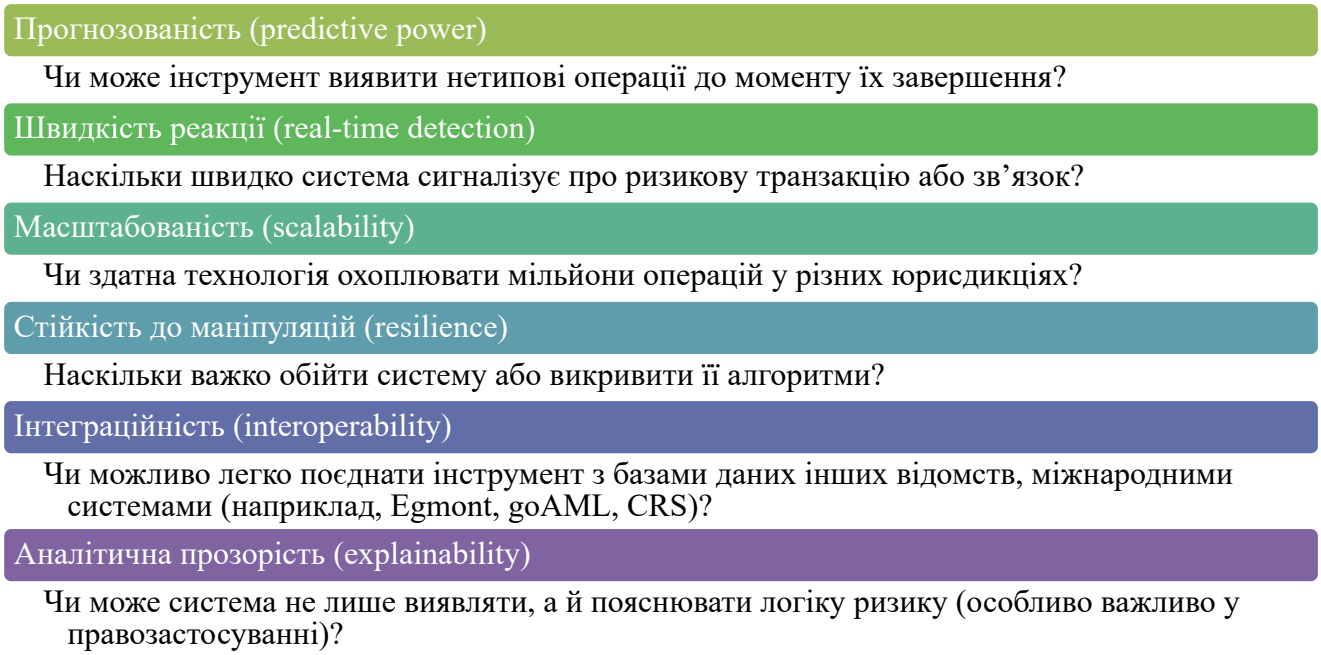

Рисунок 2.2 – Критерії ефективності інноваційних рішень у сфері фінансової безпеки

Джерело: [34]

У практичному вимірі ефективні інновації — це не "технологічний аксесуар", а центральний нервовий вузол фінансової системи, здатний замінити десятки аналітиків, виявити цифрові відбитки злочинної активності та мінімізувати людський фактор. Найуспішніші системи, такі як Palantir for AML, Chainalysis, SAS Visual Investigator, уже трансформують національні FIU з бюрократичних посередників у цифрові аналітичні платформи з ефектом превенції.

У сучасній боротьбі з фінансовими злочинами ключову роль починають відігравати аналітичні платформи на основі великих даних (Big Data) та інструменти штучного інтелекту (AI), здатні в реальному часі обробляти мільйони транзакцій, виявляти аномалії, будувати пов'язані графи та прогнозувати ризикову поведінку. Ці системи є критично важливими для національних фінансових розвідок (FIU), банків, регуляторів і митних органів, оскільки забезпечують перехід від реактивної до проактивної моделі контролю [35].

Застосування машинного навчання (ML) дозволяє не просто ідентифікувати стандартні підозрілі операції (наприклад, великі грошові перекази в офшори), а й виявляти складні нелінійні закономірності, які не очевидні для людського аналітика. Наприклад, система може виявити, що кілька на перший погляд непов'язаних компаній використовують однакові шаблони платежів із затримкою в 3 дні, що є типовим для багаторівневих схем «відкату» чи трансферного ціноутворення. У 2023 році Deutsche Bank повідомив, що завдяки впровадженню AI-модуля в платформу SAS AML виявив на 27% більше транзакцій із прихованим шахрайським потенціалом, ніж при ручному моніторингу.

Аналітичні платформи нового покоління у сфері протидії фінансовим злочинам демонструють принципово новий рівень ефективності завдяки інтеграції великих даних, машинного навчання та мережевого аналізу. Три з найбільш показових прикладів таких рішень — Palantir for AML, SAS Anti-Money Laundering та Chainalysis — ілюструють, як сучасна аналітика трансформує реагування держав і фінансових установ на складні транскордонні ризики.

Palantir for AML — це потужна американська платформа, яку застосовують фінансові регулятори США, Великої Британії та окремих країн ЄС. Її відмінністю є здатність поєднувати фінансову аналітику, геопросторові патерни та соціальні графи, що дозволяє виявляти неочевидні зв'язки між контрагентами та моделювати потенційні злочинні схеми. Наприклад, Європол використав Palantir під час розслідування справи про фінансування тероризму через формально легальні благодійні фонди в Бельгії. Завдяки автоматичному аналізу метаданих система ідентифікувала 11 підставних структур, базуючись лише на збігах номерів телефонів, поштових адрес і маршрутів транзакцій [36].

SAS Anti-Money Laundering є одним із найбільш визнаних інструментів для комерційного сектора, особливо в банківській сфері. Головною її перевагою вважається висока гнучкість налаштування правил моніторингу, можливість створення автоматичних профілів клієнтів за ризик-орієнтованим підходом (risk scoring), а також інтеграція модулів боротьби з шахрайством. У 2022 році Національний банк Польщі запровадив SAS як основу централізованої аналітичної

системи, яка охоплює більше 100 фінансових установ, забезпечуючи єдину модель оцінювання підозрілих операцій [37]. Chainalysis — це спеціалізована аналітична платформа для відстеження блокчейн-транзакцій. Її функціональність дозволяє аналізувати грошові потоки навіть через анонімізуючі сервіси (так звані mixer-гаманці). Ця система активно використовується урядовими структурами США, зокрема Міністерством фінансів (OFAC). Chainalysis була задіяна у виявленні майнінгових адрес, пов'язаних з іранськими та північнокорейськими структурами, які використовували криптовалюту для обходу міжнародних санкцій. Ефективність таких платформ має практично вимірюваний ефект [37]:

- підвищення точності виявлення ризиків на 30–70% порівняно з ручним аналізом;
- скорочення часу реакції з тижнів до хвилин, особливо в кіберінцидентах;
- здатність обробляти десятки мільйонів транзакцій одночасно в мультиюрисдикційному контексті;
- накопичення інституційної пам'яті — алгоритми навчаються на кожному кейсі, підвищуючи свою ефективність у виявленні нових або модифікованих форм шахрайства.

Таким чином, ці платформи не лише доповнюють функції фінансового нагляду, а стають стратегічними аналітичними центрами, які суттєво підвищують рівень фінансової безпеки як на національному, так і на міжнародному рівні.

