

UDC 330.1:336.7
DOI: 10.24025/2306-4420.76(3).2025.342564

JEL Classification Code: M 41, H83, M 15
Article's History:
Received: 21.05.2025; Revised: 29.05.2025; Accepted: 04.06.2025.

Denys Shcherbatykh*

Candidate of Economic Sciences, Associate Professor
Private Higher Education Establishment “European University”
03115, 16V, Academician Vernadsky Blvd., Kyiv, Ukraine
<https://orcid.org/0000-0003-0990-8376>

Application of remote identification and verification of customers to improve the quality of financial monitoring

Abstract. The article examines methods of remote identification and verification in the process of implementing customer due diligence measures, conducted by primary financial monitoring entities. The relevance of the topic is due to the general digitalisation of financial services and the necessity to reduce compliance costs for reporting institutions. The purpose of the work was to single out the main methods for remote identification and verification of customers that can increase the effectiveness of the anti-money laundering and counter-terrorist financing system. The study uses the methods of analysis and synthesis, comparison, the dialectical method of cognition and the method of generalisation. The nature of the requirements applied to financial institutions in Ukraine during video verification of customers, which can be divided into technical, legal and procedural ones, is classified. The main requirements that allow the use of other comprehensive remote verification models are analysed. A new model for customer identification and verification is proposed, since current operational schemes are unable to solve two main problems of market participants. These problems are the high cost of the customer due diligence procedure and the necessity to carry out identification and verification measures every time a customer wishes to use the services of a financial institution where he/she has not been previously identified. A possible mechanism for conducting customer due diligence using blockchain-based distributed ledger technology is revealed, and the main range of problems, without the solution of which the transition to such a fundamentally new system of interaction between customers and financial institutions is impossible, is outlined. These problems include determining the identification institutions, system administrators, quality control of conducted inspections, list of documents that identify a person, storage of identification data and payment for services of institutions that identify the person. Prospects for further research are related to an in-depth analysis of each group of problems that constrain the transition of the national financial monitoring system to the implementation of customer identification and verification measures by blockchain-based reporting institutions

Keywords: customer due diligence, video verification, primary financial monitoring, anti-money laundering and counter-terrorist financing system, distributed ledger technology, blockchain

*Corresponding author



Денис Щербатих

Кандидат економічних наук, доцент

ПВНЗ «Європейський університет»

03115, бульв. Академіка Вернадського, 16В, м. Київ, Україна

<https://orcid.org/0000-0003-0990-8376>

Застосування дистанційної ідентифікації та верифікації клієнтів для покращення якості фінансового моніторингу

Анотація. У статті досліджуються методи дистанційної ідентифікації та верифікації в процесі здійснення суб'єктами первинного фінансового моніторингу заходів належної перевірки клієнтів. Актуальність теми зумовлена загальною цифровізацією фінансових послуг та необхідністю зниження витрат звітних установ на комплаєнс. Метою роботи є виокремлення головних способів ідентифікації та верифікації клієнтів у дистанційному режимі, що здатні підвищити ефективність системи протидії відмиванню злочинних коштів та фінансуванню тероризму. В дослідженні використано методи аналізу та синтезу, порівняння, діалектичний метод пізнання, метод узагальнення. Класифіковано характер вимог, що застосовуються до фінансових установ в Україні під час проведення відеоверифікації клієнтів, які можна розділити на технічні, правові та процедурні. Проаналізовано основні вимоги, які дозволяють використання інших повноцінних моделей дистанційної верифікації. Запропоновано нову модель ідентифікації та верифікації клієнтів, оскільки поточні операційні схеми не здатні вирішити дві основні проблеми учасників ринку. Ці проблеми полягають у високій вартості процедури належної перевірки клієнта та необхідності проведення заходів з ідентифікації та верифікації кожного разу, коли клієнт бажає скористатися послугами фінансової установи, де його не було ідентифіковано. Розкрито можливий механізм проведення належної перевірки клієнта з використанням технології розподіленого реєстру на основі блокчейну, а також окреслено основне коло проблем, без вирішення яких неможливий перехід до такої принципово нової системи взаємодії між клієнтами та фінансовими установами. До цих проблем належать визначення установ-ідентифікаторів, адміністраторів системи, контроль якості проведених перевірок, перелік документів, що ідентифікують особу, зберігання ідентифікаційних даних та оплата послуг установ, що ідентифікують особу. Перспективи подальших досліджень пов'язані з поглибленим аналізом кожної групи проблем, які стримують перехід національної системи фінансового моніторингу до здійснення заходів ідентифікації та верифікації клієнтів звітними установами на основі блокчейну

Ключові слова: належна перевірка клієнтів, відеоверифікація, первинний фінансовий моніторинг, система протидії відмиванню злочинних коштів та фінансуванню тероризму, технологія розподіленого реєстру, блокчейн

Вступ

Функціонування суб'єктів первинного фінансового моніторингу є неможливим без обслуговування клієнтів, передумовою здійснення якого є виконання всіх вимог стосовно їх ідентифікації та верифікації. Така регуляторна вимога реалізується установами шляхом отримання ідентифікаційних даних клієнта та перевірки їх належності відповідній особі. Традиційний ручний процес перевірки є застарілим, витратним за часом і коштами та схильним до помилок. Використання способів, що ґрунтуються на віддаленій верифікації, дозволяє прискорити належну перевірку при одночасному зниженні витрат фінансових установ. Дослідження цих способів дасть змогу не тільки оптимізувати процеси на рівні організації, а й загалом покращити ефективність національної системи фінансового моніторингу.

