

Прокопенко Н. С.

доктор економічних наук, професор,
проректор з трансформації та інституційного розвитку,
Приватний вищий навчальний заклад "Європейський університет"
ORCID: <https://orcid.org/0000-0001-6753-8831>

СУЧАСНІ СИСТЕМИ ІНФОРМАЦІЙНОГО ОБМІНУ МІЖ СУБ'ЄКТАМИ ПЕРВИННОГО ФІНАНСОВОГО МОНІТОРИНГУ

У статті розглянуті системи обміну клієнтськими даними, призначені для підвищення ефективності виконання звітними установами у сфері фінансового моніторингу вимог щодо належної перевірки. Розкрито механізми створення інформаційного партнерства в Сінгапурі, Канаді та країнах Європейського Союзу. Визначено, що глибина контролю з боку державних регуляторів та їх залученість в операційні процеси інформаційного обміну залежить від кількості звітних установ, географічного розповсюдження суб'єктів первинного фінансового моніторингу та технічних обмежень. Враховуючи означені критерії, Сінгапуром було обрано модель обміну за принципом «згори-вниз», для якої характерна централізація, а системи обміну даними в Канаді та Європейському Союзі передбачають горизонтальну архітектуру з суворими вхідними бар'єрами, однак без присутності регуляторів ринку серед учасників погодженого інформаційного партнерства.

Ключові слова: інформаційний обмін, фінансовий моніторинг, ризик, суб'єкт первинного фінансового моніторингу, підозрілі фінансові операції, належна перевірка клієнтів.

Nataliia Prokopenko

Private Higher Educational Institution «European University»

MODERN INFORMATION EXCHANGE SYSTEMS BETWEEN PRIMARY FINANCIAL MONITORING ENTITIES

The article discusses client data exchange systems designed to improve the efficiency of reporting entities in the field of financial monitoring due diligence requirements. The mechanisms for creating information partnerships in Singapore, Canada and the European Union are disclosed. It is determined that the depth of control by state regulators and their involvement in the operational processes of information exchange depends on the number of reporting entities, the geographical distribution of primary financial monitoring entities and technical limitations. Taking into account these criteria, Singapore chose a top-down information exchange model, which is characterized by centralization, direct administration of the system by the state regulator and control of each information disclosure by the financial intelligence unit. At the same time, data exchange systems in Canada and the European Union provide for strict entry barriers at the approval stage with the simultaneous absence of market regulators' personal data has become an additional factor in choosing a horizontal architecture of information systems. It is emphasized that all the analyzed systems have a regime of exemption from civil or criminal liability for participants in the case of good faith exchange of information for the purpose of combating money laundering or terrorist financing. An additional safeguard created in all the analyzed exchange systems to prevent the unjustified transfer of personal data is the requirement to provide information only regarding clients or high-risk transactions. Another common feature of the Singaporean, Canadian and European models of data exchange on financial monitoring is the presence of strict requirements for information protection at the stages of data transmission, receipt and storage. The ability of the Singaporean COSMIC data exchange system to distribute information within all participants in the system is highlighted, which improves the quality of calculating the client's risk profile, but creates the risk of refusal to establish or maintain business relations with the client when disseminating unconfirmed negative data.

Keywords: information exchange, financial monitoring, risk, primary financial monitoring entity, suspicious financial transactions, customer due diligence.

Постановка проблеми та її актуальність.

Першочерговим завданням суб'єкту первинного фінансового моніторингу в будь-якій юрисдикції є здійснення повного спектру заходів належної перевірки клієнтів. Враховуючи розвиненість інфраструктури фінансового ринку, фізичні та юридичні

особи мають можливість обслуговуватися в різних зобов'язаних установах, що значно ускладнює аналіз ризиків відмивання коштів та фінансування тероризму та, в свою чергу, призводить до обмеженого застосування ризик-орієнтованого підходу при встановленні ризик-профілю клієнта. Для вирішення

даної проблеми в глобальних фінансових центрах були створені системи обміну даними між звітними установами, які дозволяють легально формувати цілісну картину діяльності клієнтів та передавати підрозділу фінансової розвідки більш якісні звіти про підозрілі фінансові операції. Аналіз головних елементів таких систем дозволить оцінити їх вплив на підвищення ефективності загальнонаціональних режимів боротьби з відмиванням коштів та фінансуванням тероризму.

