Узагальнення міжнародного досвіду застосування цифрових технологій у протидії фінансовій злочинності та оцінка можливості його адаптації в українських реаліях*

Литвиненко Євгенія Віталіївна[1]

Опубліковано	Секція	УДК
30.10.2025	Право	343.37:004:336.74(100)(477)

DOI: https://doi.org/10.5281/zenodo.17864535

Анотація. Стаття присвячена комплексному аналізу міжнародного досвіду застосування цифрових технологій у протидії фінансовій злочинності та оцінці можливості його адаптації в українських реаліях. Актуальність дослідження зумовлена стрімкою цифровізацією фінансового сектору, появою криптовалют та децентралізованих платформ, що створило принципово нові виклики для виявлення та запобігання відмиванню коштів. У роботі досліджено європейський підхід до регулювання штучного інтелекту у фінансовому секторі на основі принципу оцінки ризиків, проаналізовано роль GDPR у забезпеченні прозорості автоматизованого прийняття рішень та захисту персональних даних. Систематизовано основні цифрові технології протидії фінансовій злочинності, включаючи блокчейн-аналітику, біометричну верифікацію, автоматизовані системи моніторингу транзакцій та RegTech-рішення. Обґрунтовано значний потенціал України для адаптації міжнародного досвіду завдяки успішному функціонуванню системи Дія, розвитку IT-сектору та входженню до топ-10 країн за обсягом криптовалютних операцій. Ідентифіковано ключові виклики адаптації, включаючи обмежені фінансові ресурси, недосконалість законодавства та виклики воєнного стану. Надано практичні рекомендації щодо поетапного впровадження цифрових технологій через розробку національної стратегії, удосконалення законодавчої бази та забезпечення міжвідомчої координації.

Ключові слова: фінансова злочинність, цифрові технології, штучний інтелект, блокчейн-аналітика, криптовалюти, GDPR, RegTech, протидія відмиванню коштів, біометрична верифікація, фінансовий моніторинг.

Generalization of international experience in applying digital technologies to combat financial crime and assessment of the possibility of its adaptation in ukrainian realities

Annotation. The article is devoted to a comprehensive analysis of international experience in applying digital technologies to combat financial crime and assessment of the possibility of its adaptation in Ukrainian realities. The research relevance is determined by the rapid digitalization of the financial sector, the emergence of virtual assets, cryptocurrencies and

* *Робота виконана в рамках проекта «Інтеграційна парадигма цифрової трансформації в системі протидії фінансовій злочинності: синергетичний підхід до превенції та боротьби» (номер державної реєстрації 0125U000602*

[1] доктор філософії зі спеціальності 081 Право, асистент кафедри кримінально-правових дисциплін та судочинства ННІ права, Сумський державний університет, ORCID: https://orcid.org/0000-0002-4735-3722

decentralized platforms, which have created fundamentally new challenges for combating financial crime due to transaction pseudonymity, the decentralized nature of blockchain networks and the cross-border nature of digital asset operations.

The work analyzes the European approach to regulating artificial intelligence in the financial sector, based on the risk assessment principle, which ensures a balance between stimulating innovation and protecting user rights. The GDPR provisions on automated decision-making are examined in detail, including requirements for transparency in processing personal data and the right to human review of decisions. The main digital technologies for combating financial crime are systematized: blockchain analytics for tracking cryptocurrency transactions, biometric verification for customer identification procedures, automated transaction monitoring systems in real-time, RegTech solutions for compliance automation, and international information exchange systems.

A critical assessment of Ukraine's readiness to implement advanced technologies has been conducted, taking into account the successful functioning of the Diia system, the development of Diia.City, high level of mobile technology penetration, and the country's entry into the top 10 in terms of cryptocurrency transaction volume. Key adaptation challenges have been identified: limited financial resources, imperfect legislation in the field of artificial intelligence and virtual assets, insufficient coordination between regulatory authorities, uneven level of digital literacy, and additional challenges of martial law. Practical recommendations for phased implementation of digital technologies have been developed, including the need to develop a national strategy, improve the legislative framework in accordance with GDPR standards, introduce pilot projects, create specialized training programs, and ensure a balance between control effectiveness and protection of citizens' personal data.

