

**ВСП «Харківський торговельно-економічний фаховий коледж
Державного торговельно-економічного університету»**

Циклова комісія економіки, управління та адміністрування

Шнайдер Олександр Миколайович

КУРСОВА РОБОТА

«Розробка політики протидії відмиванню коштів на підприємстві»

Навчальна дисципліна	Фінансово-економічна безпека організації назва навчальної дисципліни
Ступінь освіти	Фаховий молодший бакалавр фаховий молодший бакалавр, молодший бакалавр, бакалавр
Галузь знань	07 Управління та адміністрування шифр і назва галузі знань
Спеціальність	072 Фінанси, банківська справа, страхування та фондовий ринок код і найменування спеціальності
Освітньо-професійна програма	Фінанси і кредит назва освітньо-професійної програми
Академічна група	Ф-24 назва академічної групи

Харків, 2026 рік

Керівник:

Постольна Наталія Олександрівна, викладач
циклової комісії економіки, управління та
адміністрування, спеціаліст вищої категорії

Робота містить результати власних досліджень. Використання ідей,
результатів і текстів інших авторів мають посилання на відповідне джерело.

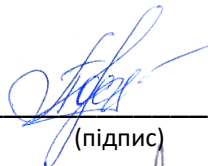
Здобувач



Шнайдер О.М.

Підсумкова оцінка: 75 (балів)

Члени комісії з захисту:



(підпис)

Н. О. Постольна



(підпис)

О.М. Тимошенко

**ВСП «Харківський торговельно-економічний фаховий коледж
Державного торговельно-економічного університету»**

Циклова комісія економіки, управління та адміністрування

Шнайдер Олександр Миколайович

ЗАВДАННЯ НА КУРСОВУ РОБОТУ

Навчальна
дисципліна

Фінансово-економічна безпека організації

назва навчальної дисципліни

Тема роботи

«Розробка політики протидії відмиванню коштів н
підприємстві»

Термін подання
завершеної роботи

26.04.2026 р.

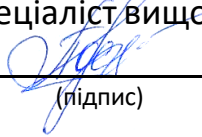
фаховий молодший бакалавр, молодший бакалавр, бакалавр

Графік виконання роботи

Виконання роботи за розділами	Термін виконання
Вибір та затвердження теми	02.02 – 08.02.2026
Добір та аналіз літератури за обраною темою	09.02 – 15.02.2026
Складання плану курсової роботи	16.02 – 22.02.2026
Написання вступу та I розділу	23.02 – 15.03.2026
Написання розрахункової частини (II розділ) курсової роботи	16.03 – 05.04.2026
Написання висновків та пропозицій, оформлення курсової роботи	06.04 – 19.04.2026
Подання курсової роботи керівнику для рецензування (для рекомендації до захисту)	20.04 – 26.04.2026
Захист курсової роботи	04.05 – 09.05.2026

Завдання видав

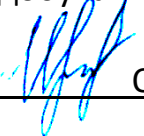
Науковий керівник,
спеціаліст вищої категорії

 Наталія ПОСТОЛЬНА
(підпис)

«02» лютого 2026 р.

Завдання отримав

Здобувач

 Олександр ШНАЙДЕР

«02» лютого 2026 р.

ЗМІСТ

ВСТУП.....	5
РОЗДІЛ 1. ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ОСНОВИ ФУНКЦІОНУВАННЯ СИСТЕМИ ПРОТИДІЇ ВІДМИВАННЮ КОШТІВ	7
1.1. Сутність та еволюція поняття «відмивання коштів» у сучасній економіці.....	7
1.2. Нормативно-правове регулювання системи протидії відмиванню коштів в Україні та світі	10
1.3. Ризик-орієнтований підхід як база побудови внутрішньої системи моніторингу.....	14
РОЗДІЛ 2. ПРОЄКТУВАННЯ ТА ВПРОВАДЖЕННЯ СИСТЕМИ ПРОТИДІЇ ВІДМИВАННЮ КОШТІВ НА ПІДПРИЄМСТВІ.....	17
2.1. Алгоритм розробки внутрішньої політики та процедур фінансового моніторингу.....	17
2.2. Автоматизація процесів ідентифікації та верифікації клієнтів	20
2.3. Оцінка ефективності системи ПВК та напрями її вдосконалення в умовах цифровізації.....	23
ВИСНОВКИ.....	25
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	27
ДОДАТКИ	29

ВСТУП

У сучасних умовах розвитку світової та національної економіки проблема протидії відмиванню коштів набуває особливої актуальності. Легалізація доходів, отриманих злочинним шляхом, становить серйозну загрозу для фінансової безпеки держави, стабільності банківської системи та нормального функціонування суб'єктів господарювання. Підприємства, незалежно від форми власності та сфери діяльності, можуть бути як об'єктами, так і інструментами у схемах відмивання коштів, що підвищує необхідність впровадження ефективних механізмів фінансового контролю.

Особливої важливості набуває система протидії легалізації злочинних доходів у контексті посилення вимог міжнародних організацій, зокрема FATF, а також гармонізації національного законодавства України з європейськими стандартами. Впровадження дієвих процедур фінансового моніторингу дозволяє своєчасно виявляти підозрілі операції та мінімізувати ризики участі підприємства у незаконних фінансових схемах.

Актуальність теми курсової роботи зумовлена необхідністю підвищення рівня фінансової безпеки підприємств, удосконалення внутрішніх систем контролю та забезпечення відповідності діяльності компаній вимогам законодавства у сфері протидії відмиванню коштів.

Метою курсової роботи є дослідження теоретичних засад та розробка практичних рекомендацій щодо створення ефективної системи протидії відмиванню коштів на підприємстві.