Огляд літератури

Проблемам оптимізації процесів, пов'язаних із виконанням вимог щодо належної перевірки клієнтів, присвячено праці багатьох вітчизняних та зарубіжних вчених. Так, М. В. Шевченко (2022) вивчав міжнародний досвід визначення фінансовою установою публічних діячів серед своїх клієнтів, N. K. Ostern та J. Riedel (2020) окреслили проблеми щодо зберігання клієнтських даних у блокчейні при первинному розміщенні монет, що є популярним способом залучення коштів, пов'язаних з криптовалютою. Р. Patil та М. Sangeetha (2022) розробили метод, при якому банки можуть контролювати якість ідентифікаційних даних, наданих клієнтом, та здійснювати розподіл витрат на належну перевірку. D. Fekete та Р. Bárkányi (2023) вивчали різні моделі штучного інтелекту, які б дозволяли ефективно розпізнавати дані шляхом обробки фотографій на ідентифікаційних документах клієнтів. Однак динаміка розвитку глобальних регулятивних технологій та специфіка використання віддалених методів належної перевірки в умовах української системи фінансового моніторингу вимагають здійснення нових досліджень.

Метою статті є визначення основних способів дистанційної ідентифікації та верифікації клієнтів, які б дозволили покращити ефективність системи фінансового моніторингу українських фінансових установ і національної системи фінансового моніторингу.

Результати дослідження

Базові вимоги щодо здійснення процесу ідентифікації та верифікації клієнтів (Know your customer – KYC) містяться в статтях 11-13 Закону України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення» (Верховна Рада України. (2019, Грудень 06) та ґрунтуються на рекомендаціях Групи з розробки фінансових заходів боротьби з відмиванням грошей (Financial Action Task Force on Money Laundering – FATF) № 10, 12, 13, 19, 22 (FATF, 2025, June). Суттю ідентифікації та верифікації є однозначне встановлення фінансовою установою особи клієнта та впевненість установи в тому, що клієнт не є самозванцем.

Ідентифікація вимагає надання клієнтом фінансовій установі своїх ідентифікаційних даних. Фінансова установа, отримавши ідентифікаційні документи клієнта, аналізує їх на предмет чинності та відповідності вимогам законодавства. Наступним етапом є підтвердження установою факту належності клієнту ідентифікаційних даних. Таке підтвердження вважається верифікацією особи. Процес KYC включає обмін документами між фінансовою установою та клієнтом, в межах якого суб'єкт первинного фінансового моніторингу зобов'язаний зібрати базову інформацію про клієнта та всіх його бенефіціарних власників з метою перевірки на наявність незаконної діяльності та виявлення «політично значущих осіб» (Politically exposed persons – PEPs). Процес також включає актуалізацію даних щодо поточних клієнтів фінансової установи через певні проміжки часу, які залежать від встановленого установою рівня ризику клієнта щодо відмивання коштів чи фінансування тероризму.

Вимоги здійснення належної перевірки клієнтів не є новими та містяться, наприклад, у Законі про банківську таємницю, прийнятому в США в 1970 р. (U.S. Financial Crimes Enforcement Network, n.d.). Однак закони про боротьбу з відмиванням грошей (Anti Money Laundering – AML) у різних юрисдикціях стають дедалі складнішими. Це знаходить своє відображення в переліках прийнятих ідентифікаційних документів, поділі клієнтів на різні типи, підвищенні технологічних вимог до процесу KYC. Разом з тим, процес ідентифікації та верифікації все ще значною мірою залежить від ручного опрацювання інформації співробітниками фінансових установ, що призводить до нестабільних результатів та значних витрат. Згідно з глобальними опитуваннями річна вартість процесу KYC для середнього міжнародного банку становить близько 60 млн. дол. США. Водночас 89 % опитаних клієнтів заявили, що мали негативний досвід щодо KYC (Thomson Reuters, 2016, May 09).

Іншим важливим елементом системи фінансового моніторингу, який робить тиск на фінансові установи, є можливість регуляторних органів застосовувати вагомні засоби впливу при невиконанні вимог належної перевірки клієнтів. При одночасному зростанні кількості та якості вимог до фінансових установ зростають і обсяги штрафів. У 2021 р. на учасників фінансового ринку в глобальному масштабі було накладено штрафів на 2,7 млрд. дол. США. У 2022 р. ця цифра становила вже 4,2 млрд. дол. США (Fenergo, 2022). Причому розмір штрафу для однієї фінансової установи може бути настільки суттєвим, що ставить під загрозу подальше її перебування на ринку. Наприклад, банк HSBC був оштрафований на 1,92 млрд. дол. США після виявлення, що через нього картель Sinaloa (Мексика) і картель Norte del Valle (Колумбія) відмили 881 млн. дол. США. ING Bank сплатив 619 мдн. дол. США штрафів за порушення санкційних вимог (Moyano & Ross, 2017).