Keywords: financial crime, digital technologies, artificial intelligence, blockchain analytics, cryptocurrencies, GDPR, RegTech, anti-money laundering, biometric verification, financial monitoring.

Вступ

Стрімка цифровізація фінансового сектору, поява віртуальних активів, криптовалют та децентралізованих платформ створили принципово нові виклики для протидії фінансовій злочинності. Традиційні методи виявлення та запобігання відмиванню коштів виявилися недостатньо ефективними в умовах псевдонімності транзакцій, децентралізованого характеру блокчейн-мереж та транскордонної природи операцій з цифровими активами.

Водночас розвинені країни активно впроваджують передові цифрові технології – штучний інтелект, блокчейн-аналітику, біометричну верифікацію, автоматизовані системи моніторингу та RegTech-рішення – для ефективної боротьби з фінансовими злочинами. Проте відставання державного нагляду від темпів технологічних змін, відсутність уніфікованих підходів до регулювання та складність адаптації міжнародного досвіду до національних реалій створюють серйозні перешкоди для створення ефективних систем протидії фінансовій злочинності.

Для України, яка входить до топ-10 країн за обсягом операцій з криптовалютами та демонструє високу готовність до цифровізації, питання адаптації міжнародного досвіду застосування цифрових технологій у протидії фінансовій злочинності набуває особливої актуальності в контексті євроінтеграції, модернізації фінансового сектору та необхідності відповідності міжнародним стандартам.

Аналіз останніх досліджень і публікацій. Аналіз наукових досліджень свідчить про зростаючий інтерес до застосування цифрових технологій у протидії фінансовій злочинності. Дослідження у цій сфері мають міждисциплінарний характер та охоплюють

як технологічні, так і правові аспекти регулювання фінансового сектору в умовах цифровізації.

Єфремова К.В. досліджує правові аспекти застосування ШІ у фінансовому секторі ЄС, підкреслюючи необхідність балансу між інноваціями та захистом прав споживачів. Нормативну основу формує GDPR, який регулює автоматизоване прийняття рішень та обробку персональних даних.

Truby J., Brown R. та Dahdal A. обґрунтовують потребу проактивного регулювання ШІ, наводячи приклади упередженості алгоритмів. Marous J. аналізує трансформаційний вплив ШІ на банківську індустрію. Біла книга Європейської Комісії 2020 року пропонує регуляторну модель на основі оцінки ризиків.

Головко К.В. досліджує правила AML, розглядаючи блокчейн-аналітику, біометричну верифікацію та автоматизований моніторинг транзакцій, підкреслюючи важливість захисту приватності.

Метою статті є комплексний аналіз міжнародного досвіду застосування цифрових технологій у протидії фінансовій злочинності, виявлення основних стратегічних викликів та способів їх подолання, а також оцінка можливості адаптації передових технологічних рішень в українських реаліях з урахуванням національних особливостей, наявних ресурсів та існуючих обмежень.

Завдання статті є наступними: проаналізувати роль штучного інтелекту у фінансовому секторі та особливості його регулювання в ЄС, систематизувати основні цифрові технології протидії фінансовій злочинності, вивчити міжнародні підходи до регулювання FinTech, та застосування цифрових технологій у фінансових послугах, зокрема практики FCA, PRA, оцінити готовність України до впровадження передових технологій, ідентифікувати ключові виклики адаптації міжнародного досвіду, розробити практичні рекомендації щодо поетапного впровадження цифрових технологій в Україні.