Таблиця 2.4 Порівняння трьох провідних аналітичних платформ — Palantir for AML, SAS AML та Chainalysis

Платформа	Точність виявлення ризиків	Швидкість аналізу	Інтеграція з іншими системами	Типова сфера застосування
Palantir for AML	Висока (до 70%)	Секунди–хвилини	Висока (API + графові модулі)	Тероризм, офшори, транснаціональні схеми
SAS AML	Середньо-висока (~60%)	Хвилини–години	Гнучка (банківські платформи)	Банківський сектор, compliance
Chainalysis	Висока (70%+ у криптотранзакціях)	Миттєвий (у blockchain explorer)	Висока (використовується урядами, біржами)	Криптоаналіз, санкційний моніторинг

Джерело: [38]

У відповідь на стрімке зростання ринку криптовалют та децентралізованих фінансів (DeFi), з’явилися інноваційні рішення для аналізу блокчейн-транзакцій, відстеження криптоактивів і автоматизації контролю ризиків. Серед них — аналітика блокчейну (Chainalysis, Elliptic), смарт-контракти з вбудованими тригерами безпеки, KYT-платформи (Know Your Transaction), а також risk engines для DeFi-середовища. Вони дозволяють ідентифікувати підозрілі шаблони поведінки, миттєво реагувати на транзакції та навіть прогнозувати шахрайські схеми — без людського втручання (табл.2.5).

Таблиця 2.5 Цифрові технології контролю активів

Технологія	Основне призначення	Типова сфера застосування	Переваги
Blockchain analytics (Chainalysis, Elliptic)	Відстеження криптотранзакцій, пов’язаних із незаконною діяльністю	AML, санкційний моніторинг, крипторинки	Трасування монет, виявлення mixer-гаманців
Смарт-контракти з тригерами	Автоматична блокування/сповіщення при настанні фінансових подій	Протоколи DeFi, DAO, автоматизоване управління ризиком	Автоматизація дій без втручання людини
DeFi risk engines (Gauntlet, OpenZeppelin)	Моделювання ризику в децентралізованих протоколах	Регуляторна аналітика в Web3-середовищі	Прогнозування збоїв і шахрайства в DeFi
Транзакційні аналізатори (TRM Labs)	Оцінка походження та шляху транзакції в реальному часі	Слідчі органи, криптобіржі, фінансові розвідки	Миттєва реакція на підозрілі шаблони
KYT-системи (Know Your Transaction)	Моніторинг підозрілих транзакцій на основі шаблонів поведінки	Банки, біржі, платформи цифрових платежів	Динамічне оцінювання ризику в реальному часі

Джерело: [39]

У сучасній фінансовій екосистемі ідентифікація клієнтів (KYC) та транзакцій (KYT) трансформувалася в динамічну, автоматизовану систему моніторингу, де штучний інтелект, біометрія та децентралізовані рішення забезпечують як швидкість, так і глибину перевірки. Нові технології дають змогу не просто знати, хто клієнт, а як він поводиться в реальному часі, виявляючи відхилення ще до того, як настане порушення. Такі інструменти знижують витрати

банків, підвищують безпеку й відкривають шлях до прозорих DeFi-платформ (табл.2.6).

Таблиця 2.6 Інновації у сфері KYC, KYT та ідентифікації

Інновація	Призначення	Ключові переваги	Сфера використання
Електронна ідентифікація (eKYC)	Онлайн-верифікація особи на основі офіційних документів	Миттєва ідентифікація, зниження витрат на onboarding	Банки, неофіси, онлайн-фінанси
Біометричні системи автентифікації	Розпізнавання обличчя, відбитків, голосу для підтвердження дій	Підвищення безпеки, зменшення шахрайства	Платіжні системи, мобільні додатки, банкомати
KYT-системи (Know Your Transaction)	Моніторинг поведінки транзакцій, а не лише клієнта	Реакція в реальному часі на аномальні фінансові дії	Криптобіржі, аналітичні служби, банківські AML-системи
AI-based клієнтські профілі (risk scoring)	Аналіз клієнтської поведінки на основі великих даних	Персоналізований контроль ризиків і кредитоспроможності	Фінтех, страхові компанії, онлайн-кредитування
Децентралізовані цифрові ідентифікатори (DID)	Контроль доступу до фінансових послуг без розкриття персональних даних	Посилення конфіденційності, контроль над власними даними	Web3-платформи, DeFi, цифрові гаманці

Джерело: [40]

Інноваційні проєкти у сфері протидії фінансовим злочинам, що реалізуються на міжнародному рівні, демонструють перехід від декларативного контролю до технологічно орієнтованої, прогнозованої та адаптивної моделі фінансової безпеки. Особливо показовими є ініціативи на рівні наднаціональних інституцій ЄС, провідних фінтех-юрисдикцій (Сінгапур, ОАЕ, Естонія) та центральних банків, які інтегрують штучний інтелект, блокчейн-аналітику та автоматизовані KYC/KYT-механізми у щоденну фінансову практику.

Найамбітнішим проєктом європейського масштабу є створення AMLA (Anti-Money Laundering Authority) — першого наднаціонального органу, що забезпечуватиме централізований моніторинг підозрілих транзакцій у всіх 27 країнах ЄС. Запуск AMLA запланований на 2025 рік, штаб-квартира знаходитиметься у Франкфурті-на-Майні, а штат налічуватиме близько 250 експертів з аналізу даних, права та комплаєнсу. AMLA отримає повноваження [41]:

- безпосередньо контролювати найбільш ризикові банківські установи;
- запровадити єдиний цифровий реєстр підозрілих транзакцій в ЄС;

- застосовувати штучний інтелект для розпізнавання складних схем відмивання коштів (layering, trade-based laundering, synthetic identities).

За оцінками Єврокомісії, щорічні втрати від фінансових злочинів у ЄС перевищують €100–120 млрд, що еквівалентно 1% ВВП регіону. Очікується, що створення AMLA дозволить зменшити нелегальні капітальні потоки на 30–40% протягом перших трьох років функціонування.

Деякі малі, але технологічно розвинені держави вже стали еталонними кейсами впровадження інновацій у державне фінансове регулювання. Сінгапур у 2020 році запустив національну платформу COSMIC (Collaborative Sharing of ML/TF Information) — першу у світі систему обміну між банками не лише транзакційними, а й поведінковими та профільними даними про клієнтів. За офіційними даними MAS, після впровадження COSMIC [41]:

- середній час реагування на підозрілу транзакцію скоротився з 96 годин до 2 годин;
- кількість false-positive тривог зменшилася на 35%;
- понад 100 банків та платіжних платформ під'єднані до системи.

ОАЕ інтегрували AI-модулі в національні платіжні системи Central Bank of UAE, що дозволило у 2022 році [42]:

- виявити понад 5 300 підозрілих транзакцій на загальну суму $245 млн;
- заблокувати $115 млн у криптоактивах, більшість з яких використовувались через неавторизовані DeFi-платформи;
- створити єдиний цифровий досьє підозрюваних осіб, доступне правоохоронцям і банкам у режимі real-time.

Естонія запровадила першу в Європі національну блокчейн-реєстрацію віртуальних активів, синхронізовану з державною системою e-KYC та цифрового громадянства. За даними естонського FIU: кількість нелегальних платформ скоротилася на 76% за 3 роки; кожна ліцензована платформа проходить автоматизовану перевірку на зв'язок із офшорними юрисдикціями.

Системи аналітики центральних банків також поступово перетворюються на антифрод-центри, здатні виявляти аномальні патерни не лише у класичних

даних, а й у поведінці споживачів та корпоративних клієнтів. Банк Канади тестує аналітичну платформу, що поєднує транзакції, дані з маркетплейсів та open banking API, аби виявити "фінансові вібрації" — непрямі сигнали можливих маніпуляцій до моменту офіційного порушення [43]. Центральний банк Нігерії у межах розробки цифрової валюти eNaira впровадив AI-модуль для моніторингу криптопереказів, що імітує поведінку нелегальних бірж. ЄЦБ у 2024 році разом з AMLA запустить пан'європейську платформу звітності про великі транзакції (Cross-Border Transaction Reporting Hub) із обов'язковими алертами ("тригерними прапорами") для операцій понад €100 000 у зоні SEPA.