Ситуацію з перевіркою клієнтів ускладнює глобальна цифровізація фінансової сфери, наслідком якої є невпинне зростання кількості фінансових операцій та обсягу здійснюваних трансакцій. Цей тренд можна простежити навіть в Україні в часи воєнного стану на прикладі статистики Системи електронних платежів Національного банку України (рисунок 1).

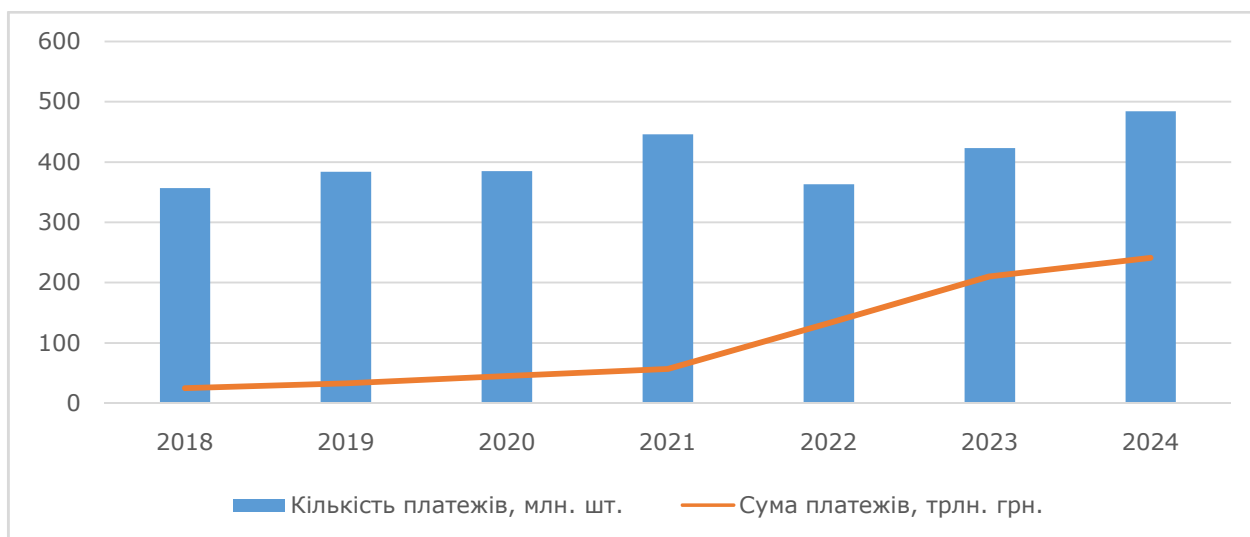


Рисунок 1. Обсяги платежів, здійснених через СЕП НБУ з 2018 по 2024 рр.

Джерело: побудовано автором за (Національний банк України, 2025, Травень)

Для спрощення підходу до процесу КУС була запроваджена можливість здійснення ідентифікації та верифікації клієнтів-фізичних осіб у віддаленому режимі. В українському правовому полі існують три моделі віддалених процедур КУС, які можна використовувати незалежно від суми фінансової операції та встановленого ризику ділових відносин: відеоверифікація, використання системи «ДІЯ», застосування Системи BankID від Національного банку України (Національний банк України, 2020, Травень 19; Національний банк України, 2020, Липень 28).

При здійсненні відеоверифікації фінансова установа для верифікації клієнта використовує режим відеотрансляції. Під час такої верифікації власник документа пред'являє оригінал ідентифікаційного документа співробітнику установи, дотримуючись при цьому вимог, які встановлені нормативно-правовими актами регуляторних органів у сфері фінансового моніторингу. При виконанні вищевказаних вимог процес відеоверифікації прирівнюється до верифікації, яка здійснюється в особистій присутності клієнта. Детальний опис українських регуляторних вимог до процесу відеоверифікації представлено в таблиці 1.

