Аналітичні матеріали

Січень 2026 року

Залучення партнерств і технологій для боротьби з грошовими мулами

Олів'є Крафт і Марта Попик

RUSI

CENTER FOR FINANCIAL INTEGRITY | ЦЕНТР ФІНАНСОВОЇ ЦІЛІСНОСТІ

Відмова від відповідальності

Зміст цієї публікації надається лише для загального ознайомлення. Його не слід розглядати як пораду, на яку можна покладатися. Перед вчиненням будь-яких дій або утриманням від них на підставі матеріалів цієї публікації слід отримати професійну консультацію.

Думки, висловлені в цій публікації, належать її авторам і не обов'язково відображають погляди RUSI чи будь-якої іншої установи.

У максимально повному обсязі, дозволеному законом, RUSI не несе відповідальності за будь-які прямі чи непрямі, передбачувані або непередбачувані збитки чи шкоду будь-якого характеру (зокрема пов'язані з дифамацією), що виникають унаслідок або у зв'язку з відтворенням чи використанням цієї публікації або будь-якої інформації, що в ній міститься, вами або будь-якою третьою стороною. Згадки про RUSI поширюються на її директорів, довірених осіб та співробітників.

© 2026 Королівський Об'єднаний інститут оборонних досліджень

Ця робота ліцензована відповідно до Міжнародної ліцензії Creative Commons "Із зазначенням авторства – Некомерційна – Без похідних творів" 4.0. Для отримання додаткової інформації перейдіть за посиланням <http://creativecommons.org/licenses/by-nc-nd/4.0/>.

Аналітичні матеріали RUSI, січень 2026 р.

Команда з питань публікацій

Редакція

Директор з публікацій: Еліс Траунсер

Головний редактор: Сара Хадсон

Помічник редактора: Софі Боултер

Дизайн

Графічний дизайнер: Ліза Вестторп

Редакція досліджень

Керівник з питань управління дослідженнями та редакційної діяльності: Еліас Форнеріс

Обкладинка: надано Adobe Stock / mitarart

Контакти

www.rusi.org

enquiries@rusi.org

+44 (0)207 747 2600

Королівський Об'єднаний інститут оборонних досліджень

Уайтхолл, 61, Лондон

SW1A 2ET

Сполучене Королівство

Слідуйте за нами

Огляд

9 та 10 грудня 2025 року Центр фінансів та безпеки при RUSI та Центр фінансової цілісності (ЦФЦ) провели третю зустріч Робочої групи з питань державно-приватного партнерства у боротьбі з фінансовими злочинами в Україні. П’ятдесят учасників, серед яких були представники державного та приватного секторів України, а також низка міжнародних експертів, зібралися у Варшаві на дводенну серію очних зустрічей. Обговорення зосередилися на використанні так званих "грошових мулів" в Україні, а також на наявних заходах пом’якшення ризиків, що пропонуються державно-приватними партнерствами (ДПП) та регуляторними технологіями (RegTech).

Учасники розробили рекомендації щодо розуміння, запобігання, виявлення та реагування на загрозу грошових мулів в Україні. Цей аналітичний матеріал узагальнює основні висновки зустрічі. Жодне з обговорень, що відбулися на зустрічі, не стосується жодної конкретної особи чи організації. Якщо не вказано інше, заяви, що містяться в цьому документі, відображають питання, підняті в ході обговорень.

© Королівський Об'єднаний інститут оборонних досліджень

Вступ

Як зазначено в нещодавній публікації ЦФЦ, схеми за участю грошових мулів стали серйозною проблемою фінансових злочинів в Україні, особливо після початку повномасштабного вторгнення Росії.

Грошові мули — це фізичні особи, чиї банківські рахунки, платіжні картки або персональні дані використовуються для переміщення незаконно здобутих коштів, але самі вони зазвичай не залучені до основної злочинної діяльності, що генерує дохід, або предикатних злочинів. Дехто свідомо дозволяє використовувати свої рахунки в обмін на грошову винагороду, тоді як інші виявляються залученими через обман або без повного розуміння наслідків. У всіх випадках рахунки грошових мулів використовуються для фрагментації фінансових потоків і ускладнення відстеження незаконної діяльності.