Результати

Цифрова ера відкриває нові горизонти для бізнесу, де технології стають ключовими партнерами, трансформуючи традиційні методи ведення справ і прийняття рішень. Штучний інтелект швидко впливає на фінансовий сектор, пропонуючи численні переваги для вдосконалення послуг і забезпечення відповідності нормам. У цій галузі алгоритми ШІ вже відповідають за облік транзакцій, виявлення шахрайських дій, перевірку платоспроможності клієнтів, планування ресурсів і підготовку звітів. Однак впровадження таких інструментів супроводжується новими загрозами. Метою є окреслення основних стратегічних викликів і способів їх подолання для створення ефективних систем використання ШІ на ринку фінансових послуг. Це включає розуміння ролі ШІ, потенційних ризиків у фінансах для подальшого регулювання та уникнення негативних наслідків.

Дослідження правового регулювання ШІ у різних галузях привертає увагу науковців з початку XXI століття, часто маючи міждисциплінарний характер. Значні ризики технологій ШІ та відставання державного нагляду стимулюють вивчення аспектів регулювання FinTech і застосування ШІ. Серед зарубіжних робіт варто відзначити публікації D.W. Arner, J. Barberis, R.P. Buckley про FinTech, RegTech і переосмислення фінансового регулювання; праці Jon Truby, Rafael Brown та Andrew Dahdal про банківські операції з ШІ та потребу в проактивному регулюванні ШІ у фінансах. Серед українських авторів виділяються дослідження О.А. Баранова про правове забезпечення інформаційної сфери, О.В. Вінник про регулювання цифровізації економіки, її переваги та ризики, а також І.В. Яковюка, А.П. Волошина та А.О. Шовкуна про протидію фішингу в ЄС; Н.Б. Пацурія про електронні страхові послуги.

Впровадження ШІ радикально змінює соціальне, політичне та економічне життя. Згідно зі звітом Econsultancy та Adobe «Цифрові тенденції фінансових послуг у 2018 році», майже 20% постачальників фінансових послуг глобально вже застосовують ШІ в операціях, а 41% планують це зробити незабаром [1]. Аналітика великих даних на базі ШІ дозволяє великим фінансовим провайдерам реагувати на споживчі та економічні тренди в реальному часі. Системи автоматизації комплаєнсу на ШІ зменшують витрати на юридичні відділи та ризики, знижуючи людські помилки. Застосування ШІ в банках і FinTech охоплює від клієнтських сервісів (чат-боти, персоналізований маркетинг) до внутрішніх процесів (автоматизація операцій, аналіз контрактів, управління ризиками).

FinTech охоплює технології, пов'язані з цифровізацією фінансових сервісів. З середини 90-х PayPal став піонером у платіжних рішеннях, а нині поширені онлайн-покупки та безконтактні платежі. Розвиток FinTech перейшов від електронних платежів до цифрового управління активами. Поява P2P-кредитування призвела до зростання компаній як Lufax і Lending Club, які є лідерами за капіталізацією. PayPal стикається з конкуренцією від Square, iZettle, Revolut. Далі FinTech еволюціонував до цифрового управління капіталом, де компанії фокусуються на персоналізації послуг відповідно до змінених уподобань споживачів [2].

Загалом FinTech означає цифрові фінансові послуги, інфраструктури для нових угод у банківській сфері, як кредитування, інвестиції, платежі. Інновації стимулюють нові ніші, як альтернативні фінанси, краудфандинг, P2P-кредити, роботизовані консультації та автоматизоване інвестування. Глобальне регулювання ШІ наразі на рівні політики. Попри консенсус щодо принципів управління ШІ, законодавці ще не перетворили їх на норми для фінансів. Межі регулювання залежать від застосування ШІ та ризиків.

Регулювання ризиків FinTech у Європі розподілене між наглядовими органами, вимагаючи міжсекторної співпраці. Зазвичай нагляд за FinTech покладено на автономні підрозділи з ресурсами для розробки норм і дослідження. Розглянемо застосування ШІ у фінансах для виявлення ризиків. ШІ сильний у постійному зборі даних: ширша база – ефективніша система. Банки впливають на клієнтську поведінку через великі дані, інтегруючи інформацію з соціальних мереж для персоніфікованих продуктів, що часто випереджають запити клієнтів.