Таблиця 1. Вимоги до здійснення відеоверифікації

Вид вимоги	Характер вимоги
Технічні вимоги	якісна аудіовізуальна інформація (обмеження на рух інших осіб у зоні камери або наявності стороннього шуму)
	унеможливлення спостереження за відеоверифікацією третіх осіб
	цілісність та конфіденційність інформації, що передається між працівником фінансової установи та клієнтом
	відсутність перерв при проведенні відеоверифікації
	вимоги до зображення та звуку при відеотрансляції
	забезпечення резервного зберігання записів відеотрансляції
Юридичні вимоги	отримання згоди клієнта на проведення та запис відеоверифікації
	перевірка захисних елементів ідентифікаційних документів клієнта
	накладення КЕП на отримані від клієнта електронні копії документів
Процедурні вимоги	передбачення різних варіантів спілкування
	озвучення клієнтом фінансового номеру телефону та правильне введення отриманого пароля, що надсилається на такий номер телефону
	здійснення фотофіксації клієнта
	перевірка ідентифікаційного документа
	перевірка відсутності тиску на клієнта з боку третьої особи при здійсненні відеоверифікації

Джерело: розроблено автором за (Національний банк України, 2020, Травень 19; Національний банк України, 2020, Липень 28)

Відеоверифікація допомагає пришвидшити процес КУС та зробити його менш затратним. Водночас, вона не усуває необхідності спілкування між клієнтом та представником фінансової установи. Відповідно залишаються всі основні проблеми, пов'язані з традиційним здійсненням заходів належної перевірки: клієнт має підготувати документи для верифікації, установа має утримувати штат співробітників для перевірки даних, комунікація між клієнтом та фінансовою установою можлива лише в робочий час. Логічним розвитком відеоверифікації стало впровадження процедур, які б уможливили дистанційну процедуру КУС без прямої взаємодії клієнта та установи. Прикладом такого процесу є використання Державного підприємства «ДІА». Для цього фінансова установа має отримати від клієнта електронний паспорт або електронний паспорт для виїзду за кордон, який завірений кваліфікованою електронною печаткою від Державного підприємства «ДІА». Також фіксується кваліфікована електронна позначка часу, яка має відповідати даті здійснення установою верифікації клієнта. На додаток до отримання паспорта, фінансовій установі необхідно отримати копії ідентифікаційних документів клієнта або опитувальника, на які клієнт має накласти свій КЕП. Альтернативою надання копій документів є здійснення фотофіксації клієнта з використанням методів розпізнавання реальності з подальшим накладенням на таку фотографію КЕП працівника фінансової установи з кваліфікованою електронною позначкою часу.

Іншою повноцінною моделлю дистанційної верифікації є використання Системи BankID НБУ. Для використання такого методу фінансова установа через систему отримує ідентифікаційні дані клієнта. Після цього клієнт надсилає фінансовій установі копії своїх ідентифікаційних документів, на які ним було накладено КЕП. На завершальному етапі установа здійснює перевірку ідентифікаційних даних, які містяться в копіях документів, КЕП та файлі від Системи BankID НБУ, на їх відповідність.

Враховуючи відсутність обмежень щодо видів ідентифікаційних документів та широке проникнення банківських продуктів у сегмент клієнтів-фізичних осіб, використання дистанційної процедури КУС на основі Системи BankID НБУ має стабільну позитивну динаміку, візуалізація якої зображена на рисунку 2.

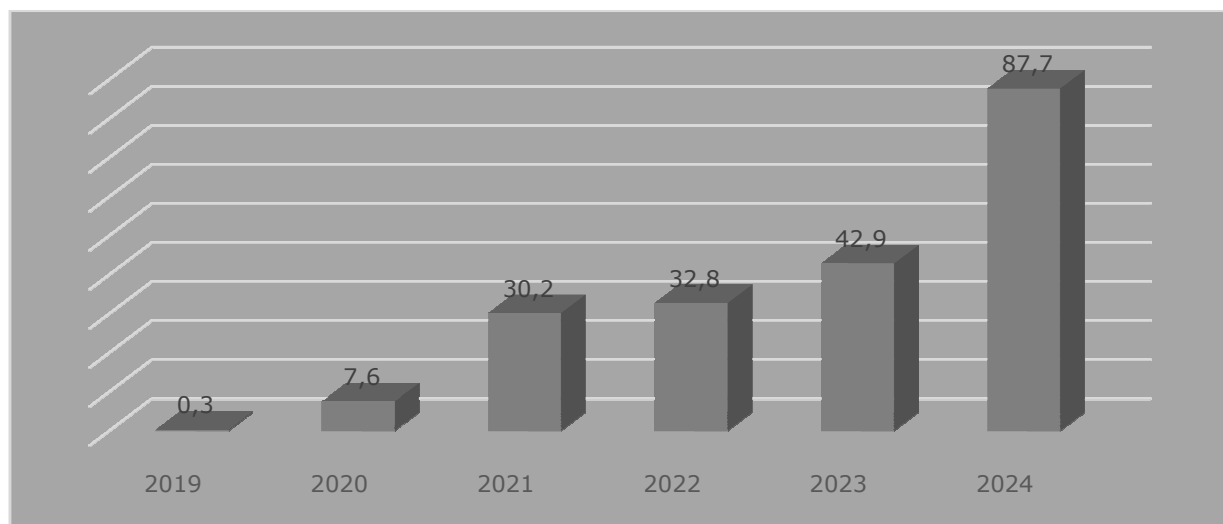


Рисунок 2. Кількість успішних ідентифікацій у Системі BankID НБУ, млн. шт.