У документі ЦФЦ розглядається вплив загрози грошових мулів на окремих осіб, фінансову систему та державні фінанси. За оцінками, щорічно через схеми грошових мулів проходить понад 200 мільярдів гривень (4,8 мільярда доларів), що призводить до втрати податкових надходжень на суму до 50 мільярдів гривень (1,25 мільярда доларів). Ці втрати безпосередньо впливають на ресурси для військових потреб, соціальних послуг та відновлення.

© Королівський Об'єднаний інститут оборонних досліджень

Розуміння загрози

Під час зустрічі було зазначено, що всебічне розуміння природи та загального середовища діяльності грошових мулів є необхідною передумовою для ефективного реагування.

Типології грошових мулів

Не існує єдиного профілю грошового мула. Хоча часто вважається, що грошові мули, як правило, молоді або літні люди, один з учасників повідомив, що люди у віці від 25 до 40 років також стають дедалі вразливішими до цієї загрози. Деякі учасники наголосили на відмінності між особами, які не усвідомлюють, що їхні рахунки використовуються в незаконних цілях, і тими, хто свідомо дозволяє використовувати свої рахунки або платіжні інструменти в обмін на грошову винагороду. У будь-якому випадку фізичні особи часто не до кінця розуміють юридичні та фінансові наслідки такої діяльності.

Обговорювані методи вербування охоплювали цілий ряд шахрайських дій і методів соціальної інженерії. Наприклад, деяких осіб вводили в оману, переконуючи, що вони допомагають внутрішньо переміщеним особам зі сходу України, які нібито не мають доступу до банківських послуг. Методи вербування швидко адаптуються до соціальних умов, і їм важко протистояти за допомогою статичного контролю.

Учасники також підкреслили, що для вербування грошових мулів часто використовуються соціальні мережі і месенджери. Високий рівень цифровізації в Україні був описаний як фактор, що посилює охоплення онлайн-реклами, що пропонує придбати банківські картки або рахунки, іноді з підробленими банківськими логотипами.

У відповідь на ці ризики в останні роки було запроваджено обмеження щодо роздрібних банківських продуктів для молодих клієнтів, зокрема рахунків, доступних особам віком 14–16 років, які не несуть кримінальної відповідальності за законодавством України й тому можуть перебувати в групі підвищеного ризику залучення як грошові мули. Однак, як зазначалося вище, учасники відзначили, що зусилля з вербування змістилися в бік інших вікових груп.

© Королівський Об'єднаний інститут оборонних досліджень

Предикатні злочини та злочинні мережі

Учасники застерегли від того, щоб розглядати грошових мулів ізольовано. Діяльність грошових мулів була описана як один з елементів ширших злочинних систем, а не як окремий, самостійний вид злочину. Під час обговорень схеми з використанням грошових мулів були пов'язані з численними предикатними злочинами, що генерують доходи, одержані злочинним шляхом, зокрема із шахрайством та ухиленням від сплати податків. Поширеність неформальної економічної діяльності та ухилення від сплати податків сприяє формуванню середовища, у якому можуть функціонувати схеми із залученням грошових мулів, що свідчить про наявність глибших структурних проблем за межами фінансового сектору.

Учасники не дійшли консенсусу щодо типових джерел і напрямів руху доходів, одержаних злочинним шляхом, що відмиваються через мережі грошових мулів в Україні, а також щодо того, до якої з трьох наведених категорій вони найчастіше належать: доходи, отримані в Україні та залишені в країні; доходи, отримані за межами України та відмиті через українські рахунки; або доходи, отримані в Україні та переказані за кордон.

Транснаціональні організовані злочинні групи навмисно використовують для схем із грошовими мулами ті юрисдикції, де процеси відкриття рахунків є швидкими, а моніторинг трансакцій — менш суворим, оскільки в таких країнах транзакції важче відстежити. Учасники зустрічі погодилися, що деякі фінансові установи України пропонують майже миттєве відкриття рахунків з обмеженими початковими перевірками, покладаючись переважно на моніторинг уже після залучення клієнта. Вони відзначили, що більш суворе застосування в Україні вимог "Знай свого клієнта" (KYC) на етапі реєстрації може значно знизити кількість випадків неправомірного використання рахунків для виведення грошей.