Для досягнення поставленої мети необхідно вирішити такі завдання:

- розкрити сутність поняття «відмивання коштів» та його основні форми;
- дослідити нормативно-правове регулювання у сфері протидії легалізації злочинних доходів;

- проаналізувати ризики, пов'язані з відмиванням коштів для підприємств;
- визначити роль фінансового моніторингу у системі запобігання фінансовим злочинам;
- розробити практичні рекомендації щодо удосконалення системи протидії відмиванню коштів на підприємстві.

Об'єктом дослідження є процеси фінансової діяльності підприємства в контексті протидії відмиванню коштів.

Предметом дослідження виступають методи, інструменти та механізми запобігання легалізації доходів, отриманих злочинним шляхом.

У процесі написання курсової роботи використовувалися такі методи дослідження: аналіз і синтез, порівняння, узагальнення, системний підхід, а також елементи економічного та нормативно-правового аналізу.

Практична значущість роботи полягає у можливості застосування запропонованих рекомендацій для вдосконалення внутрішніх систем фінансового моніторингу на підприємствах різних форм власності.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ПРОТИДІЇ ВІДМИВАННЮ КОШТІВ НА ПІДПРИЄМСТВІ.

1.1. Сутність та поняття відмивання коштів.

Феномен легалізації (відмивання) доходів, одержаних злочинним шляхом, є однією з найбільш деструктивних загроз для стабільності національних та глобальної фінансових систем. У науковій літературі та міжнародному праві під «відмиванням коштів» розуміють процес приховування незаконного походження фінансових активів з метою надання їм вигляду легально отриманих прибутків. Як зазначає Т. Гуржій, цей процес є логічним завершенням будь-якої корисливої злочинної діяльності, оскільки дозволяє злочинним угрупованням користуватися активами без ризику викриття їхнього джерела [2].

Еволюція цього поняття пройшла шлях від вузького сприйняття як результату торгівлі наркотиками, що було закріплено у Конвенції ООН 1988 року до широкого трактування, що охоплює будь-які предикатні злочини, включаючи корупцію, кіберзлочинність та податкові махінації.

Сучасний етап розвитку (2020-2025 рр.) характеризується інтеграцією цифрових активів у схеми легалізації. За визначенням FATF, сучасне відмивання коштів все частіше використовує віртуальні активи та послуги VASP, що вимагає перегляду традиційних підходів до моніторингу [5].

У класичній економічній теорії процес відмивання коштів поділяють на три ключові стадії, які залишаються актуальними, попри трансформацію методів:

1. Розміщення: введення «брудних» грошей у фінансову систему через банківські депозити, купівлю товарів або валюти.
2. Розшарування: створення складної мережі фінансових операцій для віддалення коштів від їхнього джерела використання офшорних компаній,

"переливання" коштів між рахунками.

3. Інтеграція: надання активам статусу законних шляхом інвестування в нерухомість, бізнес або цінні папери.

Дослідник З. Живко підкреслює, що в умовах 2024 року межа між цими стадіями розмивається через використання технологій блокчейн та смарт-контрактів, які дозволяють проводити тисячі транзакцій за секунди, що суттєво ускладнює роботу комплаєнс-підрозділів підприємств [3].

Особливістю періоду 2022-2025 років для України стало виникнення нових схем легалізації, пов'язаних із воєнним станом, зокрема під виглядом волонтерської допомоги або через фіктивні зовнішньоекономічні контракти. Це змушує суб'єктів первинного фінансового моніторингу розглядати відмивання коштів не лише як кримінальну проблему, а як комплексний ризик для економічної безпеки підприємства.

Отже, сутність «відмивання коштів» сьогодні трансформувалася з простої банківської операції у високотехнологічний процес, який поєднує методи соціальної інженерії, цифрові валюти та глобальні фінансові інструменти. Це вимагає від підприємств розробки гнучких систем протидії, здатних адаптуватися до нових викликів у режимі реального часу [4].

Аналіз статистики виявлених правопорушень та механізмів використання криптоактивів у схемах легалізації (2023–2024 рр.)

Сучасний стан протидії відмиванню коштів в Україні характеризується адаптацією національної системи фінансового моніторингу до викликів воєнного стану та стрімкої цифровізації фінансових послуг. Згідно з офіційними звітами Державної служби фінансового моніторингу України, протягом 2023 року та першої половини 2024 року діяльність підрозділу фінансової розвідки була зосереджена на виявленні схем, пов'язаних із розкраданням бюджетних коштів, колабораційною діяльністю та фінансуванням тероризму.

За результатами аналітичних досліджень Держфінмоніторингу, у 2023

році до правоохоронних органів було спрямовано понад 1000 матеріалів, які стосувалися підозрілих операцій на загальну суму понад 100 млрд грн. Важливою тенденцією 2024 року стало зростання частки операцій, пов'язаних із віртуальними активами. Якщо у 2021 році такі кейси були поодинокими, то у 2023-2024 роках вони стали системними, особливо в контексті обходу міжнародних санкцій та виведення капіталу за кордон.

1.2. Нормативно-правове регулювання системи протидії відмиванню коштів в Україні та світі.

Сучасна архітектура нормативно-правового регулювання у сфері протидії відмиванню коштів та фінансуванню тероризму в Україні базується на принципі гармонізації національного законодавства із міжнародними стандартами. Фундаментом цієї системи є Рекомендації FATF, які визначають глобальні орієнтири для урядів та приватного сектору. Як зазначають дослідники, у період 2020–2025 рр. особлива увага міжнародних регуляторів зосереджена на прозорості бенефіціарної власності та контролі за віртуальними активами [5].