Джерело: побудовано автором на основі інформації (Національний банк України, 2025, Травень)

Однак наявні в Україні моделі дистанційної ідентифікації та верифікації клієнтів не вирішують двох головних проблем учасників ринку та клієнтів. Для фінансових установ основою проблемою є висока вартість процедури KYC. Клієнти головним чинником невдоволення вважають необхідність здійснення заходів KYC щоразу при бажанні використати фінансову послугу нової установи. Принциповим вирішенням вищевказаних проблем може бути використання технології розподіленого реєстру (Distributed Ledger Technology – DLT). Ключовими компонентами цієї технології є однорангова (peer-to-peer) мережа, в якій усі дані дублюються на кількох вузлах, а також відповідний протокол консенсусу, який керується певними вузлами для забезпечення дійсності змін стану та синхронізації всіх копій. Аутентифікація у DLT здійснюється за допомогою криптографії з відкритим ключем, що дозволяє брати участь у консенсусі або взаємодіяти з мережею та авторизувати транзакції. Розподілені реєстри стійкі до збоїв, а також до зловмисної поведінки невеликої частини вузлів, що робить їх надійною та децентралізованою цифровою інфраструктурою. Особливим випадком DLT є технологія блокчейн, ключовою характеристикою якої є те, що транзакції групуються у блоки, і кожний блок містить хеш-значення попереднього блоку. Таким чином, блоки формують структуру лише з додаванням нових даних (ланцюг) з метою створення стійкого до підробок історичного запису.

З огляду на зазначені загальні властивості DLT, нейтральна платформа на основі блокчейну, на якій фінансові установи могли б співпрацювати щодо електронної ідентифікації та верифікації, виглядає дуже привабливою. Зокрема, DLT дозволяє створити хронологічний, децентралізований реєстр, в якому фінансові установи, які мають необхідність у здійсненні перевірки KYC щодо певного клієнта, можуть перевіряти результат процесу, який вже було здійснено стосовно такого клієнта іншою установою. Цей алгоритм дозволяє уникнути повторного здійснення однакових процедур перевірки при зверненні клієнта до іншої фінансової установи, оскільки повна перевірка KYC буде здійснюватися лише однією фінансовою установою. Далі така установа буде ділитися результатами здійсненої перевірки з іншими установами, до яких надійшов запит від клієнта з бажанням отримати фінансову послугу. Крім того, використання DLT потенційно дасть можливість суттєво зменшити комплаєнс-витрати фінансових установ через процедуру розподілу вартості процесу KYC між усіма фінансовими установами, що надають послуги певному клієнту.

Після здійснення стандартизації вимог до процедури ідентифікації та верифікації DLT зможе виконувати роль «єдиного джерела істини», тобто джерела даних, яке визнається всіма суб'єктами первинного фінансового моніторингу та регуляторами ринку. Водночас при

використанні блокчейну загострюється питання конфіденційності, оскільки незмінність даних і вбудоване надмірне дублювання означають, що всі вузли мають доступ до перегляду збережених у ланцюжку даних. Іншою проблемою є фактична неможливість видалення даних з блокчейну. Відповідно зберігання персональних даних клієнтів у реєстрі є недоцільним, адже така практика суперечить Загальному регламенту про захист даних (General Data Protection Regulation – GDPR), який гарантує право на забуття (EUR-Lex, 2016, April 27). До того ж, зберігання файлів з ідентифікаційними даними безпосередньо в реєстрі є економічно недоцільним, зважаючи на вартість такого зберігання. Рішенням, яке дозволяє усунути проблему захисту даних, є запис на блокчейн не документів, а лише факту успішного проходження процесу KYC у формі хеш-значення. В цій концепції фактичні дані зберігаються в базі даних, що керується банками або централізованим постачальником послуг. Після успішного проходження процесу KYC клієнт матиме змогу не здійснювати його заново при зверненні до іншої фінансової установи. Натомість, йому достатньо буде лише підтвердити свою особу, використовуючи хеш-значення, збережене в реєстрі.

Важливим кроком до практичної імплементації технології блокчейну в процес KYC стало створення та значне поширення смарт-контрактів, які були вперше запропоновані в проєкті Ethereum. Смарт-контракти складаються з інструментів і протоколів, які дозволяють створювати децентралізовані додатки (Decentralized applications – DApps), які працюють згідно з запрограмованим сценарієм (Karsoulis *et al.*, 2020). Застосування смарт-контрактів дозволяє налаштувати функціонування блокчейн-системи ідентифікації та верифікації, яка буде відповідати вимогам та баченню здійснення фінансового моніторингу у конкретній юрисдикції. Тобто саме в смарт-контракт можна буде записувати весь алгоритм дій щодо процесу належної перевірки, який попередньо повинен бути погодженим усіма учасниками національної системи фінансового моніторингу, від стандартизованого переліку необхідних ідентифікаційних документів до процедури клірингу за послуги KYC. Перелік потенційних проблем, які необхідно вирішити в кожній національній системі фінансового моніторингу для практичної імплементації технології блокчейну в процес належної перевірки клієнтів, міститься в таблиці 2.