25 травня 2018 року набув чинності GDPR ЄС [3], що застосовується безпосередньо в державах-членах відповідно до Договору про функціонування ЄС [4]. GDPR гарантує право на перегляд автоматизованих рішень людиною. Стаття 22 GDPR регулює автоматизоване прийняття рішень, включаючи профілювання, і стосується всіх, хто обробляє дані громадян ЄС [3, Art. 22]. Суб'єкт даних не підлягає рішенню виключно на автоматизованій обробці, якщо воно має юридичні наслідки, за винятком випадків договору, законодавства чи згоди. Поняття як «законний інтерес» ще розробляються.

Законодавство про захист даних ключове для ШІ у фінансових послугах клієнтам. Ризики: компанії не отримують згоду на дані з соціальних мереж, що може призвести до дискримінації. GDPR вимагає прозорої обробки, надання інформації про логіку використання даних і наслідки. Фінансові установи враховують право на компенсацію за порушення даних за GDPR і DPA 2018.

Щодо великих даних у Європі, FCA у бізнес-плані 2018/19 планував перегляд використання даних фірмами, включаючи машинне навчання, торгівлю та ШІ. Ризик упередженості даних може призводити до несправедливих рішень. У липні 2018 FCA та PSR відзначили приклади ШІ, що посилюють соціальне виключення, як скорочення кредитних лімітів при оплаті консультацій з розлучення [5]. Установи повинні моніторити використання особистої інформації.

Фінансові компанії стикаються з новими ризиками, що можуть призвести до втрат. Питання відповідальності: хто відповідає за помилки – спеціаліст, розробник чи орган,

що використовував ШІ. Приклад: алгоритм, навчений на історичних даних, може відмовляти кредитами жінкам з дітьми через упередженість вибірки.

Європейський досвід: PRA та FCA застосовують принципи регулювання до ШІ, наголошуючи на недопустимості залежності від автоматизації та недостатньому нагляді. Для робо-консультацій потрібен чіткий контроль і розподіл обов'язків. Для алгоритмічної торгівлі PRA може вимагати опис стратегій протягом 14 днів [6]. Це вимагає розуміння принципів ШІ.

ШІ використовується для чат-ботів, що відповідають на питання, формують портфелі, готують звіти. Питання відповідальності за помилки стосується всіх рішень ШІ.

Довго ЄС не мав спеціального регулювання ШІ. У червні 2018 створено AI HLEG для рекомендацій щодо надійності ШІ. 19 лютого 2020 Комісія видала «Білу книгу про штучний інтелект – європейський підхід до досконалості та довіри» [7], вимоги якої можуть стати основою законодавства, подібного до GDPR.

Побудова регуляторної інфраструктури вимагає співпраці політиків і експертів для управління ризиками ШІ в цифровій, фізичній, економічній та політичній сферах. Найактуальніші ризики: для прав, конфіденційності, безпеки, ефективності та відповідальності. Підхід до регулювання – на основі оцінки ризику, для пропорційного контролю без перешкод інноваціям. Замість окремих актів Комісія виклала вимоги для надійності ШІ з повагою до цінностей ЄС.

Розглянувши застосування штучного інтелекту у сфері фінансових послуг Європейського Союзу, доцільно розширити аналіз на інші цифрові технології, які активно використовуються на міжнародному рівні для протидії фінансовій злочинності. Якщо ШІ відіграє ключову роль у виявленні підозрілих операцій та автоматизації комплаєнс-процесів, то глобальна практика боротьби з відмиванням коштів демонструє комплексне застосування широкого спектру цифрових рішень.

Трансформація фінансового сектору через віртуальні активи, криптовалюти та децентралізовані платформи створила нові виклики для регуляторів та правоохоронних органів у всьому світі. Псевдонімність транзакцій, децентралізований характер блокчейн-мереж та транскордонна природа операцій з цифровими активами вимагають впровадження спеціалізованих технологічних інструментів, здатних ефективно виявляти та запобігати фінансовим злочинам.