Ключовим законодавчим актом в Україні є Закон № 361-IX «Про запобігання та протидію легалізації (відмиванню) доходів...», прийнятий наприкінці 2019 року, але який зазнав суттєвих трансформацій протягом 2022–2024 років у зв'язку з отриманням Україною статусу кандидата у члени ЄС. Цей Закон запровадив принципово нову модель — ризик-орієнтований підхід, згідно з яким підприємства повинні самостійно оцінювати ризики своїх клієнтів та операцій, а не просто формально звітувати про них [1].

На державному рівні регулювання забезпечується системою органів, серед яких ключове місце посідають:

— Державна служба фінансового моніторингу України — орган, що виконує функції фінансової розвідки;

— Національний банк України та Міністерство фінансів — регулятори, що встановлюють специфічні вимоги до суб'єктів первинного фінансового моніторингу.

Важливим етапом еволюції права у 2023–2024 роках стало посилення вимог щодо ідентифікації публічно значущих осіб. Згідно з оновленими нормами, статус PEP в Україні знову став довічним, що відповідає стандартам ЄС та вимогам Міжнародного валютного фонду. Це накладає на комплаєнс-підрозділи підприємств додаткові обов'язки щодо посиленої перевірки джерел походження статків таких клієнтів [4].

Також неможливо ігнорувати вплив європейського права, зокрема V та VI Антидопінгових директив ЄС. Директива (EU) 2018/843 V Директива розширила коло суб'єктів моніторингу, включивши до них платформи обміну криптовалюти, а VI Директива (EU) 2018/1673 уніфікувала перелік предикатних злочинів та посилила кримінальну відповідальність за відмивання коштів на рівні всього Європейського Союзу. Для українських підприємств, що працюють на європейських ринках, дотримання цих директив є обов'язковою умовою «гігієни бізнесу» та уникнення санкцій [6].

Для глибокого розуміння трансформації європейського законодавства, яке є орієнтиром для України, необхідно проаналізувати ключові зміни у Директивах ЄС щодо протидії відмиванню коштів.

Взаємодія Держфінмоніторингу з Егмонтською групою

Державна служба фінансового моніторингу України, як підрозділ фінансової розвідки, відіграє роль ключового вузла в системі національної безпеки. Важливим аспектом її діяльності є членство в Егмонтській групі — міжнародному об'єднанні, що налічує понад 160 фінансових розвідок світу.

Взаємодія в рамках Егмонтської групи у 2020–2025 роках базується на таких принципах:

1. Захищений обмін інформацією: Використання закріпленої мережі дозволяє українській розвідці в режимі реального часу отримувати дані про підозрілі транзакції українських резидентів за кордоном.

Критерій порівняння	IV Директива (2015/849)	V Директива (2018/843)	VI Директива (2018/1673)
Основний фокус	Посилення ризик-орієнтованого підходу.	Прозорість та цифровізація активів.	Уніфікація кримінального права та відповідальності.
Бенефіціарна власність	Створення центральних реєстрів бенефіціарів.	Публічний доступ до реєстрів; обов'язкова перевірка даних.	Посилення транскордонного співробітництва щодо виявлення бенефіціарів.
Віртуальні активи	Не регулювалися належним чином.	Включення платформ обміну криптовалют до суб'єктів моніторингу.	Визначення кіберзлочинів як предикатних для відмивання коштів.
Політично значущі особи (РЕР)	Посилений контроль за іноземними РЕР.	Розширення переліку функцій, що визначають статус РЕР.	Посилення санкцій за пособництво РЕР у відмиванні доходів.
Криміналізація	Загальні положення про відповідальність.	Фокус на адміністративних заходах та штрафах.	Визначення 22 предикатних злочинів ; мін. термін ув'язнення — 4 роки.
Анонімні інструменти	Обмеження використання передплачених карток.	Суттєве зниження лімітів для анонімних платежів (до 150 євро).	Повна криміналізація приховування джерел через анонімні активи.

Рисунок 1.1. Еволюція вимог Директив ЄС у сфері Протидії відмивання коштів (2015–2025 рр.)

Джерело: складено автором на основі [5, 6].

2. Спільні розслідування: У 2024 році особливий акцент зроблено на виявленні активів, пов'язаних із фінансуванням тероризму та агресивної війни. Егмонтська група сприяє швидкому накладенню арешту на закордонні рахунки до моменту їх повного виведення в офшорні зони.

3. Типологічні дослідження: Держфінмоніторинг бере участь у розробці глобальних "схем-шаблонів" відмивання коштів, що допомагає українським підприємствам краще ідентифікувати новітні загрози.

Кореляція українського законодавства із санкційними списками OFAC та ЄС.

В умовах глобалізації комплаєнс-система підприємства не може обмежуватися лише національним законодавством. Українське правове поле у 2022–2025 роках тісно інтегрувалося із міжнародними санкційними режимами.

Управління контролю за іноземними активами Міністерства фінансів США публікує списки SDN. Хоча ці списки є частиною юрисдикції США, для українських підприємств вони мають критичне значення через:

1. Ризик вторинних санкцій: Співпраця з особами з реєстру OFAC може призвести до блокування доларових платежів підприємства через банки-кореспонденти.

2. Вимоги НБУ: Регулятор зобов'язує українські банки перевіряти клієнтів за списками OFAC, що автоматично робить ці списки обов'язковими для будь-якого бізнесу, що користується банківськими послугами.

Санкції Європейського Союзу є обов'язковими в межах гармонізації законодавства. Згідно зі статтею 15 Закону № 361-IX, операції, учасники яких включені до міжнародних санкційних списків ухвалених РБ ООН, ЄС або іншими організаціями, до яких приєдналася Україна, підлягають негайному замороженню.

Механізм кореляції на підприємстві:

1. Автоматичний скринінг: При розробці системи Протидії Відмиванню Коштів підприємство має впроваджувати програмне забезпечення, яке щоденно оновлює базу даних із реєстрів РНБО, OFAC та ЄС.