Типології грошових мулів можуть дати уявлення про структуру та рівень складності основної злочинної діяльності, допомагаючи фінансовим установам і правоохоронним органам краще виявляти та розслідувати таку діяльність. Наприклад, було наведено емпіричне дослідження, проведене в Нідерландах, щоб проілюструвати, як грошові мули діють в рамках ширших злочинних мереж. Дослідження, засноване на даних банківських транзакцій, показує, що грошові мули зазвичай перебувають на периферії злочинних мереж і використовуються для приховування зв'язків з організаторами. Дослідження розрізняє менш технологічні схеми, що спираються на більшу кількість переважно місцевих грошових мулів, і складніші схеми, які зазвичай залучають менше мулів і активніше використовують міжнародні або бізнес-рахунки.

© Королівський Об'єднаний інститут оборонних досліджень

Рівень загрози

Серед учасників не було єдиної думки щодо того, збільшується чи зменшується загальна кількість грошових мулів в Україні. Деякі учасники повідомили про щорічне збільшення кількості виявлених випадків, тоді як інші описували зміни в типології та методах вербування, а не явне зростання абсолютних показників.

Досягнення спільного взаєморозуміння

Учасники дійшли згоди, що потрібно подальше дослідження для глибшого розуміння масштабу та рушійних чинників діяльності грошових мулів, зокрема організаторів (так званих "пастухів"), які займають центральне місце в мережах грошових мулів. Поліпшення збору даних, аналізу та обміну інформацією між державним та приватним секторами було визнано необхідним для створення більш точної та всебічної картини загрози.

Було висловлено занепокоєння щодо обмеженості каналів зв'язку між НУО, банками, платформами та державними органами. Учасники описували процес повідомлення про шахрайський контент як ресурсозатратний, оскільки адміністративні можливості для обробки великої кількості випадків обмежені.

Обговорювалися питання ДПП як засобу консолідації інформації між різними установами. Наприклад, Литовський Центр передового досвіду з питань протидії відмиванню коштів (AML) організовує регулярні зустрічі між банками, службою фінансової розвідки, поліцією та іншими зацікавленими сторонами, а також публікує узагальнені дані про виявлені випадки та збитки, яких вдалося уникнути.

© Королівський Об'єднаний інститут оборонних досліджень

Виявлення та реагування

Велику частину обговорення було присвячено заходам, які впроваджують державні та приватні учасники в Україні та світі для виявлення та протидії діяльності грошових мулів відповідно до стандартів AML та заходів контролю за шахрайством.

Поточні зусилля в Україні

Експерти з України розповіли про заходи, які вони вжили для зниження ризиків, пов'язаних з грошовими мулами, під наглядом Національного банку України (НБУ). Ці заходи охоплюють:

- **Оцінка ризиків.** Під час реєстрації нових клієнтів українські банки збирають їхні ідентифікаційні дані безпосередньо від клієнтів та доповнюють їх інформацією з зовнішніх джерел: державних реєстрів, застосунку "Дія", системи BankID, агрегаторів даних, а також відкритих джерел і медіа для формування початкового профілю ризику. Потім ці дані поєднуються з даними моніторингу транзакцій та обслуговування клієнтів для оцінки загального ризику для клієнтів. Оцінки ризиків різняться в різних установах, що відображає відмінності в схильності до ризику та історії клієнтів, а це означає, що різні банки можуть по-різному оцінювати одну і ту ж особу.
- **Сценарії.** Банки розробляють і постійно оновлюють сценарії, які можуть свідчити про використання клієнта як грошового мула або на етапі відкриття рахунку або на пізніших етапах його обслуговування. Останню ситуацію було охарактеризовано як таку, що важче виявити чи передбачити, оскільки клієнт, який пізніше дозволяє використовувати свій рахунок третім особам, зазвичай має низький профіль ризику.
- **RegTech.** Рішення RegTech можуть бути використані для об'єднання даних з декількох джерел (зокрема, дані KYC, дані про транзакції та інформацію про пристрій) для виявлення поведінки, яка може вказувати на активність грошових мулів. Деякі банки зазначили, що поряд із традиційним

AML-моніторингом вони використовують контроль на основі пристроїв, який включає відстеження змін пристроїв і електронних адрес, а також постійне оновлення сценаріїв виявлення підозрілої діяльності.

Учасники визнали обмеженість заходів, що вживаються банками окремо, враховуючи, що грошові мули можуть обійти такі заходи, перевівши свою діяльність в інший банк. Крім того, злочинці, які здійснюють схеми з грошовими мулами, часто розподіляють свою діяльність між кількома банками, щоб уникнути виявлення. Дві ініціативи спрямовані на зниження цього ризику.