Аналіз останніх досліджень і публікацій. Наукові праці щодо обміну даними в сфері фінансового моніторингу, зазвичай, стосуються взаємодії між підрозділами фінансових розвідок різних юрисдикцій. Зокрема, головною темою дослідження К. McNaughton був аналіз національних моделей підрозділів фінансової розвідки у десяти вибраних країнах [8]. М. Brewczyńska проаналізувала проблеми при обробці персональних даних підрозділами фінансової розвідки, зважаючи на європейські вимоги Загального регламенту про захист даних та Директиви про правоохоронну діяльність [1]. J. Malala, N. Azinge-Egbiri та A. Sunmonі здійснили огляд міжвідомчої співпраці між підрозділами фінансової розвідки в Нігерії та Кенії [6]. Y. Li, T. Ranbaduge та K.S. Ng дослідили можливості використання сучасних технологій конфіденційності для безпечного аналізу даних державними регуляторами та представниками фінансової галузі [5]. T. Legrand та C. Leuprecht проаналізували результати діяльності транскордонних мереж безпеки між США та Канадою [4]. Таким чином, питання функціонування сучасних систем обміну даними між суб'єктами первинного фінансового моніторингу в цілях здійснення заходів належної перевірки клієнтів, залишаються недостатньо дослідженими.

Метою статті є визначення головних аспектів функціонування систем інформаційного обміну між звітними установами в сфері фінансового моніторингу, які запроваджені в світових фінансових центрах.

Виклад основного матеріалу дослідження. Однією з найбільш відомих систем обміну інформацією щодо клієнтів фінансових установ, яка була заснована на принципах державно-приватного партнерства, можна вважати платформу «Спільний обмін інформацією та справами щодо відмивання коштів/фінансування тероризму» (Collaborative Sharing of Money Laundering/Terrorism Financing Information and Cases – COSMIC). Суб'єкти первинного фінансового моніторингу Сінгапуру отримали змогу здійснювати обмін даними про клієнтів на даній платформі з 1 квітня 2024 року, після набуття чинності змінами до Закону про фінансові послуги та ринки (Financial Services and Markets Act – FSMA) [2].

Наразі до платформи COSMIC під'єднано шість великих комерційних банків Сінгапуру, а функції оператора системи здійснюються Валютним управлінням Сінгапуру (Monetary Authority of Singapore – MAS), яке одночасно є і центральним банком, і органом нагляду. Повноваженнями включення банків та небанківських установ до інформаційної платформи теж володіє MAS [7].

Головними рисами інформаційного обміну за допомогою COSMIC є алгоритмізація та державний контроль. Згідно зі статтею 28D Закону FSMA звітна установа у сфері фінансового моніторингу має право на здійснення запиту до іншої звітної установи лише при одночасній наявності трьох критеріїв: щодо клієнта існує принаймні один індикатор високого ризику; виконуються порогові критерії; присутнє розуміння, яким чином отримана інформація допоможе суб'єкту первинного фінансового моніторингу в аналізі ризиків відмивання коштів, фінансування тероризму чи фінансування розповсюдження зброї масового знищення [2]. Звітна установа може доповнити запит будь-якою інформацією про ризики, яку запитувач вважає необхідною. Перед розкриттям інформації, надавач повинен переконатися в істинності кожного з трьох критеріїв запиту, а також в тому, що специфіка та обсяг запитуваної інформації про клієнта є пропорційним ризикам у сфері фінансового моніторингу.

Відповідно до статті 28G Закону FSMA критерії та індикатори високого ризику не підлягають публічному розголошенню та повинні бути надані Валютним управлінням Сінгапуру окремо кожній звітній установі. Дана вимога перешкоджає організованим злочинним групам створювати траси платежів, які б перешкоджали фінансовим установам ефективно виявляти підозрілі транзакції. Крім того, використання COSMIC згідно з вимогами FSMA надає суб'єктам первинного фінансового моніторингу правовий імунітет від необхідності дотримання банківської таємниці чи інших обмежень щодо розголошення інформації.