2. Правило 50%: Відповідно до стандартів OFAC та аналогічних підходів в Україні, санкції поширюються і на ті компанії, де підсанкційна особа володіє часткою 50% і більше, навіть якщо сама компанія не вказана в списках.

Така багаторівнева фільтрація дозволяє підприємству мінімізувати ризики втрати активів та зберегти доступ до міжнародних ринків капіталу [4, 7].

Окремим вектором регулювання у 2024–2025 роках стала адаптація системи Протидії Відмиванню Коштів до умов воєнного стану. Постанови НБУ та

нормативні акти Кабінету Міністрів України впровадили спрощені процедури ідентифікації для певних категорій операцій, водночас посиливши контроль за транзакціями, що можуть бути пов'язані з державою-агресором або обходом міжнародних санкцій [2].

Отже, нормативна база протидії відмиванню коштів в Україні станом на 2025 рік є динамічною структурою, що поєднує жорсткі міжнародні стандарти із гнучкими національними механізмами контролю. Це вимагає від керівництва підприємств постійного моніторингу законодавчих змін та регулярного оновлення внутрішніх регламентів фінансового моніторингу.

1.3. Ризик-орієнтований підхід як база побудови внутрішньої системи моніторингу.

Впровадження ризик-орієнтованого підходу (далі скорочено-РОП) є фундаментальною зміною парадигми фінансового моніторингу, що відбулася в межах останніх міжнародних реформ FATF. Сутність цього підходу полягає у відмові від «суцільного» формального контролю всіх операцій на користь концентрації ресурсів підприємства на тих ділянках, де ризики легалізації доходів є найвищими.

Згідно зі статтею 7 Закону України № 361-IX, суб'єкт первинного фінансового моніторингу зобов'язаний у своїй діяльності застосовувати РОП, враховуючи відповідні критерії ризику, пов'язані з його клієнтами, географічним розташуванням, видами товарів та послуг, а також каналами поставки.

Механізм функціонування внутрішньої системи моніторингу на базі РОП включає наступні критичні етапи:

1. Ідентифікація та оцінка ризиків. Підприємство має розробити власну методику оцінки, яка дозволяє присвоїти кожному клієнту певний рівень ризику (низький, середній, високий). Критерії оцінки зазвичай поділяються на:

— *Клієнтські ризики*: статус PEP, наявність у санкційних списках, непрозора структура власності.

— *Географічні ризики*: реєстрація контрагента в країнах, що не виконують рекомендації FATF, або в зонах активних бойових дій.

— *Операційні ризики*: використання готівкових розрахунків у великих розмірах, нетипові для профілю клієнта транзакції.

2. Розробка заходів мінімізації. Для клієнтів із високим рівнем ризику підприємство зобов'язане застосовувати посилені заходи належної перевірки. Це включає отримання додаткової інформації про джерела походження коштів, посилений моніторинг ділових відносин та обов'язкове схвалення встановлення відносин вищим керівництвом.

3. Автоматизація процесів. В умовах 2025 року реалізація РОП неможлива без використання спеціалізованого програмного забезпечення. Сучасні системи автоматично проводять скринінг контрагентів через бази даних та сигналізують про «червоні прапорці» у режимі реального часу.

4. Пропорційність контролю. Важливою перевагою РОП є можливість спрощеної ідентифікації для клієнтів із низьким ризиком, що зменшує адміністративне навантаження на бізнес та підвищує його конкурентоспроможність, не порушуючи при цьому вимог безпеки.

Ефективна побудова внутрішньої системи моніторингу на основі РОП дозволяє підприємству змінити роль комплаєнс-підрозділу з «гальма бізнес-процесів» на стратегічного партнера, який захищає активи компанії від залучення у незаконні схеми. Це забезпечує не лише юридичну чистоту операцій, а й високий рівень довіри з боку банків-кореспондентів та іноземних інвесторів [3, 12].

Практичний приклад застосування РОП: Кейс-стаді «Оцінка ризику транскордонної операції»

Для ілюстрації механізму роботи внутрішньої системи моніторингу розглянемо типовий сценарій, з яким може зіткнутися українське промислове підприємство (далі — Підприємство).

Об'єкт аналізу: Потенційний контрагент — компанія "Larnaka Trade Ltd", зареєстрована на Кіпрі. Суть операції: Закупівля обладнання на суму 15 млн грн. Оплата пропонується через банківську установу в юрисдикції, що входить до «сірого списку» FATF, із залученням третьої сторони як платника.

Алгоритм дій комплаєнс-офіцера на основі РОП:

1. Початковий скринінг: Система автоматично перевіряє назву компанії та її директорів за списками РНБО, OFAC та ЄС. Прямих збігів не виявлено, проте встановлено, що одним із бенефіціарів є особа, яка була пов'язана з державним сектором України до 2021 року.

Рівень ризику підвищується до «Середнього».

2. Географічний аналіз: Незважаючи на те, що Кіпр є членом ЄС, він часто використовується як транзитна зона для приховування кінцевих власників. Використання банку з «сірого списку» для проведення платежу є критичним «червоним прапорцем».

Рівень ризику підвищується до «Високого».

3. Застосування посилених заходів належної перевірки: Оскільки встановлено високий рівень ризику, Підприємство не має права формально провести ідентифікацію. Комплаєнс-офіцер ініціює наступні дії:

— Запит декларації про джерело походження коштів: Контрагент має надати документи, що підтверджують легальність 15 млн грн (наприклад, виписки про дивіденди або кредитні договори).

— Встановлення кінцевого бенефіціарного власника: Вимога надати розгорнуту структуру власності до рівня фізичних осіб.

— Аналіз суті операції: Чому платіж здійснює третя сторона? Чи має це логічне економічне обґрунтування, чи це спроба розірвати ланцюжок

транзакцій?