Глобальні кейси впровадження фінансових інновацій — це не просто набір пілотних рішень, а початок трансформації логіки державного фінансового контролю. Нове покоління платформ на основі AI, блокчейну, KYT і цифрових ідентифікаторів формує не лише нові інструменти, а й нові принципи: швидкість замість формальності, прогноз замість реакції, інтеграція замість фрагментації. І чим раніше країна інтегрується в ці процеси — тим вищий її шанс стати не жертвою фінансової злочинності, а її випереджувальним контргравцем.

2.3. Перспективи підвищення ефективності запобігання міжнародним фінансовим злочинам

Світова фінансова система сьогодні водночас перебуває на вершині технічного озброєння у боротьбі з фінансовими злочинами — і в глибокій кризі практичної результативності. З одного боку, держави і наднаціональні органи мають у розпорядженні потужні інструменти: від алгоритмічних платформ типу Palantir AML до міждержавних систем обміну типу CRS та Egmont. З іншого — щорічні втрати від фінансових злочинів оцінюються в понад $2 трлн, при цьому менше 1% "брудних грошей" вдається вилучити або заблокувати, за даними UNODC [44].

Упродовж останнього десятиліття система міжнародної протидії фінансовим злочинам зазнала суттєвих трансформацій — передусім у бік

цифровізації, підвищення координації та застосування інноваційних інструментів. Одним із ключових досягнень стала цифрова трансформація фінансових розвідувальних підрозділів (FIU): у розвинених країнах, зокрема у США (FinCEN), Франції (TRACFIN) та Сінгапурі (MAS), активно впроваджуються аналітичні системи на основі штучного інтелекту, машинного навчання та великих даних. Це дозволяє не лише фіксувати підозрілі транзакції, а й прогнозувати їх на основі поведінкових патернів.

Іншим важливим досягненням є розвиток міжнародної координації, що проявляється у поширенні багатосторонніх форматів — таких як рекомендації FATF, ініціативи CARIN, платформи Egmont Group та проєкти типу StAR (World Bank + UNODC). Вони не лише уніфікують терміни та підходи, а й забезпечують оперативний обмін інформацією між десятками юрисдикцій, скорочуючи час реагування на глобальні схеми. Не менш значущим є впровадження KYT-систем (Know Your Transaction) у банківському секторі — це новий клас інструментів, що дозволяє виявляти підозрілі операції в режимі реального часу, часто ще до їх завершення. Таким чином, акценти зміщуються з постфактум-реакції на превентивний ризик-контроль [45].

Крім того, зростає роль публічного та медійного тиску. Журналістські розслідування — зокрема FinCEN Files, Panama Papers, Paradise Papers та Luanda Leaks — стали каталізаторами для офіційних проваджень у більш ніж 60 країнах, а в низці випадків призвели до арештів активів, відставок посадовців та зміни національного законодавства. Попри ці досягнення, ефективність боротьби з фінансовими злочинами залишається низькою, і для цього існує кілька системних причин.

Перш за все, правова фрагментація глобального середовища: понад 200 країн мають різні кримінальні, процесуальні та фінансові норми. Це створює перешкоди для екстрадиції, ускладнює визнання доказів, а в багатьох випадках — повністю блокує транснаціональні розслідування. Такі прогалини системно використовуються злочинцями для розміщення коштів у "юрисдикційних дірах" [46].

Крім того, антикорупційні органи часто перебувають у залежності від політичних або бізнесових еліт. У країнах із перехідною економікою FIU часто не є незалежними й можуть блокувати справи проти політично значущих осіб (PEP), а керівництво змінюється за кулуарними домовленостями. Ще одна критична проблема — недофінансованість регуляторів: за даними Egmont Group (2023), лише 34% фінансових розвідок мають достатні ресурси для ведення повноцінної аналітичної роботи, обробки звітів та міжнародної взаємодії. Решта — технічно відстають, мають обмежений доступ до баз даних і використовують застаріле програмне забезпечення [46].

Окремий виклик — технологічна перевага злочинців у сфері криптовалют і децентралізованих фінансів (DeFi). За даними Chainalysis, у 2023 році частка нелегального обігу через DeFi-протоколи зросла на 63%, особливо в країнах, де регулятори не мають повноважень щодо цифрових активів або не встигають за швидкістю інновацій. Нарешті, значна частина світу — Глобальний Південь — фактично залишається "сліпою зоною" у глобальній фінансовій архітектурі. Близько 70% виявлених транснаціональних схем відмивання коштів зосереджені в 20% юрисдикцій, тоді як у більшості країн Африки, Південно-Східної Азії та Латинської Америки немає ефективного фінансового моніторингу, або він діє лише формально.

Таким чином, прогрес є, але він нерівномірний, крихкий і вразливий. Для реальної протидії фінансовим злочинам недостатньо технологій — необхідна системна політична воля, правова уніфікація та незалежність інституцій, без чого навіть найкращі платформи та протоколи залишаються лише декларацією.

Таблиця 2.7 Сильні сторони, вузькі місця та критичні бар’єри протидії фінансовим злочинам

Показник / Критерій	Досягнення	Наявні прогалини / бар’єри	Приклади країн
Аналітичні системи в FIU	AI-аналітика, обробка великих даних, інтерфейси з банками	Недоступність API, слабкий IT-парк, відсутність кейсів навчання	США, Франція vs. Україна, Філіппіни

Правова гармонізація	Загальні стандарти FATF, AMLD, CRS	Різне визначення термінів, невизнання юрисдикцій, конфлікти суверенітету	ЄС vs. ОАЕ, Росія, Туреччина
Політична незалежність FIU	Частково забезпечена у G7	Політичне втручання, замовне блокування справ, відставки керівників	Канада vs. Україна, Казахстан, Мексика
Ефективність обміну даними	Egmont, goAML, FIU.net	Запізнення відповідей, обмеження за національним законодавством	Естонія, Литва vs. Італія, Індія
Контроль криптоактивів	Створення публічних реєстрів, Chainalysis, FATF Guidance on VASP	Анонімні токени, mixer-гаманці, обхід ліцензування	Сінгапур, Німеччина vs. ОАЕ, Ліван, Бразилія
Санкційна спроможність і впровадження рішень	Sanctions Tracker, публічні чорні списки	Відсутність санкційної відповідальності, політичне "прикриття"	США, ЄС vs. Китай, Африка пд. Сахари
Судовий супровід фінансових розслідувань	Частина справ доходить до конфіскації	Менше 1% справ завершуються поверненням коштів	Велика Британія vs. більшість країн Азії та Лат. Америки

Джерело: [46]

Міжнародна система протидії фінансовим злочинам перебуває у парадоксі: технологічна готовність зростає, але системна результативність залишається критично низькою. Без реформи судової та політичної відповідальності, уніфікації правових процедур та виведення FIU з-під впливу державних еліт, жодна навіть найкраща платформа не дасть реального ефекту.

У сучасних умовах, коли фінансові потоки дедалі більше втрачають фізичну прив’язку до території, а злочинці можуть розміщувати активи у віртуальних екосистемах, ефективна протидія фінансовим злочинам неможлива без комплексної модернізації нормативно-правової бази. Йдеться не лише про оновлення термінології чи окремих положень, а про створення нового правового каркасу, здатного реагувати на ризики глобалізованого цифрового ринку [46].