Для підвищення якості отримуваних даних в системі COSMIC створено правові запобіжники, до яких належать статті 28J та 28L Закону FSMA. Зокрема, встановлено відповідальність фінансової установи та посадової особи установи за надання іншій фінансовій установі в межах COSMIC інформації, що є неправдивою в суттєвих деталях. Підрозділу фінансової розвідки Сінгапуру надано право отримувати копію кожного випадку розкриття інформації про ризики та право на доступ до кожної публікації інформації про ризики, яка була здійснена фінансовою установою [2]. Відповідно, архітектура COSMIC побудована на трьох рівнях контролю. На першому рівні якість інформації оцінюють фі-

нансові установи, які є одержувачами інформації. На другому рівні контроль здійснює Валютне управління Сінгапуру, яке здійснює регулювання ринку та є оператором інформаційної системи. За третій рівень контролю в межах COSMIC відповідає Сінгапурське управління звітності про підозрілі транзакції (Singapore Suspicious Transaction Reporting Office – STRO), що виконує функції підрозділу фінансової розвідки.

Обмін даними про клієнтів між членами COSMIC має здійснюватися лише в електронній системі обміну інформацією, яку повинно створити та підтримувати Валютне управління Сінгапуру. Відповідно, будь-який запит на інформацію про ризики, розкриття інформації про ризики та виправлення помилки в даних про ризики повинні здійснюватися з використанням електронної системи обміну інформацією MAS. У випадку неможливості фінансової установи отримати доступ до публікації інформації про ризики з електронної системи обміну, Валютне управління Сінгапуру повинне надати розумні альтернативні засоби, за допомогою яких учасник системи обміну може отримати доступ до інформації про ризики. У випадку не дотримання фінансовою установою будь-яких правил використання електронної системи обміну інформацією, MAS має право припинити, призупинити або обмежити доступ фінансової установи до електронної системи обміну інформацією [2].

Керівні вказівки MAS вимагають від звітних установ створення та періодичного оновлення політик, процедур та засобів контролю, які мають забезпечувати дотримання вимог щодо обміну інформацією в системі COSMIC. Крім того, суб'єкти первинного фінансового моніторингу повинні забезпечити здійснення належного навчання посадових осіб для якісного виконання вищевказаних внутрішніх документів фінансової установи. Додатково до поточних контрольних процедур, учасникам системи обміну рекомендується здійснювати періодичні регулярні аудити на відповідність вимогам та перевірки для забезпечення якості [3].

Надзвичайно суворі система внутрішнього контролю, до якої залучені органи державної влади, дозволила впровадити в межах COSMIC практику розповсюдження важливої інформації про клієнта в межах всіх учасників системи обміну даними. Відповідно до статті 28F Закону FSMA, фінансова установа може опублікувати будь-яку інформацію про ризики, що стосується певного клієнта, для всіх фінансових установ в електронній системі обміну інформацією [2]. Дана архітектура інформаційного обміну значно відрізняється від стандартних принципів державно-приватного партнерства в інших юрисдикціях, які дозволяють обмін інформацією

в сфері фінансового моніторингу лише між одним надавачем та одним отримувачем даних. Жорсткі внутрішні запобіжники допомагають COSMIC підвищити ефективність загальнонаціональної системи фінансового моніторингу шляхом можливості встановлення більш точного ризик-профілю клієнтів та, водночас, не поширювати недостовірну інформацію серед усіх учасників системи.

Інша система обміну даними з фінансового моніторингу набула чинності в березні 2025 року після внесення змін до Закону про доходи від злочинної діяльності (відмивання грошей) та фінансування тероризму (Proceeds of Crime (Money Laundering) and Terrorist Financing Act – PCMLTFA). Зокрема, розділ 11.01 PCMLTFA надає право звітним установам Канади на розкриття персональної інформації про особу суб'єкту первинного фінансового моніторингу без відома або згоди такої особи [10]. Інформація може надаватися лише для цілей виявлення або запобігання відмиванню коштів, фінансуванню тероризму та ухиленню від санкцій. Відповідно до розділу 11.01 PCMLTFA, обмін даними між учасниками системи є можливим лише при поєднанні наступних умов: інформація про клієнта була зібрана в процесі діяльності такої особи чи організації; розкриття даних вважається доцільним, оскільки знизить ризики відмивання коштів, фінансування тероризму або ухилення від санкцій; розкриття клієнту інформації щодо обміну даними створить ризики невиконання учасником системи своїх обов'язків в сфері фінансового моніторингу; обмін даними здійснюється в межах встановлених правил [10].