Зі зростанням популярності віртуальних активів з'являються прогресивні технології для вирішення проблем протидії фінансовій злочинності. Серед найбільш перспективних напрямків можна виділити блокчейн-аналітику, яка використовується для відстеження та моніторингу криптовалютних транзакцій. Блокчейн-аналітика представляє собою спеціалізовані інструменти для аналізу транзакцій у блокчейн-мережах, які дозволяють відстежувати рух коштів, виявляти зв'язки між адресами гаманців та ідентифікувати підозрілі кластери активності. Рішення для моніторингу криптотранзакцій аналізують великі обсяги даних для виявлення потенційного відмивання коштів чи інших незаконних дій, допомагаючи установам та постачальникам послуг віртуальних активів дотримуватися регуляторних норм та повідомляти про підозрілі операції до відповідних органів.

Біометрична верифікація стала ще одним важливим технологічним рішенням у протидії фінансовій злочинності. Рішення для верифікації особи використовують біометричні технології, автоматизовану перевірку документів та блокчейн-платформи для ідентифікації користувачів, зберігаючи при цьому їхню приватність. Ці системи є критично важливими для забезпечення процедур "Знай свого клієнта" у цифровому фінансовому просторі, дозволяючи ефективно ідентифікувати клієнтів та запобігати використанню підроблених документів чи крадіжці ідентичності. Інтеграція таких

рішень у процедури протидії відмиванню забезпечує належну ідентифікацію користувачів та ефективний моніторинг операцій.

Системи автоматизованого моніторингу транзакцій відіграють ключову роль у виявленні підозрілих фінансових операцій. Ефективний моніторинг транзакцій передбачає впровадження автоматизованих систем для виявлення підозрілих дій в режимі реального часу, таких як незвично великі чи часті операції, операції зі структуруванням сум, або транзакції з високоризиковими юрисдикціями. Ці системи використовують комбінацію встановлених правил та алгоритмів для аналізу патернів поведінки користувачів, що може свідчити про відмивання коштів або фінансування тероризму. Моніторинг є особливо важливим для операцій з віртуальними активами через їх специфічні характеристики, включаючи швидкість проведення транзакцій, псевдонімність учасників та можливість здійснення операцій цілодобово без географічних обмежень.

Ведення детального обліку транзакцій є невід'ємною частиною системи протидії фінансовій злочинності. Детальний облік забезпечує прозорість операцій та полегшує проведення аудитів, розслідувань та регуляторної звітності, включаючи інформацію про суми транзакцій, дати проведення операцій, сторони угод та інші релевантні дані. Цифрові технології дозволяють автоматизувати процеси збору, зберігання та аналізу цієї інформації, забезпечуючи її доступність для уповноважених органів у випадку необхідності проведення розслідувань. Технологічні особливості блокчейн-мереж, такі як розподілена структура та незмінність записів, додають складності для традиційних методів обліку, що вимагає впровадження спеціальних технічних інструментів для забезпечення відповідності регуляторним вимогам без шкоди для безпеки та ефективності операцій з віртуальними активами.

Регуляторні технології, відомі як RegTech, представляють собою інноваційні рішення для автоматизації процесів комплаєнсу. Ці технології охоплюють широкий спектр функцій, включаючи автоматизацію звітності до регуляторних органів, управління змінами в регуляторних вимогах, автоматизовану оцінку ризиків клієнтів та цифровізацію документообігу. Інтеграція регуляторних технологій у процедури протидії фінансовій злочинності дозволяє зменшити витрати на комплаєнс, підвищити точність аналізу та забезпечити своєчасне реагування на нові загрози. З розвитком сфери віртуальних активів норми протидії відмиванню адаптуються до технологічних змін та нових ризиків, а регулятори працюють над створенням чітких правил для цього сектору.