Одним із першочергових напрямів реформування є гармонізація фінансового, кримінального та процесуального законодавства між державами. У 2020-х роках світ стикається з парадоксом: міжнародні злочинні схеми дедалі більше інтегровані, тоді як національні правові системи залишаються фрагментованими. Наприклад, поняття «бенефіціарна власність» або «електронний

підпис» можуть мати різне правове значення навіть у країнах ЄС. Це створює правові колізії, ускладнює екстрадицію, унеможливлює спільне слідство або блокування активів у реальному часі. Ключовими інструментами гармонізації є [47]:

- Уніфіковані підходи FATF (рекомендації та типології);
- AML-директиви Європейського Союзу (4-та, 5-та, 6-та AMLD), які змушують держави оновлювати свої закони згідно з загальноєвропейською логікою контролю;
- Міжнародні моделі обміну — такі як CRS (Common Reporting Standard) від OECD, що дозволяє автоматичне зіставлення фінансових даних між понад 110 юрисдикціями.

На думку експертів Світового банку, неузгодженість законодавства залишається одним із головних чинників неефективності глобальної фінансової безпеки. Понад 40% країн не мають дієвих договорів про взаємну правову допомогу або їх положення надто вузькі.

Другий ключовий вектор удосконалення — створення правового поля для контролю цифрових активів, DeFi-сервісів та транснаціональних криптовалютних транзакцій. Більшість сучасних законів залишаються прив’язаними до фізичної юрисдикції, у той час як цифрові платформи — ні. Злочинці можуть обирати криптобіржі без ліцензії, використовувати mixer-гаманці або конвертувати активи у NFT — усе це відбувається поза межами звичних правових структур [47].

Згідно з даними Chainalysis (2023), понад $23,8 млрд було відмито через криптовалюту упродовж останніх трьох років, із них майже половина — через DeFi-платформи без юридичного резидентства. Це свідчить про критичну необхідність створення глобального режиму регулювання віртуальних активів. Ключові кроки, що вже впроваджуються [47]:

- Рамка FATF щодо VASP (Virtual Asset Service Providers) — встановлення мінімальних вимог до ліцензування, моніторингу та бенефіціарної звітності.
- Регламент MiCA (Markets in Crypto-Assets) в ЄС — комплексне регулювання обігу криптовалют, стейблкоїнів та токенізованих активів.

• Програми цифрової ідентифікації та автоматизованої звітності (KYT/Travel Rule) — нове покоління механізмів контролю за транзакціями у блокчейн-середовищі.

Однак велика частина світу досі не має чітко визначених правил гри. У понад 60 країнах немає закону про криптовалюту, а в 25 — її використання взагалі не регулюється жодним документом.

Ефективна боротьба з фінансовими злочинами у XXI столітті залежить не лише від інституцій або технологій, а й від здатності правових систем адаптуватися до нової реальності без меж і посередників. Гармонізація законодавства та регулювання цифрових активів — це не лише питання техніки, а фундаментальний чинник легітимності, довіри та виживання фінансових інституцій у світі, що стрімко змінюється. Без цих змін ризик залишається незмінним, а злочинець — завжди на крок попереду.

У контексті зростаючої складності транснаціональних фінансових схем, що дедалі частіше реалізуються через цифрові активи, DeFi-протоколи та офшорні юрисдикції, посилення інституційної координації між фінансовими, слідчими та судовими органами набуває вирішального значення. Саме синхронізовані дії на міждержавному рівні — це не просто бажана практика, а необхідна передумова для ефективної протидії криміналізованим грошовим потокам.

Таблиця 2.8 Інструменти міжнародної інституційної координації

Механізм координації / інструмент	Функціональне призначення	Країни-лідери / приклади впровадження	Ключова перевага
FIU з розширеними повноваженнями (наприклад, FinCEN, TRACFIN)	Аналітика + ініціація кримінальних проваджень, блокування активів	США, Франція, Сінгапур, Литва	Зменшення залежності від прокуратури, швидка реакція
Спільні розслідувальні групи (Joint Investigation Teams, JITs)	Координація дій поліції, митниці, фінансових інспекцій у кількох країнах	Нідерланди–Німеччина–Італія (боротьба з відмиванням через логістику)	Синхронізоване затримання активів, свідків і даних
Платформа FIU.net (EU)	Європейська мережа обміну підозрілою інформацією між FIU	Усі країни ЄС, особливо Бельгія, Іспанія, Словенія	Реакція в межах 24 годин, узгоджені протоколи

Egmont Secure Web (ESW)	Захищений обмін запитами/відповідями між 170+ FIU	Egmont Group (більше 170 країн)	Миттєвий обмін і верифікація транзакцій
Cross-Border Reporting Hub (пілот ЄЦБ + AMLA)	Автоматизований моніторинг транскордонних транзакцій >€100,000	Єврозона, запуск у 2024–2025 роках	Уніфіковані стандарти та real-time аналіз великих операцій

Джерело: [47]

У низці країн спостерігається чіткий зсув від пасивної аналітичної моделі до проактивної операційної участі FIU (Financial Intelligence Units) у кримінальних розслідуваннях. Наприклад, FinCEN (США), TRACFIN (Франція) та MAS (Сінгапур) мають повноваження не лише подавати аналітичні звіти, але й ініціювати арешт активів, блокувати рахунки та направляти справи безпосередньо до прокуратури. Така модель скорочує часові лаги між аналітикою і реагуванням, зменшуючи залежність від політично впливових ланок.

Водночас у багатьох країнах — зокрема в Україні, Казахстані, Мексиці — FIU досі залишаються допоміжними аналітичними структурами без реальних механізмів примусового впливу, що знижує їхню роль у ланцюгу реагування [48].

Окремим пріоритетом стає створення єдиних, захищених платформ для обміну фінансовою інформацією в режимі реального часу. Платформи нового покоління, такі як FIU.net у межах ЄС або Egmont Secure Web, дозволяють миттєво передавати структуровані досьє, обмінюватися шаблонами ризиків, запитами про активи чи транзакції та формувати спільні розслідувальні файли. Більш того, у 2024 році планується запуск Cross-Border Reporting Hub — пілотного проєкту ЄЦБ та AMLA, який дозволить уніфіковано відслідковувати всі транзакції понад €100 000 у зоні SEPA, з автоматичними "прапорами" ризику та доступом для національних FIU. Такі ініціативи створюють екосистему транскордонної відповідальності, де жодна транзакція не лишається поза увагою через юрисдикційні прогалини [48].

Таким чином, інституційна взаємодія еволюціонує від обміну "після факту" до попереджувального партнерства, де аналітика, кримінальне переслідування та міжнародна співпраця зливаються в єдину, інтегровану екосистему безпеки. Але для повноцінного ефекту ці механізми потребують не лише технічної реалізації, а

й політичної підтримки, правової гармонізації та незалежності від національного тиску.

У глобалізованому фінансовому середовищі, де грошові потоки долають національні кордони в лічені секунди, ефективність боротьби з фінансовими злочинами визначається не лише внутрішніми можливостями окремих держав, а й рівнем міжінституційної та міждержавної взаємодії. Особливої актуальності це набуває у світлі зростання обсягів нелегального переміщення капіталу, а також з огляду на зростання ролі неконвенційних каналів обігу активів — таких як цифрові валюти, стейблкоїни, приватні біржі тощо.