Участь в системі обміну даними є добровільною. Перед початком взаємодії, заснованої на праві згідно з розділом 11.01 PCMLTFA, зобов'язані установи мають розробити кодекс практики та надати даний документ до Управління Комісара з питань конфіденційності Канади для розгляду та затвердження. Копія кодексу практики також повинна бути надана підрозділу фінансової розвідки Канади (Financial Transactions and Reports Analysis Centre of Canada – FINTRAC) для перевірки відповідності партнерства цілям фінансового моніторингу та правильності вказання реєстраційних даних звітних установ. Після погодження кодексу практики регуляторними органами учасники системи обміну даними отримують законодавчий захист від цивільної чи кримінальної відповідальності для осіб та установ, які розголошують, збирають або використовують персональні дані, за умови, що обмін даними здійснюється сумлінно та у суворій відповідності до затвердженого кодексу практики та вимог PCMLTFA [10].

В цілях адекватного розуміння національними суб'єктами господарювання в сфері фінансового моніторингу специфічних регуляторних вимог,

необхідних для можливості обміну даними в межах розділу 11.01 PCMLTFA, Управлінням Комісара з питань конфіденційності Канади було розроблено типовий кодекс практики, який звітні установи можуть використовувати для підготовки власних унікальних внутрішніх документів. Згідно з типовим кодексом практики, інформаційний обмін може стосуватися реєстраційних, фінансових та технічних даних. Інформація щодо реєстрації може включати ім'я, адресу, електронну пошту, номери телефонів, документи, що посвідчують особу, громадянство особи, дані щодо роботодавця, інформацію про бенефіціарну власність. Дані про здійснені транзакції, спроби проведення транзакцій та інформація про рахунки мають право передаватися у складі фінансових даних. Зокрема, суб'єкти первинного фінансового моніторингу можуть здійснювати обмін інформацією стосовно: дати, часу та місця транзакцій; суми коштів або інших активів, які брали участь в транзакціях; ідентифікаторів транзакцій; власників рахунків; номерів рахунків; номерів відділень або номерів фінансових установ. До технічних даних, якими дозволяється обмінюватися учасникам відповідно до розділу 11.01 PCMLTFA, належить інформація, пов'язана з пристроями, що використовуються в транзакціях, адресами інтернет-протоколів, даними онлайн-сесій. Водночас в PCMLTFA наголошується на необхідності усвідомлення зобов'язаними установами неможливості ефективного досягнення цілей належної перевірки клієнтів шляхом обміну меншою кількістю персональної інформації [9].

В якості запобіжників, які унеможливають неправомірне використання інформації, переданої через систему обміну даними згідно з розділом 11.01 PCMLTFA, суб'єкти первинного фінансового моніторингу повинні використовувати повний спектр заходів щодо забезпечення захисту персональної інформації. До безпечних електронних методів зв'язку Управління Комісара з питань конфіденційності Канади відносить зашифровані електронні листи, використання API, віртуальні кімнати даних та мережі безпечної співпраці, безпечні служби передачі файлів або протоколи інформаційних технологій. Безпечними фізичними способами зв'язку вважаються захищена телефонна лінія або рекомендований лист. В кодексі практики мають бути присутні посилання на визнані галузеві стандарти захисту інформації, які застосовують звітні установи в своїй діяльності.

Крім того, дані, отримані в результаті обміну, повинні зберігатися національними суб'єктами первинного фінансового моніторингу лише протягом періоду, необхідного для їх використання відповідно до визначених цілей, або відповідно до власної політики учасника системи обміну. Звітні установи

мають застосовувати механізми, які гарантують збереження персональної інформації не довше, ніж це необхідно для виконання вимог належної перевірки та застосування ризик-орієнтованого підходу. Записи про рішення щодо розкриття, збору або використання персональної інформації, а також обґрунтування цього рішення, враховуючи відповідні критерії, викладені у встановлених рамках, також повинні бути задокументовані та збережені учасниками системи обміну. Доступ до отриманої інформації в межах системи обміну даними має бути захищеним. Серед іншого, засобами захисту персональних даних, згідно з типовим кодексом практики, можуть бути шифрування, багатофакторна автентифікація, керування ключами, контроль доступу на основі ролей [9].