Системи обміну інформацією та міжнародної співпраці є критично важливими для боротьби з транскордонною фінансовою злочинністю. Міжнародні організації надають рекомендації для протидії відмиванню у сфері віртуальних активів, а країни інтегрують ці рекомендації у національне законодавство для забезпечення відповідності глобальним стандартам. Обмін інформацією між агенціями, співпраця з міжнародними партнерами та координація зусиль на глобальному рівні допомагають ефективно виявляти та припиняти складні схеми відмивання коштів, які часто використовують криптовалюти через їх транскордонну природу. Перевірка гаманців, належна перевірка клієнтів, обмін інформацією та співпраця між різними учасниками фінансової екосистеми є ключовими елементами для забезпечення відповідності нормам протидії відмиванню у сфері віртуальних активів.

Технології захисту даних відіграють важливу роль у збалансуванні потреби у моніторингу фінансових операцій з правом користувачів на приватність. Баланс між приватністю та відповідністю регуляторним вимогам є делікатним питанням у криптоіндустрії: з одного боку, приватність є фундаментальною цінністю децентралізованих систем, але з іншого боку, вона може сприяти незаконним діям. Передові криптографічні технології дозволяють проводити аналіз транзакцій для

виявлення підозрілих операцій, зберігаючи при цьому конфіденційність персональних даних користувачів. Це особливо важливо у контексті впровадження процедур "Знай свого клієнта", які мають бути достатньо надійними для запобігання злочинам, але не надто обтяжливими для звичайних користувачів [8].

Міжнародний досвід застосування цифрових технологій у протидії фінансовій злочинності має значний потенціал для адаптації в українських реаліях, хоча й потребує врахування специфічних національних особливостей та поетапного впровадження.

Україна вже демонструє високу готовність до цифровізації, що підтверджується успішним функціонуванням системи електронного урядування Дія, розвитком Дія.Сіті як спеціального правового режиму для IT-бізнесу, та загальним високим рівнем проникнення мобільних технологій серед населення. Ці чинники створюють сприятливе середовище для впровадження передових технологій у фінансовому секторі. Крім того, український IT-сектор демонструє наявність кваліфікованих фахівців, здатних розробляти та впроваджувати складні технологічні рішення, а досвід боротьби з корупцією через електронні системи ProZorro та інші антикорупційні платформи свідчить про можливість успішної імплементації цифрових інструментів контролю.

Щодо конкретних технологій, описаних у статті, штучний інтелект може бути адаптований в українських банках та фінансових установах для автоматизації процесів виявлення шахрайських операцій, проте це потребує значних інвестицій у технічну інфраструктуру та навчання персоналу. Національний банк України вже впроваджує деякі елементи автоматизованого моніторингу, що може стати основою для розширення використання ШІ. Блокчейн-аналітика та моніторинг криптовалютних транзакцій є особливо актуальними для України, враховуючи зростаючу популярність криптовалют та віртуальних активів серед населення. Україна входить до топ-10 країн за обсягом операцій з криптовалютами, що робить впровадження спеціалізованих інструментів блокчейн-аналітики критично важливим завданням.

Біометрична верифікація вже частково використовується в Україні через систему BankID та біометричні паспорти, що створює хорошу базу для розширення застосування таких технологій у процедурах ідентифікації клієнтів фінансових установ. Системи автоматизованого моніторингу транзакцій можуть бути інтегровані у діяльність Держфінмоніторингу та комерційних банків, хоча це потребуватиме модернізації існуючих систем та забезпечення їх сумісності. RegTech-рішення для автоматизації комплаєнсу особливо актуальні для українських фінансових установ, які стикаються з необхідністю дотримання як національних, так і міжнародних регуляторних вимог, особливо в контексті євроінтеграції.

Проте існує ряд викликів, які потрібно враховувати при адаптації. Обмежені фінансові ресурси багатьох українських банків та фінансових установ можуть ускладнити впровадження дорогих технологічних рішень, особливо для малих та середніх гравців ринку. Українське законодавство у сфері штучного інтелекту, захисту даних та регулювання віртуальних активів потребує суттєвого доопрацювання для створення чіткої правової бази, аналогічної до європейського GDPR. Недостатня координація між різними регуляторними органами може створювати перешкоди для ефективного обміну інформацією та міжвідомчої співпраці у боротьбі з фінансовими злочинами.