Таблиця 2. Проблеми функціонування процесу KYC, що ґрунтується на технології блокчейну, та можливі варіанти їх вирішення

Проблеми	Можливі варіанти вирішення
Адміністрування системи	Централізовано (наприклад національним регулятором)
	Спеціалізована установа, до якої підключені учасники ринку
	Децентралізована система
Верифікатори клієнтів	Суб'єкти первинного фінансового моніторингу
	Спеціалізована установа, до якої підключені учасники ринку
	Державні установи, які здійснюють видачу певних видів документів
Контроль якості процесу KYC	Відсутній (недобросовісна фінансова установа може бути виявлена лише в рамках стандартних регуляторних процедур)
	Наявний (шляхом встановлення граничної кількості клієнтів, які були ідентифіковані та верифіковані фінансовою установою з помилками)
Набір документів для ідентифікації	Стандартизований (встановлений нормативно-правовими актами регуляторів щодо певної категорії клієнтів)
	Розширений (доповнений даними, які є необхідними фінансовим установам при реалізації певних видів фінансових продуктів)
Зберігання даних клієнтів	Централізоване сховище даних
	У кожній фінансовій установі, до якої клієнт звернувся за послугою
Оплата за здійснення KYC	Відсутня (всі первинні витрати залишаються на стороні установи, яка вперше здійснила процес KYC щодо клієнта)
	Наявна (розподіл витрат між усіма учасниками системи, послугами яких користується ідентифікований та верифікований клієнт)

Джерело: розроблено автором

Як видно з таблиці 2, першим питанням, яке має бути вирішене на національному рівні, є адміністрування системи. Для його вирішення може бути використана централізована схема, спеціалізована установа або децентралізована схема. При централізованій схемі адміністрування системи на базі блокчейну буде обов'язком національного регулятора (наприклад центрального банку). При використанні спеціалізованої установи таку роль може виконувати недержавна організація, щодо якої здійснюється посилений контроль з боку державних органів. Альтернативою може бути повністю децентралізована схема адміністрування системи верифікації, яка успішно використовується в обігу криптоактивів.

Наступним питанням є набір установ, яким буде надано право підтверджувати ідентифікаційну інформацію, записану клієнтом на блокчейн. Очевидної відповіді на це питання теж не існує, тому в таблиці 2 зазначені три можливі варіанти. Першим варіантом є надання права верифікувати дані самим звітним установам. Цей варіант найбільш схожий до поточної практики, коли самі суб'єкти первинного фінансового моніторингу роблять висновок щодо «істинності» документів, наданих установам клієнтом. Надалі підтверджені дані можуть використовуватися іншими учасниками ринку через інструмент покладання. Однак такий спосіб верифікації містить ризик підтвердження установою «істинності» фальшивих документів, оскільки працівник фінансової організації не є спеціалістом у сфері шахрайства з ідентифікаційними документами. Тому альтернативним варіантом є використання недержавних організацій, які спеціалізуються на отриманні даних з різноманітних джерел, обробці інформації та наданні даних звітним установам у сфері фінансового моніторингу. Перевагою використання такого варіанта є швидке отримання звітними установами актуальної інформації та підвищений рівень захисту персональних даних. Альтернативою є використання державних установ-ідентифікаторів, які спеціалізуються на наданні певних видів послуг та підтвердженні певних документів. Учасники ринку, використовуючи цей варіант, зможуть напряду отримувати інформацію від таких установ через автоматизовані запити до спеціалізованих реєстрів.

Контроль якості даних є малодослідженим, але від того не менш важливим елементом процесу КҮС. Для ефективності системи кожний учасник має бути впевненим, що записані на блокчейн дані є правильними та не потребують від установи використання додаткових ресурсів для перевірки отриманої інформації. В таблиці 2 зазначено два можливі варіанти рішення: або такий контроль якості здійснюється, або ні. Сучасні вимоги до належної перевірки клієнта ґрунтуються на відповідальності звітної установи, яка встановлює ділові відносини з клієнтом. Тобто ризик використання неактуальних або фальшивих даних несе звітна установа, навіть якщо вона отримала їх від іншого суб'єкта первинного фінансового моніторингу або агента. Альтернативою, яку можна використовувати при створенні новітньої системи верифікації на базі блокчейну, може стати облік виявлених інцидентів отримання неправдивих відомостей. При досягненні граничної межі таких інцидентів до установи-ідентифікатора можуть бути застосовані заходи впливу.

Важливим практичним питанням, яке потребує вирішення перед створенням системи належної перевірки на основі технології блокчейну, є погодження переліку документів для ідентифікації особистості клієнта. Поточна практика містить нормативно затверджений перелік інформації, які звітні установи повинні використовувати в своїй діяльності для ідентифікації певних груп клієнтів. Однак альтернативою може бути надання клієнтом в блокчейн додаткової інформації, яка дозволить мати переваги при отриманні певних фінансових послуг. Технічна можливість та економічна доцільність такої «розширеної належної перевірки клієнта» має бути погодженою регулятором ринку та надавачами фінансових послуг.