В Європейському Союзі система обміну даними між суб'єктами первинного фінансового моніторингу була запроваджена шляхом затвердження 31 травня 2024 року Регламенту ЄС 2024/1624, стаття 75 якого унормувала питання створення інформаційного партнерства між звітними установами [11]. Участь у партнерстві з обміну інформацією є добровільною та залежить від політики ризик-менеджменту зобов'язаного суб'єкту. Для створення інформаційного партнерства звітні установи мають повідомити відповідні наглядові органи, які здійснюють перевірку механізмів захисту даних, процедури управління та дотримання інших регуляторних вимог. В разі необхідності, до процесу перевірки можуть бути залучені підрозділи фінансових розвідок. Практичне впровадження нових правил обміну даними стане можливим з 10 липня 2027 року, коли Регламент ЄС 2024/1624 набере чинності.

Система обміну в межах інформаційного партнерства дозволяє суб'єктам первинного фінансового моніторингу обмінюватися широким спектром даних про клієнтів, однак лише в межах ризиків відмивання коштів або фінансування тероризму. Зокрема, до об'єктів обміну належать: дані, отримані при ідентифікації та верифікації клієнтів; інформація про кінцевих бенефіціарних власників; характер ділових відносин; джерело походження статків і джерело походження коштів; дані про фінансові операції; фактори ризику, пов'язані з клієнтом; встановлений ризик-профіль клієнта; інформація про підозри. Водночас, частина 4 статті 75 Регламенту ЄС 2024/1624 обмежує обмін інформацією про підозрілі операції лише випадками, в яких підрозділ фінансової розвідки, до якого було подано звіт про підозрілу операцію, погодився на таке розголошення даних [11].

Зобов'язані суб'єкти мають реєструвати всі випадки обміну інформацією в межах партнерства та не покладатися виключно на дані, отримані в контексті партнерства. Відповідно, звітні установи по-

винні здійснювати власну оцінку фінансових операцій за участю клієнтів з метою визначення можливої пов'язаності транзакцій з відмиванням коштів або фінансуванням тероризму. Захист від відповідальності для зобов'язаних суб'єктів за розкриття та обмін інформацією в межах інформаційного партнерства гарантується загальним правовим механізмом, вказаним у преамбулі Регламенту ЄС 2024/1624.

В цілях недопущення передачі між фінансовими установами персональних даних стосовно великої кількості клієнтів, європейська система обміну інформацією обмежує використання дії статті 75 Регламенту ЄС 2024/1624 виключно випадками, в яких присутній високий ризик. Враховуючи дану вимогу, звітні установи мають право надсилати запит на отримання даних лише щодо клієнтів високого ризику, розрахований відповідно до оцінки ризиків на рівні Європейського Союзу або згідно з національною оцінкою ризиків. Для прозорого розуміння категорій клієнтів, обмін даними щодо яких дозволено в межах інформаційного партнерства, визначено перелік статей Регламенту ЄС 2024/1624, в яких окреслені специфічні ситуації підвищеного ризику, які вимагають обов'язкового застосування посиленних заходів належної перевірки клієнтів. Такими ситуаціями вважаються: виявлення політично значущих осіб, членів їх сімей та осіб, пов'язаних з політично значущими особами; транскордон-

ні кореспондентські відносини між фінансовими установами; кореспондентські відносини за участю постачальників послуг у сфері криптоактивів; підозри щодо співпраці з компаніями-оболонками; дані щодо заявників на отримання громадянства через інвестиції; операції з юрисдикціями високого ризику [11].

До початку обміну кожен з учасників інформаційного партнерства повинен затвердити у власних внутрішніх документах політику та процедури обміну даними, які мають передбачати можливий обсяг наданої інформації, ролі та обов'язки сторін партнерства з обміну даними, оцінки ризиків, які зобов'язаний суб'єкт братиме до уваги для визначення ситуацій підвищеного ризику, за яких можливий обмін інформацією. Додатковою контрольною процедурою, наявність якої мають право вимагати державні регулятори, є проведення незалежного аудиту функціонування інформаційного партнерства. У випадку здійснення такої перевірки, суб'єкти первинного фінансового моніторингу зобов'язані надавати його результати наглядовим органам.