4. Прийняття рішення: На основі зібраних даних складається звіт. Якщо контрагент відмовляється надати дані про UBO або не може підтвердити походження коштів, згідно з РОП, Підприємство зобов'язане:

- Відмовити у встановленні ділових відносин (ст. 15 Закону № 361-IX).
- Повідомити Держфінмоніторинг про спробу проведення підозрілої операції.

Цей кейс демонструє, що РОП — це не перешкода для бізнесу, а фільтр. Якби Підприємство прийняло платіж без перевірки, воно б ризикувало потрапити під санкції банку-кореспондента, що призвело б до блокування всіх валютних рахунків компанії. Таким чином, ризик-орієнтований підхід виступає гарантом фінансової безпеки та репутації суб'єкта господарювання.

РОЗДІЛ 2. ПРОЄКТУВАННЯ ТА ВПРОВАДЖЕННЯ СИСТЕМИ ПРОТИДІЇ ВІДМИВАННЮ КОШТІВ НА ПІДПРИЄМСТВІ.

2.1. Алгоритм розробки внутрішньої політики та процедур фінансового моніторингу.

Розробка внутрішньої системи протидії легалізації доходів на підприємстві — це багатоетапний процес, що потребує інтеграції юридичних, технічних та управлінських рішень. Для того, щоб система була не лише формально відповідною закону, а й реально дієвою, автором пропонується наступний алгоритм впровадження.

Етап 1. Організаційне забезпечення та призначення відповідальних осіб. Першим кроком є видання наказу керівника про призначення Відповідального працівника за проведення фінансового моніторингу - комплаєнс-офіцера. Відповідно до стандартів 2024–2026 років, ця особа повинна мати бездоганну ділову репутацію та достатні повноваження для блокування підозрілих операцій [1, 14]. На цьому ж етапі затверджується «Положення про службу фінансового моніторингу» (Додаток А).

Етап 2. Розробка Внутрішніх правил фінансового моніторингу. Це основний документ, який деталізує:

- порядок проведення ідентифікації та верифікації клієнтів;
- критерії віднесення операцій до категорій підозрілих;
- процедуру документування результатів перевірки. Важливо, щоб ці правила регулярно (не рідше одного разу на рік) оновлювалися відповідно до змін у законодавстві та типологіях Держфінмоніторингу [7, 9].

Етап 3. Проведення власної оцінки ризиків підприємства. Підприємство має проаналізувати свій бізнес-портфель. *Наприклад:* Якщо компанія займається експортом зерна, основними ризиками будуть розрахунки через офшорні компанії-прокладки. Якщо це ІТ-компанія — ризики будуть пов'язані з

платежами у криптовалюті або від іноземних замовників з непрозорою структурою власності.

Етап 4. Адаптація до умов воєнного стану та санкційного режиму. Окремим критичним кроком у розробці внутрішньої політики є створення протоколу дій у разі виявлення прямого або опосередкованого зв'язку контрагента з державою-агресором [4, 16]. В умовах воєнного стану алгоритм перевірки обов'язково включає:

- Скринінг за списками РНБО та міжнародними санкційними реєстрами.
- Виявлення «російського чи білоруського сліду» в структурі власності навіть через декілька рівнів афілійованості.
- Припинення ділових відносин та повідомлення правоохоронних органів у разі виявлення ознак фінансування тероризму чи колабораційної діяльності.

Етап 5. Впровадження системи автоматизованого скринінгу. В умовах великої кількості контрагентів ручна перевірка є неефективною. Підприємство має обрати та інтегрувати програмне забезпечення, яке дозволяє автоматично моніторити статус PEP та санкційні списки у режимі реального часу.

Етап 6. Навчання персоналу та створення культури комплаєнсу. Ефективність алгоритму залежить від обізнаності працівників «першої лінії». Програма навчання має включати графік інструктажів та окремий блок щодо виявлення ознак фінансування сепаратизму чи нелегальних збройних формувань.

Етап 7. Формування системи звітності та комунікації. Алгоритм має чітко визначати канали передачі інформації:

- *«Вертикальний» канал:* від працівника до Комплаєнс-офіцера.
- *«Зовнішній» канал:* подання інформації до Держфінмоніторингу з дотриманням принципу «Tipping-off».

Етап 8. Процедура актуалізації даних та аудит. Алгоритм не завершується на етапі прийняття клієнта. Внутрішня політика передбачає регулярний перегляд профілів клієнтів та щорічний незалежний аудит системи для виявлення «вузьких місць» у контролі.

Таким чином, запропонований алгоритм розробки внутрішньої політики ПВК перетворює абстрактні норми закону на конкретну послідовність дій. Це дозволяє створити на підприємстві замкнений цикл контролю, що в умовах воєнного стану стає не лише юридичним обов'язком, а й запорукою національної безпеки та захисту ділової репутації суб'єкта господарювання.

2.2. Автоматизація процесів ідентифікації та верифікації клієнтів

У сучасних умовах цифровізації фінансових послуг ручна перевірка контрагентів стає не лише неефективною, а й ризикованою. Впровадження автоматизованих систем ідентифікації клієнтів та бізнес-партнерів є критичним елементом розробки системи ПВК на підприємстві.

Для наочності розробимо блок-схему, яка демонструє життєвий цикл перевірки клієнта в системі ПВК підприємства [11, 19].

Блок-схема: «Шлях клієнта: від першого контакту до верифікації»

1. Первинний контакт- отримання реквізитів або документів клієнта.

2. Автоматичний скринінг:

Збіг знайдено - Миттєве блокування, повідомлення комплаєнс-офіцера.

Збігів не виявлено - Перехід до наступного етапу.

3. Ідентифікація та верифікація:

Перевірка дійсності документів через державні реєстри.

Пошук кінцевих бенефіціарних власників.