Рівень цифрової грамотності серед населення та деяких представників фінансового сектору залишається нерівномірним, що може ускладнити широке впровадження складних технологічних рішень. Кіберзагрози та ризики витоку даних залишаються актуальними, особливо в умовах воєнного стану, що вимагає додаткових інвестицій у кібербезпеку. Воєнний стан та економічна нестабільність створюють додаткові виклики для довгострокового планування та інвестування у технологічну модернізацію фінансового сектору.

Для успішної адаптації доцільно розробити національну стратегію впровадження цифрових технологій у протидію фінансовій злочинності з чітким планом дій та етапами реалізації. Необхідно прийняти законодавство про штучний інтелект, удосконалити норми про захист персональних даних відповідно до стандартів GDPR, та створити чітке регулювання віртуальних активів та криптовалют. Запровадження пілотних проектів у великих банках та фінансових установах дозволить протестувати технології перед масовим впровадженням та виявити потенційні проблеми.

Важливим є створення спеціалізованих навчальних програм для фахівців фінансового сектору з питань використання цифрових технологій у протидії фінансовій злочинності, а також підвищення обізнаності населення щодо цифрових фінансових послуг та ризиків. Розвиток міжнародної співпраці, особливо з країнами ЄС, для обміну досвідом, технологіями та інформацією про фінансові злочини є критично важливим. Необхідно забезпечити належне фінансування через державний бюджет, міжнародну технічну допомогу та залучення приватних інвестицій у модернізацію фінансового сектору.

Створення спеціалізованої платформи для координації дій між Національним банком України, Держфінмоніторингом, правоохоронними органами та фінансовими установами підвищить ефективність боротьби з фінансовою злочинністю. Особлива увага має приділятися захисту персональних даних при впровадженні технологій моніторингу та аналізу, забезпеченню балансу між ефективністю контролю та правом на приватність громадян.

Досвід ЄС щодо регулювання штучного інтелекту, зокрема підхід на основі оцінки ризиків, може бути взятий за основу при розробці українського законодавства, що дозволить уникнути надмірного регулювання, яке може загальмувати інновації, водночас забезпечуючи належний контроль над високоризиковими застосуваннями ШІ. Європейський досвід застосування GDPR демонструє важливість балансу між інноваціями та захистом прав громадян, що є актуальним для України в контексті євроінтеграційних прагнень.

Загалом, адаптація міжнародного досвіду застосування цифрових технологій у протидії фінансовій злочинності в Україні є не лише можливою, але й необхідною для модернізації фінансового сектору, підвищення його стійкості до загроз та забезпечення відповідності міжнародним стандартам. Успіх цього процесу залежатиме від політичної волі, достатнього фінансування, якісного законодавчого забезпечення та ефективної координації між усіма зацікавленими сторонами. Поетапний підхід з урахуванням національних особливостей та наявних ресурсів дозволить мінімізувати ризики та максимізувати позитивний ефект від впровадження передових технологій у боротьбі з фінансовою злочинністю.

Висновки

Дослідження міжнародного досвіду застосування цифрових технологій у протидії фінансовій злочинності дозволяє зробити наступні висновки. Європейський Союз формує комплексний підхід до регулювання штучного інтелекту у фінансовому секторі на основі принципу оцінки ризиків, що дозволяє забезпечити баланс між стимулюванням інновацій та захистом прав користувачів. GDPR встановлює важливі гарантії щодо автоматизованого прийняття рішень, вимагаючи прозорості обробки даних та права на перегляд рішень людиною, що є критично важливим для застосування ШІ у фінансових послугах. Ефективна протидія фінансовій злочинності в сучасних умовах вимагає комплексного застосування широкого спектру цифрових технологій, включаючи блокчейн-аналітику для відстеження криптовалютних транзакцій, біометричну верифікацію для процедур "Знай свого клієнта", автоматизовані системи моніторингу транзакцій в режимі реального часу, RegTech-рішення для автоматизації