Порівнюючи архітектуру систем інформаційного обміну в Сінгапурі, Канаді та Європейському Союзі (табл. 1), варто відзначити значно глибшу залученість регуляторного органу та підрозділу фінансової розвідки в операційну діяльність системи обміну COSMIC порівняно з механізмами, засно-

Таблиця 1

Головні характеристики систем інформаційного обміну між суб'єктами первинного фінансового моніторингу в Сінгапурі, Канаді та ЄС

Характеристика	Сінгапур (COSMIC)	Канада (розділ 11.01 PCMLTFA)	ЄС (ст. 75 Регламенту ЄС 2024/1624)
Участь в системі обміну даними	Визначається регулятором	Добровільна	Добровільна
Єдина цифрова платформа обміну даними	Так	Ні	Ні
Інтеграція регулятора в систему обміну інформацією	Так	Ні	Ні
Інтеграція підрозділу фінансової розвідки в систему обміну інформацією	Так	Ні	Ні
Підстави для обміну даними	Однчасна наявність індикатора високого ризику, порогового критерію та розуміння, як надана інформація допоможе в оцінці ризику	Пропорційно загрозам	Високий рівень ризику
Реєстрація всіх випадків обміну інформацією	Так	Так	Так
Звільнення від цивільної чи кримінальної відповідальності в разі добросовісного обміну інформацією в цілях боротьби з відмиванням коштів / фінансуванням тероризму	Так	Так	Так
Розповсюдження інформації про клієнта в межах всіх учасників системи обміну даними	Можливе	Ні	Ні

Джерело: сформовано автором на основі [2; 3; 7; 9; 10; 11]

ваними на дії розділу 11.01 PCMLTFA та статті 75 Регламенту ЄС 2024/1624.

Висновки. Архітектура систем обміну інформацією між установами в цілях фінансового моніторингу залежить від масштабу, кількості учасників та географічних меж юрисдикції. Незначна кількість банків, поєднання функцій регуляторного органу та оператора інформаційної системи Валютним управлінням Сінгапуру, контроль кожного розкриття даних в системі з боку підрозділу фінансової розвідки дозволили створити централізований механізм обміну інформацією за принципом «згори-вниз».

Враховуючи велику кількість суб'єктів первинного фінансового моніторингу, значну територію, технічну складність та ризики втрати даних при функціонуванні єдиної інформаційної системи в межах одного ринку, в Європейському Союзі та Канаді були створені системи обміну інформацією, засновані на принципах горизонтальної взаємодії та

значному регуляторному контролю перед початком здійснення діяльності. Додатковим фактором, який стимулював вибір децентралізованих систем обміну в межах режиму розділу 11.01 PCMLTFA та статті 75 Регламенту ЄС 2024/1624, можна вважати наявність суворих законодавчих вимог до захисту персональних даних.

Обмін даними в COSMIC може передбачати отримання інформації стосовно певного клієнта не лише стороною, яка здійснила запит, а й всіма іншими учасниками системи. Даний механізм не є характерним для інших систем державно-приватного партнерства в сфері інформаційної взаємодії, оскільки створює ризик створення неформального «чорного списку клієнтів» в межах фінансової системи. Водночас, перевагою використання такого обміну даними є підвищення ефективності національної системи фінансового моніторингу через зростання точності встановлення профілю ризику клієнтів.

Література:

1. Brewczyńska M. Financial Intelligence Units: Reflections on the applicable data protection legal framework. *Computer Law & Security Review*. 2021. № 43. DOI: <https://doi.org/10.1016/j.clsr.2021.105612>
2. Financial Services and Markets Act. URL: <https://sso.agc.gov.sg/Acts-Supp/19-2023/Published/20230628?DocDate=20230628>
3. Guidelines to MAS Notice FSM-N02 on Prevention of Money Laundering and Countering the Financing of Terrorism – Financial Institutions' Information Sharing Platform. URL: <https://www.mas.gov.sg/regulation/guidelines/guidelines-to-mas-notice-fsm-n02-on-prevention-of-ml-and-countering-tf--fi-info-sharing-platform>
4. Legrand T., Leuprecht, C. Securing cross-border collaboration: transgovernmental enforcement networks, organized crime and illicit international political economy. *Policy and Society*. 2021. № 40 (4). P. 565–586. DOI: <https://doi.org/10.1080/14494035.2021.1975216>
5. Li Y., Ranbaduge, T., Ng, K. S. Privacy technologies for financial intelligence. *Journal of Economic Criminology*. 2026. № 13. DOI: <https://doi.org/10.1016/j.jeconc.2026.100235>
6. Malala J., Azinge-Egbiri, N., Sunmoni, A. Inter-agency collaborations and the governance of financial intelligence in Nigeria and Kenya. *Journal of Economic Criminology*. 2026. № 13. DOI: <https://doi.org/10.1016/j.jeconc.2026.100234>
7. MAS Launches COSMIC Platform to Strengthen the Financial System's Defence Against Money Laundering and Terrorism Financing. URL: <https://www.mas.gov.sg/news/media-releases/2024/mas-launches-cosmic-platform> (дата звернення: 19.08.2026).
8. McNaughton K. J. The variability and clustering of Financial Intelligence Units (FIUs) – A comparative analysis of national models of FIUs in selected western and eastern (post-Soviet) countries. *Journal of Economic Criminology*. 2023. № 2. DOI: <https://doi.org/10.1016/j.jeconc.2023.100036>
9. Model code of practice. URL: <https://fintrac-canafe.canada.ca/guidance-directives/sharing-exchange/code-eng> (дата звернення: 19.08.2026).
10. Proceeds of Crime (Money Laundering) and Terrorist Financing Act. URL: <https://laws-lois.justice.gc.ca/PD-F/P-24.501.pdf> (дата звернення: 19.08.2026).
11. Regulation (EU) 2024/1624 of the European Parliament and of the Council. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1624&qid=1750850409685> (дата звернення: 19.08.2026).

References:

1. Brewczyńska M. (2021) Financial Intelligence Units: Reflections on the applicable data protection legal framework. *Computer Law & Security Review*, no 43. DOI: <https://doi.org/10.1016/j.clsr.2021.105612>
2. Financial Services and Markets Act. Available at: <https://sso.agc.gov.sg/Acts-Supp/19-2023/Published/20230628?DocDate=20230628> (accessed August 19, 2026).
3. Guidelines to MAS Notice FSM-N02 on Prevention of Money Laundering and Countering the Financing of Terrorism – Financial Institutions' Information Sharing Platform. Available at: <https://www.mas.gov.sg/regulation/guidelines/guidelines-to-mas-notice-fsm-n02-on-prevention-of-ml-and-countering-tf--fi-info-sharing-platform> (accessed August 19, 2026).
4. Legrand T., Leuprecht, C. (2021) Securing cross-border collaboration: transgovernmental enforcement networks, organized crime and illicit international political economy. *Policy and Society*, no 40 (4), pp. 565–586. DOI: <https://doi.org/10.1080/14494035.2021.1975216>

5. Li Y., Ranbaduge, T., Ng, K. S. (2026) Privacy technologies for financial intelligence. *Journal of Economic Criminology*, no 13. DOI: <https://doi.org/10.1016/j.jeconc.2026.100235>
6. Malala J., Azinge-Egbiri, N., Sunmoni, A. (2026) Inter-agency collaborations and the governance of financial intelligence in Nigeria and Kenya. *Journal of Economic Criminology*, no 13. DOI: <https://doi.org/10.1016/j.jeconc.2026.100234>
7. MAS Launches COSMIC Platform to Strengthen the Financial System's Defence Against Money Laundering and Terrorism Financing. Available at: <https://www.mas.gov.sg/news/media-releases/2024/mas-launches-cosmic-platform> (accessed August 19, 2026).
8. McNaughton K. J. (2023) The variability and clustering of Financial Intelligence Units (FIUs) – A comparative analysis of national models of FIUs in selected western and eastern (post-Soviet) countries. *Journal of Economic Criminology*, no 2. DOI: <https://doi.org/10.1016/j.jeconc.2023.100036>
9. Model code of practice. Available at: <https://fintrac-canafe.canada.ca/guidance-directives/sharing-echange/code-eng> (accessed August 19, 2026).
10. Proceeds of Crime (Money Laundering) and Terrorist Financing Act. Available at: <https://laws-lois.justice.gc.ca/PDF/P-24.501.pdf> (accessed August 19, 2026).
11. Regulation (EU) 2024/1624 of the European Parliament and of the Council. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1624&qid=1750850409685> (accessed August 19, 2026).

Дата надходження статті: 20.08.2026

Дата прийняття статті: 18.09.2026

Дата публікації статті: 07.10.2026