Один із провідних напрямів реформування інституційного середовища полягає у наданні фінансовим розвідкам розширених повноважень, які дозволяють не лише виконувати функції збору та аналітичної обробки інформації, а й ініціювати правозастосовні процедури, блокувати активи, вимагати примусового доступу до фінансових даних. У сучасній практиці такі функції частково виконують FinCEN (США), TRACFIN (Франція), а також FIU у Сінгапурі, Естонії та Нідерландах [48]. Це дозволяє скоротити часові втрати на міжвідомчу передачу інформації та знижує ризик втрати доказової бази через юридичні проміжки. Підвищення функціональної автономії FIU є також запорукою їх незалежності від політичного впливу, що особливо актуально для країн з перехідною економікою та нестабільною системою публічного адміністрування.

Системна координація дозволяє переходити від реактивного до превентивного режиму протидії. Синхронізовані дії FIU, податкових служб, правоохоронних органів та центральних банків створюють ефект інституційної синергії, коли кожен елемент структури виконує не ізольовану, а доповнювальну функцію. Це особливо ефективно у справах, що стосуються транснаціонального шахрайства, подвійного резидентства, фіктивних тендерів, а також фінансування терористичної діяльності [48]. Таким чином, інституційна взаємодія є не допоміжною умовою, а структурною необхідністю, без якої будь-яка антикримінальна ініціатива залишається фрагментарною, непослідовною та вразливою перед глобальними викликами фінансової безпеки.

Ні найкраще законодавство, ні найсучасніші аналітичні платформи не будуть результативними без дієвої політичної волі та сформованої фінансової культури суспільства. На практиці ефективність боротьби з відмиванням коштів, корупцією та іншими «білокомірцевими» злочинами залежить не лише від технічної спроможності держави, а й від її готовності діяти послідовно, відкрито і публічно — навіть у випадках, що стосуються власних еліт.

Прозорість не зводиться до оприлюднення звітів чи публікації бюджетів. Ідеться про відкритість алгоритмів ухвалення рішень, доступ громадськості до контрактної інформації, розкриття бенефіціарних власників і прозоре електронне декларування статків чиновників. Як показує досвід країн Балтії та Північної Європи, саме поєднання систем електронного управління, громадського контролю та ефективних антикорупційних структур дозволяє знизити толерантність до зловживань на всіх рівнях. У країнах із низьким рівнем прозорості навпаки — антикримінальні інститути часто використовуються вибірково, у політичних цілях, що підриває довіру до правозастосування.

Фінансова злочинність рідко сприймається суспільством як безпосередня загроза. Її образ абстрактний, а вплив — непрямий. Водночас досвід розвинених демократій свідчить: лише нульова суспільна толерантність до будь-якої форми зловживання бюджетними чи корпоративними ресурсами здатна створити середовище, в якому злочин стає не лише незаконним, а й соціально неприйнятним. Це передбачає [49]:

- публічне реагування на виявлені порушення без затягувань і “покривання”;
- притягнення до відповідальності не лише «виконавців», а й бенефіціарів схем;
- медійну прозорість та постійний освітній дискурс про шкоду «білокомірцевої» злочинності.

У Швеції, наприклад, понад 80% громадян підтримують кримінальну відповідальність за невиконання обов’язку повідомити про корупційну спробу. У Німеччині понад 70% вважають фінансові махінації в держсекторі «злочином проти суспільного договору».

Таблиця 2.9 Індексна оцінка політичної волі та фінансової культури в глобальному контексті

Країна	Індекс сприйняття корупції (CPI, 2023, Transparency Int.)	Open Government Index (World Justice Project, 2023)	Соціальна нетерпимість до корупції (% громадян, які вважають її неприпустимою, OECD/UNDP)
Швеція	83	0.81	86
Німеччина	79	0.79	71
Сінгапур	83	0.74	75
Естонія	76	0.77	69
Польща	55	0.65	62
Україна	36	0.5	38
Італія	56	0.61	49
Індія	40	0.53	41
Бразилія	38	0.49	35
Нігерія	25	0.43	28

Джерело: [49]

Без послідовної політичної волі та сформованої громадянської нетерпимості до маніпуляцій із фінансами, інституційна реформа залишається незавершеною. Прозорість і фінансова етика мають стати не винятком, а повсякденним стандартом публічного життя, без якого жодна платформа, закон чи розслідування не забезпечать довготривалого ефекту. Інакше кажучи, боротьба з фінансовими злочинами — це не лише справа держави, а й зрілої спільноти, що знає ціну кожному зловживанню.

ВИСНОВКИ

1. У процесі дослідження було встановлено, що міжнародні фінансові злочини являють собою систематичне порушення фінансового порядку з транскордонним елементом, що поєднує економічну вигоду з приховуванням, шахрайством або порушенням норм валютного, податкового чи банківського законодавства. Їхні ключові ознаки — транснаціональний характер, використання складних фінансових інфраструктур і високий рівень латентності. Класифікація охоплює відмивання коштів, фінансування тероризму, податкові махінації, маніпуляції з цінними паперами, корупцію та злочини з використанням цифрових активів. Це дозволяє структурувати правове реагування та аналітичне спостереження з урахуванням конкретних ризиків.

2. Аналіз показав, що сучасні злочинці активно використовують офшорні юрисдикції, shell-компанії, трастові структури, кореспондентські рахунки, криптовалютні платформи, мистецтво, дорогоцінні метали та інші способи маскування походження коштів. Технологічна складність схем зросла: злочинці часто комбінують законні транзакції з незаконними у рамках одного ланцюга, що ускладнює виявлення. Високий рівень анонімності у DeFi, а також використання SWIFT, SEPA чи Hawala без належного контролю створює серйозні виклики для регуляторів. Стало очевидним, що традиційні методи боротьби більше не відповідають рівню адаптивності сучасних злочинних структур.

3. Було встановлено, що існує значний масив міжнародно-правових актів — Конвенція ООН проти транснаціональної організованої злочинності, UNCAC, директиви ЄС (AMLD), рекомендації FATF, — які створюють основу глобального реагування. Водночас правова фрагментація, відмінність у визначеннях, процедурах, юрисдикціях та нерівний рівень імплементації стандартів (особливо в країнах Глобального Півдня) послаблюють ефективність глобальної системи. Інституції, такі як FATF, Egmont Group, UNODC, Європол, Інтерпол, відіграють координаційну роль, проте потребують подальшої інтеграції цифрових інструментів та правового унормування транскордонної юрисдикції.

4. Інституційна складова є критично важливою для ефективної протидії: національні органи фінансового моніторингу, центральні банки, правоохоронні структури, антикорупційні агенції та судові органи повинні діяти у взаємозв'язку. Серед кращих практик — розширення повноважень FIU, створення спільних міждержавних слідчих груп (JITs), інтеграція у платформи FIU.net, ESW, AMLA-Hub. Проблемами залишаються політична залежність, нестача ресурсів, правові обмеження в обміні інформацією. Без інституційної синергії технічні та нормативні досягнення залишаються малоефективними.

5. Було доведено, що штучний інтелект, big data-аналітика, блокчейн-моніторинг, автоматизовані KYT-системи та децентралізовані цифрові ідентифікатори стають новими центрами сили у боротьбі з фінансовою злочинністю. Платформи типу Palantir, Chainalysis, SAS AML, TRM Labs демонструють високу ефективність у реальному виявленні підозрілих транзакцій. Проблемою залишається недоступність таких інструментів для багатьох країн, складність впровадження у юридично нестабільних системах та брак фахівців. Проте ці технології вже сьогодні формують парадигму попереджувального контролю, а не лише ретроспективного реагування.