Зберіганню персональних даних клієнта приділяється посилена увага в будь-якій юрисдикції з ефективною системою фінансового моніторингу. Таблиця 2 містить два варіанти такого зберігання. Перший варіант, який наразі використовується звітними установами, полягає в збереженні даних безпосередньо організацією, до якої клієнт звертається для отримання послуги. Недоліком такого процесу є ризик неправомірного заволодіння даними, оскільки доступ до них мають багато співробітників різних звітних установ, в яких обслуговується клієнт. Тому альтернативним варіантом може бути створення централізованого сховища ідентифікаційних даних, доступ до якого звітні установи отримують лише при автоматизованому запиті.

Останньою проблемою є оплата послуг організації, яка ідентифікувала клієнта. Установи та регулятор можуть обрати варіант, який не передбачає отримання коштів суб'єктом-ідентифікатором. Такий процес має право на існування, якщо суб'єкти первинного фінансового моніторингу будуть звертатися за послугою верифікації до державних спеціалізованих реєстрів, оплату діяльності яких здійснює держава. Однак при використанні схеми, в якій ідентифікацію клієнтів будуть здійснювати безпосередньо звітні установи, доцільніше використовувати систему оплати, що базується на кількості ідентифікованих клієнтів.

Тільки після вирішення всіх проблем, зазначених у таблиці 2, та закріплення їх у законодавчих або нормативних документах певної юрисдикції можливе створення нового порядку дій здійснення належної перевірки клієнта, що ґрунтується на технології блокчейну. Зазначений порядок має бути записаний до смарт-контракту та використовуватися всіма учасниками національної системи фінансового моніторингу.

Висновки

Традиційний підхід до процесу здійснення ідентифікації та верифікації клієнтів, що ґрунтується на особистій зустрічі працівника фінансової установи та клієнта, потребує трансформації з огляду на високі витрати суб'єктів первинного фінансового моніторингу та негативний клієнтський досвід. Як альтернативу ринок застосовує дистанційні моделі верифікації, спираючись на цифровізацію надання послуг.

Основними моделями дистанційної верифікації в Україні є відеоверифікація, використання сервісів Державного підприємства «ДІЯ» або Системи BankID НБУ. Попри однозначне зростання ефективності процесу KYC при використанні цих моделей, вони не здатні кардинально змінити ситуацію як щодо скорочення витрат на процеси перевірки клієнта, так і щодо необхідності глибокого залучення клієнта до процесу ідентифікації та верифікації.

Відповіддю може стати використання технології розподіленого реєстру на базі блокчейну. Для використання такої моделі в національній системі фінансового моніторингу потрібно вирішити низку складних питань, які стають ще складнішими з огляду на глобалізацію фінансової сфери. Однак перехід до KYC на базі блокчейну дозволить здійснити революційну зміну у взаємодії між фінансовими установами та їх клієнтами, яка підвищить здатність фінансової системи до протидії відмиванню коштів та фінансуванню тероризму, кардинально зменшить витрати фінансових установ на комплаєнс та покращить клієнтський досвід споживачів фінансових послуг.

Подяки

Немає.

Конфлікт інтересів

Немає.

Список використаних джерел

- Верховна Рада України. (2019, Грудень 06). *Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення*. Закон України № 361-IX. Взято з <https://zakon.rada.gov.ua/laws/show/361-20#Text>
- Національний банк України. (2020, Липень 28) *Положення про здійснення установами фінансового моніторингу*. Постанова Правління Національного банку України № 107. Взято з <https://zakon.rada.gov.ua/laws/show/v0107500-20#Text>
- Національний банк України. (2020, Травень 19). *Положення про здійснення банками фінансового моніторингу*. Постанова Правління Національного банку України № 65. Взято з <https://zakon.rada.gov.ua/laws/show/v0065500-20#Text>
- Національний банк України. (2025, Травень). *Річний звіт Національного банку України за 2024 рік*. Взято з https://bank.gov.ua/admin_uploads/article/annual_report_2024.pdf?v=13
- Шевченко, М. В. (2022). Належна перевірка щодо публічних діячів: зарубіжний досвід. *Проблеми сучасних трансформацій. Серія: право, публічне управління та адміністрування*, 2, 45–52. doi: 10.54929/pmtl-issue2-2021-09
- EUR-Lex (2016, April 27). *Regulation (EU) 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) (Text with EEA relevance)*. Retrieved from <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng>
- FATF (2025, June). *The FATF Recommendations*. Retrieved from <https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Fatfrecommendations/Fatf-recommendations.html>
- Fekete, D., & Bárkányi, P. (2023). Examination of technologies that can be used for the development of an identity verification application. *International Journal of Advanced Natural Sciences and Engineering Researches*, 7(5), 25–32. doi: 10.59287/ijanser.896
- Fenergo (2022). *Integrated KYC and Scaling for Success. Report*. Retrieved from <https://6019495.fs1.hubspotusercontent-na1.net/hubfs/6019495/integrated-kyc-and-scaling-for-success.pdf>
- Kapsoulis, N. et al. (2020). Know Your Customer (KYC) implementation with smart contracts on a privacy-oriented decentralized architecture. *Future Internet*, 12(2), 41. doi: 10.3390/fi12020041
- Moyano, J. P., & Ross, O. (2017). KYC optimization using distributed ledger technology. *Business & Information Systems Engineering*, 59, 411–423. doi: 10.1007/s12599-017-0504-2
- Ostern, N. K., & Riedel, J. (2020). Know-Your-Customer (KYC) requirements for initial coin offerings. *Business & Information Systems Engineering*, 63(5), 551–567. doi: 10.1007/s12599-020-00677-6
- Patil, P., & Sangeetha, M. (2022). Blockchain-based decentralized KYC verification framework for banks. *Procedia Computer Science*, 215, 529–536. doi: 10.1016/j.procs.2022.12.055
- Thomson Reuters (2016, May 09). *Know your customer surveys reveal escalating costs and complexity*. Retrieved from <https://www.thomsonreuters.com/en/press-releases/2016/may/thomson-reuters-2016-know-your-customer-surveys>
- U.S. Financial Crimes Enforcement Network. (n.d.). *The Currency and Foreign Transactions Reporting Act of 1970*. Retrieved from <https://www.fincen.gov/resources/statutes-and-regulations/bank-secrecy-act>