4. Оцінка ризику:

Аналіз статусу РЕР, ділової репутації, географічного ризику.

5. Прийняття рішення:

Низький/Середній ризик - Встановлення ділових відносин.

Високий ризик - Застосування посилених заходів перевірки.

Технічний аналіз програмних рішень для Протидії Відмиванню Коштів

Для реалізації вищезазначеної схеми українські підприємства найчастіше використовують вітчизняні та міжнародні ІТ-продукти. Проведемо порівняльний аналіз двох найбільш популярних рішень: YouControl та AMLBot.

1. YouControl - модуль «Експрес-аналіз» та «Compliance»

YouControl є потужною аналітичною системою, що базується на відкритих даних [21]. Для цілей Протидії Відмиванню Коштів система пропонує спеціалізований інструментарій, який дозволяє за лічені секунди отримати повне досьє на компанію.

Переваги:

— *Глибина даних*: Агрегує інформацію з понад 180 державних реєстрів України.

— *Візуалізація зв'язків*: Автоматично будує схеми афілійованості, що дозволяє виявити прихованих бенефіціарів та пов'язаних осіб - зокрема, з РФ та Білоруссю.

— *Моніторинг*: Функція автоматичного сповіщення про зміни у статусі контрагента - зміна директора, податковий борг, банкрутство.

Недоліки: Орієнтованість переважно на український ринок; для міжнародного комплаєнсу потребує інтеграції з іноземними реєстрами.

2. AMLBot

AMLBot — це інноваційне рішення, яке спеціалізується на перевірці «чистоти» транзакцій у віртуальних активах та проведенні глобального санкційного скринінгу [17, 24].

Переваги:

— *Крипто-комплаєнс*: Дозволяє перевірити криптогаманець на предмет зв'язків із даркнетом, міксерами або вкраденими активами.

— *Глобальне охоплення*: Перевірка за списками OFAC, PER, санкціями ЄС та ООН у реальному часі.

— *API-інтеграція*: Легко інтегрується у CRM-систему підприємства для автоматизації перевірок.

Недоліки: Вузька спеціалізація на скринінгу; не надає такої глибокої аналітики господарської діяльності компанії, як YouControl.

Характеристика	YouControl	AMLBot
Перевірка українських юросіб	Еталонна (глибока)	Поверхнева (тільки санкції)
Санкційні списки (Глобальні)	Наявні	Пріоритетні (оновлення real-time)
Моніторинг криптоактивів	Відсутній	Високий рівень (Blockchain-аналітика)
Пошук зв'язків та UBO	Автоматична візуалізація	Текстове підтвердження збігів
Вартість впровадження	Середня (річна передплата)	Гнучка (оплата за кількість перевірок)

Рис 2.1. Функціональні характеристики для системи Протидії Відмиванню Коштів

Таким чином, для побудови комплексної системи Протидії Відмиванню Коштів на великому промисловому або торговому підприємстві доцільно використовувати комбінований підхід: YouControl для детальної перевірки українських контрагентів та побудови структур власності, а AMLBot — для санкційного моніторингу іноземних партнерів та операцій із віртуальними активами.

Інтеграція цих інструментів у бізнес-процеси дозволяє знизити комплаєнс-ризик на 80-90% та забезпечити відповідність критеріям «належної обачності», що вимагаються державними регуляторами [11, 18].

2.3. Оцінка ефективності системи Протидії Відмиванню Коштів та напрями її вдосконалення в умовах цифровізації на прикладі ПрАТ «МХП» .

Ефективність системи Протидії Відмиванню Коштів на ПрАТ «МХП» обумовлена складністю структури холдингу та великою кількістю міжнародних контрагентів. У 2025–2026 роках компанія перейшла від ручного моніторингу до комплексної автоматизованої системи оцінки ризиків.

1. Оцінка поточної ефективності за KPI

На підприємстві впроваджено щоквартальний аудит системи за наступними показниками:

а) Повнота охоплення: Завдяки інтеграції внутрішньої ERP-системи з базами даних, наприклад, YouControl або Refinitiv, 100% нових контрагентів проходять автоматичну перевірку за списками РЕР та санкційними списками ще на етапі тендеру.

б) Точність спрацювань: У 2024 році цей показник становив 15%, проте після впровадження алгоритмів машинного навчання у 2025 році кількість «помилкових тривог» знизилася до 8%, що дозволило комплаєнс-офіцерам зосередитися на реальних ризиках.

с) Швидкість ідентифікації: Використання автоматизованих API-інтерфейсів дозволило скоротити час перевірки іноземного контрагента з 2 робочих днів до 3 хвилин [19].

2. Напрями вдосконалення в умовах цифровізації

Для ПрАТ «МХП», як для експортера, критично важливим є впровадження новітніх технологій, описаних у теоретичній частині:

А. Впровадження ШІ для виявлення «карусельних» схем. Оскільки підприємство має сотні дочірніх компаній та тисячі дистриб'юторів, ШІ аналізує «мережеву активність». Система виявляє аномалії, коли група дрібних фермерських господарств синхронно проводить оплати, що можуть свідчити про спроби легалізації коштів через закупівлю сільгосппродукції за готівку.

Б. Розумний санкційний моніторинг. Враховуючи глобальну присутність ПрАТ «МХП», система використовує нечітку логіку для моніторингу суден та логістичних компаній. Це дозволяє ідентифікувати ризики, навіть якщо назва компанії-перевізника або власника судна вказана з навмисними помилками чи транслітерацією, щоб обійти санкції ЄС чи США.

В. Блокчейн-ідентифікатори для КУВ. Підприємство розглядає впровадження технології розподіленого реєстру для обміну результатами верифікації з банками-партнерами. Це дозволяє уникнути повторного збору документів (наприклад, статутів чи витягів) для надійних партнерів, з якими компанія працює понад 5 років [5, 22].