По-перше, банки підписали Меморандум про взаєморозуміння (MoU), який гармонізує окремі практики управління ризиками серед банків, зокрема обмеження переказів з карти на карту. Учасники відзначили, що ці обмеження мали відчутний вплив на скорочення великої кількості переказів з низькою вартістю; однак злочинні групи адаптувалися, переводячи потоки транзакцій на інші типи рахунків і канали.

По-друге, законопроєкт передбачає створення реєстру грошових мулів, який має на меті запобігти участі однієї особи у діяльності грошових мулів у кількох банках. Деталі впровадження реєстру ще перебувають на розгляді — серед факторів, які потрібно врахувати, є вимоги до захисту даних, а також необхідність мінімізувати можливі непередбачені наслідки для невинних осіб, чиї рахунки або особисті дані могли бути використані без їхнього відома.

Учасники застерегли від надмірно обмежувальних підходів. За словами одного з учасників, кожна третя скарга, що надходить до Управління захисту прав споживачів фінансових послуг НБУ, стосується відмов у наданні банківських послуг.

Мережева аналітика

Міжнародні учасники підкреслили важливість мережевої аналітики (аналізу зв'язків між фізичними та юридичними особами) при розслідуванні грошових мулів.

Очікуваний ефект

Грошові мули зазвичай перебувають на найнижчому рівні складних злочинних мереж. Усунення окремих грошових мулів може сприяти дезорганізації діяльності таких мереж. Водночас якщо зусилля зосереджуються виключно на грошових мулах без належного реагування на злочинні організації, яким вони (усвідомлено або неусвідомлено) слугують, існує ризик, що ці організації продовжать свою діяльність, просто залучаючи нових мулів. Мережева

© Королівський Об'єднаний інститут оборонних досліджень

аналітика є критично важливою для виявлення організаторів, а тому цей напрям має бути пріоритетним.

Крім того, мережева аналітика може допомогти краще зрозуміти масштаби проблеми, зв'язки з типовими злочинами, а також походження та призначення коштів.

Реалізація

Один із міжнародних банків, представлених на зустрічі, застосовує мережевий підхід до кожного розслідування, зокрема й до справ, пов’язаних із грошовими мулами. На основі всіх доступних даних, зокрема ідентифікаторів пристроїв, транзакцій та поведінки клієнтів, вибудовуються зв’язки між елементами.

Ідентифікатори пристроїв дають змогу виявляти закономірності, релевантні для виявлення діяльності грошових мулів, наприклад:

- Кількість пристроїв, з яких здійснюється доступ до одного банківського рахунку. Більшість клієнтів використовують від трьох до чотирьох пристроїв (таких як комп'ютер, телефон і планшет). Якщо до одного рахунку під'єднано понад 20 ідентифікаторів пристроїв, це говорить про те, що до нього мають доступ більше одного користувача, а отже, це може бути рахунок грошового мула.
- Кількість клієнтів на один пристрій. Використання одного й того самого пристрою для доступу до кількох рахунків є ще одним індикатором ризику, оскільки це може свідчити про те, що відповідний пристрій використовується злочинною групою для управління кількома рахунками грошових мулів.

Транзакції допомагають ідентифікувати всіх контрагентів. Далі може застосовуватися мережева аналітика для визначення того, з ким ще взаємодіють такі контрагенти; у результаті це часто дає змогу виявити мережу взаємопов’язаних осіб.

Поведінка клієнта та матеріали належної перевірки можуть виявити додаткові зв’язки, що виходять за межі використання пристроїв та здійснення транзакцій.

Результати мережевої аналітики багато в чому залежать від якості та повноти базового набору даних. Це означає, що мережа, побудована на основі часткової інформації (наприклад, даних, доступних одному банку), буде менш повною і матиме менше виявлених зв’язків, ніж мережа, що базується на даних із кількох фінансових установ. Враховуючи взаємозв'язок між обсягом даних і результатами, в ході обговорення були розглянуті шляхи розвитку партнерських відносин між суб'єктами приватного сектора або між державним і приватним секторами.

© Королівський Об'єднаний інститут оборонних досліджень

Розкриття потенціалу партнерських відносин

Як зазначалося вище, в Україні були вжиті різні заходи для розробки спільних заходів реагування на загрозу грошових мулів, серед яких меморандум про взаєморозуміння щодо грошових мулів і потенційний реєстр шахрайських рахунків. Спираючись на ці ініціативи, учасники визначили різні способи підвищення рівня та ефективності співпраці між приватними структурами, а також між державним і приватним секторами у сфері виявлення грошових мулів та реагування на цю загрозу.