6. Глобальні тенденції вказують на необхідність ревізії функціональної логіки антикримінальної архітектури: це передбачає не лише покращення технічних засобів, але й уніфікацію правових процедур, зміцнення незалежності інституцій, формування політичної волі та нульової толерантності до «білокомірцевої» злочинності. Особливої ваги набуває розвиток транскордонних аналітичних платформ, інтеграція цифрових валют у регуляторне поле та масова цифрова просвіта населення. Без цих умов, фінансова злочинність залишатиметься хронічною вразливістю глобальної економіки.

Крім інституційних факторів, було підкреслено критичне значення політичної волі, прозорості державних інституцій і формування фінансової культури з нульовою толерантністю до «білокомірцевої» злочинності. Саме суспільна підтримка, поєднана з технологічною спроможністю та нормативною узгодженістю, створює фундаментальні умови для сталого зниження рівня

фінансових злочинів у глобальному вимірі. Отже, ефективна боротьба з міжнародними фінансовими злочинами можлива лише за умови міждисциплінарного підходу — на перетині права, економіки, кібербезпеки та політики. Такий підхід передбачає не лише реагування на злочини, що вже відбулися, а й випереджувальне формування стійкої та адаптивної системи фінансової безпеки, що відповідає викликам XXI століття.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Basel Institute on Governance. (2020). *Typologies of financial crime and their convergence*. Retrieved from https://www.baselgovernance.org

2. Базилевич, В. Д. (2018). *Фінансова безпека: теорія, методологія, практика*. Київ: Знання. Сохацька, І. Б., & Лісовська, Л. С. (2021). *Фінансові злочини: сутність, класифікація та механізми протидії*. Науковий вісник Ужгородського національного університету. Серія: Право, (68), 179–183.

3. FATF. (2023). *Money Laundering and Terrorist Financing – Typologies and Trends*. Paris: FATF-GAFI. Retrieved from https://www.fatf-gafi.org

4. UNODC. (2020). *Combating Financial Crimes – Global Report*. United Nations Office on Drugs and Crime. Retrieved from https://www.unodc.org

5. European Commission. (2021). *Directive (EU) 2018/1673 on combating money laundering by criminal law*. Official Journal of the European Union.

6. FATF. (2023). International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations. Paris: FATF.

7. International Consortium of Investigative Journalists (ICIJ). (2016). Panama Papers Database. Retrieved from https://offshoreleaks.icij.org

8. ICIJ. (2021). Pandora Papers. Retrieved from https://www.icij.org/investigations/pandora-papers/

9. OECD. (2021). *Addressing the Tax Challenges of the Digital Economy: Global Minimum Tax Agreement*. Retrieved from https://www.oecd.org/tax/beps

10. IMF. (2022). *Financial Integrity and the Role of Correspondent Banking*. Retrieved from https://www.imf.org

11. Europol. (2022). *Financial and Economic Crime Threat Assessment*. Retrieved from https://www.europol.europa.eu

12. Interpol. (2021). *Hawala and Informal Value Transfer Systems: Global Impact Report*. Retrieved from https://www.interpol.int

13. World Bank. (2022). *Illicit Financial Flows and Asset Recovery*. Retrieved from https://www.worldbank.org

14. Chainalysis. (2024). *Crypto Crime Report*. Retrieved from https://www.chainalysis.com

15. UNODC. (2022). *Darknet and Cryptocurrency Crime Trends*. Retrieved from https://www.unodc.org

16. CipherTrace. (2023). *2023 Cryptocurrency Crime and Fraud Report*. Retrieved from https://www.ciphertrace.com

17. Transparency International. (2022). *Corruption in Infrastructure Projects*. Retrieved from https://www.transparency.org

18. Chatham House. (2022). *Humanitarian Aid and the Risk of Abuse*. Retrieved from https://www.chathamhouse.org

19. United Nations. (2005). *United Nations Convention against Corruption (UNCAC)*. Retrieved from https://www.unodc.org/unodc/en/corruption/uncac.html

20. European Banking Authority (EBA). (2020). *Report on AML/CFT efforts across the EU*. Retrieved from https://www.eba.europa.eu

21. FATF. (2023). *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations*. Paris: FATF. Retrieved from https://www.fatf-gafi.org

22. Egmont Group. (2023). *About FIUs and Information Exchange*. Retrieved from https://egmontgroup.org

23. FinCEN. (2021). *Corporate Transparency Act and Beneficial Ownership Information*. Retrieved from https://www.fincen.gov

24. CARIN. (2023). *About the Camden Asset Recovery Inter-Agency Network*. Retrieved from https://www.carin.network

25. World Bank. (2022). *Financial Sector Assessment: A Handbook*. Retrieved from https://www.worldbank.org

26. IMF. (2022). *Institutional Arrangements for Financial Integrity*. Retrieved from https://www.imf.org

27. Europol. (2023). *Financial and Economic Crime Centre (EFECC)*. Retrieved from https://www.europol.europa.eu

28. Financial Times. (2019). *Inside the Danske Bank Scandal*. Retrieved from https://www.ft.com

29. European Central Bank. (2023). *Enhanced Due Diligence for Cross-Border Banking*. Retrieved from https://www.ecb.europa.eu

30. BuzzFeed News & ICIJ. (2020). *FinCEN Files Investigation*. Retrieved from https://www.icij.org/investigations/fincen-files/

31. Mediapart. (2021). *Le rôle de TRACFIN dans les affaires politico-financières*. Retrieved from https://www.mediapart.fr

32. Transparency International Ukraine. (2022). *Оцінка ефективності фінмоніторингу в Україні*. Retrieved from https://ti-ukraine.org

33. Deutsche Bank. (2023). *Annual Financial Crime Report*. Deutsche Bank. Retrieved from https://www.db.com

34. European Commission. (2023). *Proposal for a Regulation establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism*. European Commission. Retrieved from https://ec.europa.eu

35. MAS Singapore. (2022). *Overview of Project COSMIC*. Monetary Authority of Singapore. Retrieved from https://www.mas.gov.sg

36. SAS Institute. (2022). *SAS Anti-Money Laundering for Banking*. SAS Insights. Retrieved from https://www.sas.com

37. TRM Labs. (2023). *Blockchain Intelligence Platform Overview*. TRM Labs. Retrieved from https://www.trmlabs.com

38. Palantir Technologies. (2023). *Palantir for Anti-Money Laundering: Technical Overview*. Palantir. Retrieved from https://www.palantir.com

39. OpenZeppelin. (2023). *DeFi Risk Frameworks for Governance*. OpenZeppelin. Retrieved from https://www.openzeppelin.com

40. Basel Institute on Governance. (2022). *AML Index Report: Assessing countries' risk of money laundering and terrorist financing*. https://baselgovernance.org/aml-index

41. Zoromé, A. (2007). *Concept of Offshore Financial Centers: In Search of an Operational Definition*. International Monetary

Fund. https://www.imf.org/en/Publications/WP/Issues/2016/12/31/Concept-of-Offshore-Financial-Centers-In-Search-of-an-Operational-Definition-20420

42. European Banking Authority. (2023). *Guidelines on risk-based supervision of anti-money laundering and countering the financing of terrorism*. https://www.eba.europa.eu

43. Böhme, R., Christin, N., Edelman, B., & Moore, T. (2015). Bitcoin: Economics, technology, and governance. *Journal of Economic Perspectives, 29*(2), 213–238. https://doi.org/10.1257/jep.29.2.213

44. Reuter, P. (2017). *Chasing Dirty Money: The Fight Against Money Laundering*. Peterson Institute for International Economics.

45. Arnone, M., & Borlini, L. S. (2010). *International Anti-Money Laundering Programs: Empirical Assessment and Issues in Criminal Regulation*. *Journal of Money Laundering Control, 13*(3), 226–271.