3. Економічний ефект від вдосконалення

Автоматизація ПВК на підприємстві приносить не лише безпековий, а й фінансовий ефект:

- Мінімізація штрафів: 0 грн штрафних санкцій від регуляторів за останні періоди.

- Репутаційний капітал: Наявність прозорості AI-системи моніторингу дозволяє отримувати кредити від міжнародних інституцій за нижчими відсотковими ставками.

- Безперервність бізнесу: Моніторинг транзакцій 24/7 у режимі реального часу гарантує, що кошти компанії не будуть заморожені банками-кореспондентами через підозрілі дії контрагентів.

Впровадження запропонованих технологічних рішень дозволяє перетворити систему протидії відмиванню коштів з «витратного підрозділу» на

інструмент інтелектуальної підтримки бізнесу. Автоматизація та використання AI мінімізують ризики людських помилок, забезпечують 100% відповідність вимогам законодавства та створюють умови для безпечного масштабування підприємства на міжнародних ринках.

ВИСНОВКИ

У ході виконання курсової роботи було проведено комплексне теоретичне та прикладне дослідження механізмів побудови системи протидії відмиванню коштів на рівні сучасного підприємства. Отримані результати дозволяють сформулювати наступні узагальнюючі висновки:

1. Трансформація сутності легалізації доходів. Дослідження показало, що у період 2020–2026 рр. процеси відмивання коштів остаточно втратили суто банківський характер, перетворившись на загрозу для реального сектора економіки. Інтеграція віртуальних активів, зокрема використання стейблкоїнів та біткоїна через децентралізовані платформи, вимагає від підприємств докорінного перегляду підходів до ідентифікації контрагентів. Встановлено, що класична тріада Протидії Відмиванню Коштів - розміщення, розшарування, інтеграція сьогодні дедалі частіше реалізується за допомогою цифрових інструментів, що ускладнює роботу комплаєнс-підрозділів.

2. Гармонізація з європейськими стандартами. Проведений порівняльний аналіз IV, V та VI Директив ЄС підтвердив, що українське законодавство (зокрема Закон № 361-IX) успішно імплементувало ключові вимоги щодо прозорості бенефіціарного володіння та ризик-орієнтованого підходу. Для українських підприємств це означає необхідність дотримання міжнародних стандартів «належної обачності» як обов'язкової умови для збереження доступу до зовнішніх ринків капіталу та співпраці з іноземними партнерами.

3. Вплив воєнного стану та національна безпека. Ключовим результатом роботи є аналіз функціонування системи ПВК в умовах повномасштабної збройної агресії РФ проти України. Встановлено, що воєнний стан докорінно змінив пріоритети фінансового моніторингу:

— Санкційний комплаєнс: став пріоритетним напрямом, що вимагає від підприємств негайного розірвання зв'язків із будь-якими особами чи структурами, що мають «російський чи білоруський слід».

— Фінансування тероризму: виявлено нові ризики, пов'язані з використанням криптоактивів та волонтерських зборів для приховування фінансування колабораційної діяльності та нелегальних збройних формувань.

— Державний контроль: доведено, що воєнний стан не лише не послабив вимоги Протидії Відмиванню Коштів, а навпаки — посилив відповідальність бізнесу за чистоту фінансових потоків, оскільки ефективна боротьба з відмиванням коштів є невід'ємною частиною економічного спротиву ворогу.

4. Практична цінність автоматизації. У другому розділі обґрунтовано, що реалізація ризик-орієнтованого підходу неможлива без використання сучасного програмного забезпечення. Порівняльний аналіз систем YouControl та AMLBot продемонстрував, що автоматизація дозволяє скоротити час на верифікацію клієнта на 80-90% та мінімізувати ризик людської помилки. Впровадження розробленого автором алгоритму та «Проекту положення про службу ПВК» (Додаток А) забезпечує підприємству системний контроль: від першого контакту з клієнтом до постійного моніторингу його операцій.

5. Перспективи та інновації. Резюмовано, що подальший розвиток систем ПВК на підприємствах пов'язаний із впровадженням Штучного Інтелекту та технології Fuzzy Logic для виявлення прихованих зв'язків між суб'єктами господарювання. Це дозволить прогнозувати ризики ще на етапі підготовки контрактів, що є критично важливим для збереження фінансової стійкості та ділової репутації підприємства у повоєнний період відновлення України.

Таким чином, розроблена система протидії відмиванню коштів у сучасних реаліях є не просто бюрократичною вимогою, а потужним стратегічним інструментом економічної безпеки, що захищає підприємство від санкційних ризиків, кримінальної відповідальності та сприяє очищенню національної економіки від кримінальних капіталів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.

1. Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення: Закон України від 06.12.2019 № 361-IX. Редакція від 01.01.2025.
2. Гуржій Т. О. *Фінансовий контроль та моніторинг: правовий аспект*. Навчальний посібник. Київ: Юрінком Інтер, 2022. 312 с.
3. Живко З. Б. *Економічна безпека підприємства: комплаєнс-підхід*. Львів: Растр-7, 2021. 240 с.
4. Бойко С. М. Трансформація критеріїв ризик-орієнтованого підходу в умовах воєнного стану. *Фінанси України*. 2023. № 8. С. 12–25.
5. FATF (2023), *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation*, FATF, Paris, France. URL: www.fatf-gafi.org.
6. Директива (ЄС) 2024/1640 Європейського Парламенту та Ради від 31 травня 2024 року про механізми запобігання використанню фінансової системи для відмивання коштів.
7. Державна служба фінансового моніторингу України. *Звіт про проведення Національної оцінки ризиків у сфері ПВК/ФТ 2023-2024*. URL: <https://fiu.gov.ua>.
8. Ковальчук А. Т. *Фінансове право України: підручник*. Київ: Знання, 2023. 450с.
9. Резнік О. М. *Адміністративно-правове забезпечення фінансового моніторингу в Україні*. Суми: СумДУ, 2021. 380 с.
10. Фоміна О. В. *Облік і аудит у системі ПВК/ФТ: сучасні виклики*. Харків: Право, 2024. 215 с.
11. Безпалько О. В. Використання штучного інтелекту в системах автоматизації фінансового моніторингу. *Економіка та держава*. 2024. № 3. С. 45–51.
12. Котляревська О. А. Особливості ідентифікації PEPs: нові законодавчі вимоги 2024 року. *Юридичний радник*. 2024. № 1.