References

- EUR-Lex (2016, April 27). *Regulation (EU) 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) (Text with EEA relevance)*. Retrieved from <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng>
- FATF (2025, June). *The FATF Recommendations*. Retrieved from <https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Fatfrecommendations/Fatf-recommendations.html>
- Fekete, D., & Bárkányi, P. (2023). Examination of technologies that can be used for the development of an identity verification application. *International Journal of Advanced Natural Sciences and Engineering Researches*, 7(5), 25–32. doi: 10.59287/ijanser.896
- Fenergo (2022). *Integrated KYC and Scaling for Success. Report*. Retrieved from <https://6019495.fs1.hubspotusercontent-na1.net/hubfs/6019495/integrated-kyc-and-scaling-for-success.pdf>

- Kapsoulis, N. et al. (2020). Know Your Customer (KYC) implementation with smart contracts on a privacy-oriented decentralized architecture. *Future Internet*, 12(2), 41. doi: 10.3390/fi12020041
- Moyano, J. P., & Ross, O. (2017). KYC optimization using distributed ledger technology. *Business & Information Systems Engineering*, 59, 411–423. doi: 10.1007/s12599-017-0504-2
- National Bank of Ukraine. (2020, July 28). *Regulations on the implementation of financial monitoring by institutions*. Resolution of the Board of the National Bank of Ukraine No. 107. Retrieved from <https://zakon.rada.gov.ua/laws/show/v0107500-20#Text>
- National Bank of Ukraine. (2020, May 19). *Regulations on the implementation of financial monitoring by banks*. Resolution of the Board of the National Bank of Ukraine No. 65. Retrieved from <https://zakon.rada.gov.ua/laws/show/v0065500-20#Text>
- National Bank of Ukraine. (2025, May). *Annual Report of the National Bank of Ukraine for 2024*. Retrieved from https://bank.gov.ua/admin_uploads/article/annual_report_2024.pdf?v=13
- Ostern, N. K., & Riedel, J. (2020). Know-Your-Customer (KYC) requirements for initial coin offerings. *Business & Information Systems Engineering*, 63(5), 551–567. doi: 10.1007/s12599-020-00677-6
- Patil, P., & Sangeetha, M. (2022). Blockchain-based decentralized KYC verification framework for banks. *Procedia Computer Science*, 215, 529–536. doi: 10.1016/j.procs.2022.12.055
- Shevchenko, M. V. (2022). Due diligence regarding public figures: Foreign experience. *Problems of Modern Transformations. Series: Law, Public Management and Administration*, 2, 45–52. doi: 10.54929/pmtl-issue2-2021-09
- Thomson Reuters (2016, May 09). *Know your customer surveys reveal escalating costs and complexity*. Retrieved from <https://www.thomsonreuters.com/en/press-releases/2016/may/thomson-reuters-2016-know-your-customer-surveys>
- U.S. Financial Crimes Enforcement Network. (n.d.). *The Currency and Foreign Transactions Reporting Act of 1970*. Retrieved from <https://www.fincen.gov/resources/statutes-and-regulations/bank-secrecy-act>
- Verkhovna Rada of Ukraine. (2019, December 06). *On prevention and counteraction to the legalization (laundering) of proceeds of crime, financing of terrorism and financing of the proliferation of weapons of mass destruction*. Law of Ukraine No. 361-IX. Retrieved from <https://zakon.rada.gov.ua/laws/show/361-20#Text>