46. Financial Transparency Coalition. (2022). *Illicit Financial Flows and the Global South*. https://financialtransparency.org

47. Global Financial Integrity. (2021). *Illicit Financial Flows to and from Developing Countries: 2008–2019*. https://gfintegrity.org

48. International Monetary Fund. (2023). *The Role of Technology in Strengthening Anti-Money Laundering Frameworks*. IMF Policy Paper. https://www.imf.org

49. Levi, M., & Reuter, P. (2006). *Money Laundering*. *Crime and Justice, 34*, 289–375. https://doi.org/10.1086/501509

ДОДАТКИ

ДОДАТОК А

ОГЛЯД СПЕЦІАЛЬНОЇ ЗАРУБІЖНОЇ ЛІТЕР АТУРИ

Money Laundering: The Economics of Regulation (1995) – Donato Masciandaro

This article analyzes the cost-benefit paradox of anti-money laundering (AML) regulation. The author argues that although financial regulation aims to reduce illicit financial flows, excessive enforcement may distort market dynamics and increase compliance costs. Masciandaro was among the first to propose an economic approach to understanding laundering patterns and regulatory efficiency, thus laying the groundwork for a functionalist understanding of compliance burdens.

The Money Laundry: Regulating Criminal Finance in the Global Economy (2011) – Jason Sharman

Sharman's book challenges the conventional wisdom of the global AML regime. He questions whether global institutions like FATF actually reduce financial crime or simply expand bureaucratic compliance. Drawing on empirical cases, he shows how offshore secrecy jurisdictions and weakly regulated financial institutions undermine global enforcement efforts. The work is frequently cited for its critical perspective on the limits of international cooperation.

Anti-Money Laundering Regulations: A Burden on Financial Institutions (1994) – David E. Alford

Alford presents a legal critique of AML measures from the viewpoint of U.S. financial institutions. He argues that banks are often compelled to act as quasi-law enforcement agents without adequate procedural protections or institutional support. This paper contributes to ongoing debates about the proportionality and legality of mandatory reporting mechanisms under the Bank Secrecy Act and beyond.

The Anti-Money Laundering Risk Assessment: A Probabilistic Approach (2019) – Halliday, Levi, and Reuter

This study proposes a quantitative model for assessing AML risks using probabilistic reasoning and scenario analysis. The authors criticize the often arbitrary assignment of "high-risk" statuses and call for data-driven frameworks. Their work is particularly relevant in policy circles exploring outcome-based AML supervision rather than rule-based checklists.

Fintech and Anti-Money Laundering Regulation (2023) – Nadia A. Roide

Roide investigates how regulatory hierarchies adapt to emerging fintech models. The paper explores gaps in AML compliance among crypto exchanges, neobanks, and peer-to-peer platforms, proposing international regulatory convergence. The article is notable for proposing a multi-tiered risk-based approach to integrating technological innovation with regulatory frameworks.

Network Analytics for Anti-Money Laundering (2024) – Deprez et al.

This systematic review evaluates the application of network science to AML efforts. The authors assess over 50 models using graph theory, link prediction, and anomaly detection, demonstrating how criminal money trails can be reconstructed using transaction networks. This paper is at the forefront of computational approaches to financial crime.

Gold Laundering: The Dirty Secrets of the Gold Trade (2019) – Mark Pieth

Pieth exposes how gold trading is used to clean illicit funds. The book offers case studies across Switzerland, UAE, and sub-Saharan Africa. He argues that gold is an underregulated sector with high laundering risk, and calls for integration of precious metals into the global AML regime.

Realistic Synthetic Financial Transactions for AML Models (2023) – Altman et al.

The authors introduce a synthetic dataset generator based on real-world financial behavior to train and test machine learning models for AML. This technical paper helps solve the issue of data unavailability due to confidentiality and is widely cited in data science applications within the compliance industry.

Literature Review of International AML Research: A Scientometric Perspective (2014) – Mei, Ye, & Gao

This paper reviews over 300 articles on AML, identifying major clusters of research and thematic trends. It traces the shift from legal to data-driven approaches and maps out influential authors and institutions. It is a valuable meta-analysis for understanding the evolution of the field.

Money Laundering and the Financing of Terrorism: An Overview (2005) – Jean-François Thony

This IMF publication provides a foundational overview of global standards against financial crime, emphasizing the intersection between money laundering and terrorist financing. Thony outlines the evolution of international law in the early 2000s, including the influence of FATF recommendations and post-9/11 legal changes.

The Puzzle of Money Laundering: A Literature Review of Regulations and Effectiveness (2023) – Fadli, R. & Widodo, T.

This study investigates the effectiveness of AML regulations globally, highlighting the challenges in harmonizing international standards and the varying degrees of enforcement across jurisdictions. The authors emphasize the need for a more cohesive global framework to combat money laundering effectively.

Anti-Money Laundering: The World's Least Effective Policy Experiment Together, We Can Fix It (2020) – Ronald F. Pol

Pol critically examines the global AML regime, arguing that despite extensive regulations, the actual impact on reducing financial crime is minimal. He suggests that the current system is more about compliance than effectiveness, calling for a fundamental reevaluation of AML strategies.

A Systematic Review of Anti-Money Laundering Systems Literature: Exploring the Efficacy of Machine Learning and Deep Learning Integration (2023) – Alzahrani, S. & Alabdulatif, A.

This paper reviews the integration of machine learning and deep learning techniques in AML systems, assessing their effectiveness in detecting suspicious activities. The authors find that while these technologies offer promise, challenges remain in data quality and algorithm transparency.

Fighting Money Laundering with Statistics and Machine Learning (2022) – Jensen, R. & Iosifidis, A.

Jensen and Iosifidis explore the application of statistical and machine learning methods in AML, proposing a unified terminology and framework for client risk profiling and suspicious behavior detection. They highlight the potential of these techniques while acknowledging the need for more public datasets.

Deep Learning Approaches for Anti-Money Laundering on Mobile Transactions: Review, Framework, and Directions (2025) – Fan, J. et al.

This comprehensive review addresses the challenges of applying deep learning to AML in mobile transactions, proposing a novel framework that integrates machine learning techniques with account profiling to enhance fraud detection under data constraints.

Advances in Continual Graph Learning for Anti-Money Laundering Systems: A Comprehensive Review (2025) – Deprez, B. et al.

The authors evaluate state-of-the-art continual graph learning approaches for AML applications, categorizing methods and providing experimental evaluations that demonstrate improved model adaptability and robustness in detecting evolving fraud patterns.

Network Analytics for Anti-Money Laundering: A Systematic Literature Review and Experimental Evaluation (2024) – Deprez, B. et al.

This paper presents a taxonomy of network analytics approaches in AML, offering a comprehensive experimental framework to evaluate and compare the performance of prominent methods, concluding that network analytics enhances the predictive power of AML models.

Money Laundering as a Transnational Business Phenomenon (2021) – Levi, M. & Reuter, P.

Levi and Reuter analyze money laundering as a transnational issue, discussing its implications for global governance and the effectiveness of current regulatory measures. They advocate for more coordinated international efforts to address the complexities of financial crimes.

The Anti-Money Laundering Risk Assessment: A Probabilistic Approach (2023) – Halliday, T.C., Levi, M., & Reuter, P.

This study proposes a probabilistic model for AML risk assessment, emphasizing the need for data-driven frameworks over arbitrary risk assignments, and highlighting the importance of outcome-based supervision.

Money Laundering: A Review of Literature and Future Research (2024) – Singh, R. & Jain, M.

Singh and Jain provide a comprehensive review of money laundering literature, identifying gaps in current research and suggesting areas for future study, particularly in the context of emerging technologies and their impact on AML efforts.