13. Мельник Т. Г. Ризики використання віртуальних активів у схемах легалізації доходів. *Наукові записки НаУКМА*. 2023. Т. 8.
14. Петренко В. І. Комплаєнс-офіцер як ключова фігура внутрішнього контролю. *Вісник економічної науки України*. 2022. № 2.
15. Савченко Л. А. Співпраця Держфінмоніторингу з Егмонтською групою. *Право та державне управління*. 2024. № 2.
16. Ткаченко Р. В. Санкційний комплаєнс: інтеграція списків OFAC та РНБО. *Бізнес Інформ*. 2023. № 11.
17. Шевченко О. О. Автоматизація KYC процедур за допомогою технології блокчейн. *Цифрова економіка*. 2025. № 1.
18. Ющенко Г. О. Проблеми перевірки кінцевих бенефіціарних власників. *Зовнішня торгівля: економіка, фінанси, право*. 2023. № 4.
19. Ярема Н. М. Методи оцінки ефективності системи ПВК на підприємствах. *Менеджмент та підприємництво в Україні*. 2024. № 5.
20. Положення про здійснення установами фінансового моніторингу: Постанова Правління НБУ від 28.07.2020 № 107.
21. Transparency International Ukraine. *Аналіз прозорості реєстрів бенефіціарних власників (2024)*. URL: <https://ti-ukraine.org>.
22. FATF. *Guidance on the Risk-Based Approach to Virtual Assets*. 2023 update.
23. Офіційний сайт Егмонтської групи (Egmont Group). *Case Studies 2023-2024*. URL: <https://egmontgroup.org>.
24. Регламент (ЄС) 2023/1113 про інформацію, що супроводжує перекази криптоактивів.
25. Кримінальний кодекс України: Закон України від 05.04.2001 № 2341-III (із змінами 2024 р.

ДОДАТКИ

ДОДАТОК А

ПРОЕКТ ПОЛОЖЕННЯ

про службу фінансового моніторингу (комплаєнс-підрозділ) ТОВ «[Назва підприємства]»

1. Загальні положення 1.1. Це Положення визначає правовий статус, завдання, функції, а також права та обов'язки служби фінансового моніторингу (далі — Служба) ТОВ «[Назва підприємства]» (далі — Підприємство). 1.2. Служба є самостійним структурним підрозділом, що підпорядковується безпосередньо керівнику Підприємства або Наглядовій раді. 1.3. У своїй діяльності Служба керується Конституцією України, Законом України «Про запобігання та протидію легалізації (відмиванню) доходів...» № 361-ІХ, нормативно-правовими актами НБУ, Держфінмоніторингу та цим Положенням. 1.4. Очолює Службу відповідальний працівник — Комплаєнс-офіцер, який призначається на посаду наказом керівника.

2. Забезпечення незалежності Служби та Комплаєнс-офіцера 2.1. Незалежність Служби забезпечується шляхом виключення втручання будь-яких осіб у процес підготовки висновків та звітів про підозрілі фінансові операції. 2.2. Комплаєнс-офіцер має право прямого доступу до вищих органів управління Підприємства. 2.3. Забороняється суміщення посади в Службі з функціями, що створюють конфлікт інтересів (бухгалтерія, юридичний супровід угод). 2.4. Підприємство забезпечує Службу технічними ресурсами для доступу до санкційних списків та автоматизованих систем перевірки (YouControl, AMLBot тощо).

3. Основні завдання та функції 3.1. Розробка та регулярне оновлення Внутрішніх правил фінансового моніторингу. 3.2. Проведення ідентифікації та верифікації клієнтів (процедури KYC/KYB). 3.3. Впровадження ризик-орієнтованого підходу та класифікація клієнтів за рівнями ризику. 3.4. Виявлення операцій, що підлягають обов'язковому моніторингу, та повідомлення про них Державної служби фінансового моніторингу України. 3.5. Моніторинг операцій на предмет зв'язку з державою-агресором або підсанкційними особами в умовах воєнного стану. 3.6. Організація щорічного навчання та інструктажів для працівників Підприємства.

4. Права та обов'язки Комплаєнс-офіцера

4.1. Права:

- Отримувати від підрозділів документи, необхідні для перевірки походження коштів клієнта.
- Приймати рішення про відмову у встановленні ділових відносин у разі виявлення високого ризику.
- Самостійно приймати рішення про подання інформації про підозрілі операції до регулятора.

4.2. Обов'язки:

- Забезпечувати конфіденційність факту перевірки операцій (принцип «Anti-tipping off»).
- Проводити регулярну переоцінку ризиків діяльності Підприємства.
- Зберігати документи щодо ідентифікації клієнтів протягом терміну, встановленого законом (не менше 5 років).

5. Відповідальність

5.1. Служба несе відповідальність за належне виконання функцій суб'єкта первинного фінансового моніторингу. 5.2. Комплаєнс-офіцер несе персональну відповідальність за несвоєчасне повідомлення про підозрілі операції згідно з чинним законодавством України.

«ЗАТВЕРДЖЕНО:

Директор ТОВ [Назва] _____ (Прізвище)».