комплаєнсу та системи міжнародного обміну інформацією. Україна демонструє значний потенціал для адаптації міжнародного досвіду, що підтверджується успішним функціонуванням системи Дія, розвитком Дія.Сіті, високим рівнем проникнення мобільних технологій, наявністю кваліфікованих ІТ-фахівців та досвідом впровадження електронних антикорупційних платформ. Входження України до топ-10 країн за обсягом операцій з криптовалютами робить впровадження спеціалізованих інструментів блокчейн-аналітики критично важливим завданням. Проте адаптація міжнародного досвіду стикається з низкою об'єктивних обмежень, включаючи обмежені фінансові ресурси багатьох українських фінансових установ, недосконаліть законодавства у сфері ШІ та віртуальних активів, недостатню координацію між регуляторними органами, нерівномірний рівень цифрової грамотності, кіберзагрози та додаткові виклики, пов'язані з воєнним станом. Успішна адаптація потребує поетапного підходу, що включає розробку національної стратегії, удосконалення законодавчої бази відповідно до стандартів GDPR, запровадження пілотних проектів у великих банках, створення спеціалізованих навчальних програм, розвиток міжнародної співпраці, забезпечення належного фінансування та створення платформи координації між усіма зацікавленими сторонами. Критично важливим є забезпечення балансу між ефективністю технологічного контролю та захистом персональних даних і права на приватність громадян, оскільки європейський досвід демонструє, що запобігання надмірному регулюванню при одночасному забезпеченні належного контролю над високоризиковими застосуваннями ШІ є запорукою успішної цифровізації фінансового сектору. Загалом, адаптація міжнародного досвіду застосування цифрових технологій у протидії фінансовій злочинності в Україні є не лише можливою, але й необхідною для модернізації фінансового сектору, підвищення його стійкості до загроз та забезпечення відповідності міжнародним стандартам у контексті євроінтеграційних прагнень, при цьому успіх цього процесу залежатиме від політичної волі, достатнього фінансування, якісного законодавчого забезпечення та ефективної координації між усіма зацікавленими сторонами.

Список використаних джерел

1. Опитування українських банків та фінтехкомпаній - 2019. Проект USAID «Трансформація фінансового сектору». 2019. URL: http://www.fst-ua.info/wp-content/uploads/2019/12/FinTech-Survey-Report_UKR_12-12-2019.pdf
2. Єфремова К.В. Особливості застосування штучного інтелекту у сфері фінансових послуг: досвід ЄС. Право та інноваційне суспільство. 2020. № 1 (14). С. 66-71.
3. Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union. 2016. (L 119) 1. URL: http://eur-lex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN
4. Consolidated Version of the Treaty on the Functioning of the European Union. Official Journal of the European Union. 2016. (C 202) 1. URL: https://eurlex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12016E/TXT&from=EN
5. Truby J., Brown R., Dahdal A. Banking on AI: mandating a proactive approach to AI regulation in the financial sector. Law and Financial Markets. 2020. Volume 14. Issue 2. URL: https://www.tandfonline.com/doi/full/10.1080/17521440.2020.1760454
6. Marous J. AI Could Destroy Traditional Banking As We Know It. 2018. URL: https://thefinancialbrand.com/74626/ai-transform-disrupt-banking-financial-wef-trends-analysis/

7. White paper. On Artificial Intelligence - A European approach to excellence and trust. European Commission. Brussels, 19.02.2020 COM(2020) 65 final. URL: https://ec.europa.eu/info/sites/info/files/commission-white-paperartificial-intelligence-feb2020_en.pdf
8. Головко К.В. Правила AML як інструмент боротьби з відмиванням грошей. Юридичний науковий електронний журнал. 2024. № 7. С. 618-621.