ДОДАТОК Б

SUMMARY

The bachelor's thesis entitled "International Financial Crimes: Types and Prevention Measures" consists of two chapters, each focusing on critical aspects of combating cross-border illicit financial activity. The topic was selected due to the increasing relevance of financial crimes in the context of globalization, digitalization, and shifting geopolitical dynamics.

The first chapter explores the theoretical foundations of international financial crimes, including their definitions, distinguishing features, and typologies. Special attention is paid to crimes such as money laundering, terrorism financing, tax evasion, and illegal use of cryptocurrencies. The chapter also examines mechanisms used to commit such crimes — including offshore jurisdictions, shell companies, manipulations in payment systems, and exploitation of high-value assets such as real estate and fine art. The legal approaches of major international conventions (UN, FATF, EU AML directives) and national systems are reviewed and compared, supported by statistical data and classification tables.

The second chapter focuses on institutional and technological tools of prevention. It assesses the role of international and national institutions (e.g., FATF, Egmont Group, Europol, FinCEN) and evaluates the effectiveness of cross-border coordination. Special attention is given to the implementation of innovative digital solutions such as AI-driven risk monitoring, blockchain analysis, real-time KYC/KYT systems, and predictive analytics in transaction surveillance. The chapter concludes with an analysis of current weaknesses, systemic gaps, and future directions for improving global anti-financial crime frameworks.

Keywords: international finance, financial crime, money laundering, AML, institutional coordination, digital compliance, blockchain analytics.

ДОДАТОК В

Операції з нерухомістю, мистецтвом і дорогоцінними металами як механізм маскування злочинного походження капіталу

Одним із ключових механізмів легалізації злочинних доходів у міжнародному середовищі є інвестування в активи з високою вартістю та низьким рівнем прозорості. До таких активів належать об’єкти елітної нерухомості, витвори мистецтва та дорогоцінні метали. Спільною рисою цих секторів є слабкий контроль з боку фінансових регуляторів, складність оперативної оцінки вартості та високий ступінь анонімності власності, що створює ідеальне середовище для інтеграції "брудних" грошей у легальну економіку.

Найпоширенішою практикою є придбання об’єктів елітної нерухомості через фіктивні компанії або офшорні трастові структури. Це дозволяє замаскувати справжнього бенефіціара угоди, використати готівкові кошти або криптовалюту, а згодом — продати актив за ринковою або завищеною ціною, формально отримавши “чистий” прибуток. Згідно з даними FATF (2021), у 22 з 37 країн-учасниць було виявлено факти відмивання коштів через ринок нерухомості, зокрема в Лондоні, Нью-Йорку, Дубаї та Ванкувері. Transparency International (2022) встановила, що лише в Лондоні налічується понад 87 тисяч об'єктів нерухомості, зареєстрованих на компанії з юрисдикцій із низьким рівнем прозорості.

Схожим чином функціонує й ринок витворів мистецтва. Він є надзвичайно вразливим до фінансових махінацій через відсутність централізованої реєстрації транзакцій, суб’єктивне оцінювання вартості об'єктів та наявність спеціалізованих митних зон (так званих "freeports"), де твори зберігаються без обов’язкового декларування. Deloitte Art & Finance Report (2023) оцінює світовий арт-ринок у понад 65 млрд доларів США, при цьому близько 5–10% транзакцій можуть мати кримінальне або підозріле походження. Особливу увагу правоохоронці звертають на випадки покупки рідкісних картин чи скульптур за готівку, а також на продаж творів мистецтва через аукціони з непрозорими власниками.

Ще одним ефективним способом приховування доходів є операції з дорогоцінними металами, зокрема золотом, платиновою групою металів, а також коштовним камінням. Перевагою цих активів є компактність, висока вартість на одиницю ваги та можливість обігу поза банківською системою. Наприклад, стандартний злиток золота в 1 кг має ринкову вартість понад 60 тис. доларів і може бути легко переміщений через кордон у ручній поклажі. За даними Global Financial Integrity (2021), у 2019–2020 роках щонайменше 40–50 млрд доларів США було відмито через нелегальну торгівлю золотом і коштовностями, особливо в країнах Близького Сходу, Індії, Західної Африки та Туреччини, де контроль над обігом таких товарів залишається низьким або фрагментованим.

Таким чином, операції з нерухомістю, предметами мистецтва та дорогоцінними металами відіграють значну роль у глобальній системі фінансових злочинів. Їх спільною характеристикою є здатність маскувати походження активів через складність у верифікації вартості, власності та джерела фінансування, а також низький рівень контролю у багатьох юрисдикціях. У зв’язку з цим посилення регулювання на ринках "нерухомого капіталу" є одним із ключових викликів для сучасної антикримінальної фінансової політики.

ДОДАТОК Д

Торгівля цінними паперами та ф'ючерсами як механізм легалізації незаконних доходів

Фінансові злочини, що здійснюються через фондовий ринок, є однією з найбільш витончених форм маскування незаконного походження активів. Особливість біржових операцій полягає у високому рівні складності, швидкості проведення транзакцій та широкому спектрі інструментів, які можуть бути використані як легально, так і з метою шахрайства. Саме це робить фондові ринки привабливим середовищем для злочинців, які прагнуть замаскувати або легалізувати свої доходи під виглядом інвестиційного прибутку.

Одним із найпоширеніших механізмів є інсайдерська торгівля — придбання або продаж цінних паперів на основі внутрішньої, неоприлюдненої інформації, що дає змогу отримати неправомірну перевагу. Цей тип злочину важко довести, оскільки він потребує доказів доступу до конфіденційних джерел та умисного використання інформації.

Ще одним інструментом є "pump and dump"-схеми, коли злочинці штучно підвищують попит на маловідомі або "сміттєві" акції через дезінформацію, а потім — масово їх продають, залишаючи інших інвесторів із знеціненими активами. Такі дії не лише шкодять добросовісним учасникам ринку, а й дозволяють злочинцям офіційно задекларувати прибуток, що формально походить із біржової діяльності.

Особливу загрозу становлять похідні фінансові інструменти (деривативи), включаючи ф'ючерси, опціони та свопи. Завдяки складній структурі цих контрактів, можливості їх використання у позабіржовому (OTC) сегменті та частій відсутності регуляторного нагляду, злочинці можуть здійснювати приховані перекази коштів, створювати фіктивні збитки або приховувати реальний обсяг операцій. Такі дії дозволяють не лише уникати податкового навантаження, а й приховувати кінцевих бенефіціарів і справжній намір транзакції.

За офіційною статистикою Комісії з цінних паперів і бірж США (SEC), щороку відкривається понад 800 справ щодо порушень на фондовому ринку, з яких значна частина пов'язана з інсайдерською торгівлею, маніпуляціями з

деривативами та шахрайськими схемами в інвестиційних фондах. Аналогічно, в Європейському Союзі, відповідно до положень 6-ї директиви щодо боротьби з відмиванням коштів (AMLD 6, 2021), маніпуляції з фінансовими інструментами офіційно класифікуються як "серйозні злочини", що потребують обов’язкової криміналізації у законодавстві всіх країн-членів.

Таким чином, фондовий ринок, попри наявність складної системи регулювання та нагляду, залишається привабливою платформою для "відбілювання" фінансових потоків. Особливо високі ризики пов’язані з транснаціональними операціями, приватними інвестиційними фондами, торгівлею на OTC-ринках і активами, які обертаються без належної перевірки джерел капіталу. Це вимагає посилення міждержавної координації, удосконалення систем автоматичного обміну біржовими даними та запровадження технологічних рішень на основі штучного інтелекту для виявлення аномальних фінансових дій у режимі реального часу.