Нормативно-правова база

Учасники визнали важливість нормативно-правової бази для стимулювання обміну інформацією та обговорили приклади з інших юрисдикцій.

Європейський союз

Стаття 75 Регламенту ЄС про протидію відмиванню коштів 2024 року (AMLR) є основою для створення партнерств приватного сектору або державно-приватних партнерств у сфері протидії відмиванню коштів. У преамбулі статті 75 прямо визнається ключова роль таких партнерств:

«Обмін інформацією між суб'єктами, зобов'язаними дотримуватися вимог, та, за необхідності, компетентними органами, може збільшити можливості виявлення незаконних фінансових потоків, пов'язаних з відмиванням коштів, фінансуванням тероризму та доходами від злочинів. З цієї причини суб'єкти, зобов'язані дотримуватися вимог, та компетентні органи повинні мати змогу обмінюватися інформацією в рамках партнерства, якщо вони вважають такий обмін необхідним для виконання своїх обов'язків у сфері AML/CFT [протидії фінансуванню тероризму]. Обмін інформацією має здійснюватися з дотриманням надійних гарантій конфіденційності, захисту даних, обмежень використання інформації та процесуальних норм кримінального провадження.»

Ще до набрання чинності статті 75 багато країн-членів ЄС вже розробили правову основу для обміну інформацією.

У контексті процесу вступу України до ЄС міжнародні учасники закликали Україну розглянути питання про те, як стаття 75 може бути реалізована в українському контексті.

Велика Британія

Відповідно до законодавства Великої Британії можливі різні форми обміну інформацією.

По-перше, розділи 339ZB-339ZG Закону про доходи від злочинної діяльності 2002 року (POCA) передбачають обмін інформацією в рамках регульованого сектора в контексті зусиль по боротьбі з відмиванням грошей. Ініціатором обміну інформацією може виступати Національне агентство з боротьби зі злочинністю (NCA), зокрема в рамках так званих «ф'южн-центрів», як-от державно-приватне партнерство 2024 року, метою якого було виявлення злочинної діяльності за допомогою банківських даних. Співробітники фінансових установ, що беруть участь у проєкті, відряджаються до цих ф'южн-центрів, складають присягу та отримують доступ до об'єднаних даних. Водночас після направлення до ф'южн-центру вони не мають права безпосередньо передавати банку отримані висновки — усі повідомлення мають надходити через NCA.

По-друге, згідно з вищезазначеними положеннями POCA, банки також можуть ініціювати обмін інформацією, дотримуючись суворих умов, коли інформація необхідна для складання звіту про підозрілу діяльність (SAR). Такий обмін дозволяє банку-ініціатору запиту зібрати більше інформації та надати повніший SAR. Інформацію також можна використати для подання спільного повідомлення, яке іноді називають "супер-SAR" — тобто SAR, який ґрунтується на даних від кількох установ. Проте на практиці спільні повідомлення залишаються рідкісними, оскільки банки не охоче покладаються на іншу установу для виконання власного обов'язку звітування.

По-третє, Закон про економічні злочини та корпоративну прозорість 2023 року (ECCTA) дозволяє обмінюватися інформацією між приватними особами щодо всіх форм економічних злочинів. Цей закон дозволяє не застосовувати цивільну відповідальність та Загальний регламент про захист даних (GDPR), якщо дотримуються певні умови (наприклад, коли обидві організації обслуговують одного й того самого клієнта та вжиті заходи для захисту та обмеження доступу до рахунку). Інформація може передаватися безпосередньо (розділ 188) або через сторонню платформу (розділ 189).

Відповідність обміну інформацією вимогам захисту даних та іншим правилам

Хоча під час обговорень на зустрічі було відзначено потенційні суперечності між обміном інформацією та вимогами щодо захисту даних і іншими нормативними положеннями, було представлено низку практичних прикладів, які продемонстрували, що обмін інформацією може здійснюватися з дотриманням цих вимог. Найчастіше саме правова невизначеність, а не юридичні бар'єри,

перешкоджає обміну інформацією між організаціями приватного сектора. Було відзначено, що *відсутність* обміну інформацією не дозволяє фінансовим установам проводити високоякісні розслідування і, отже, може призвести до подачі великої кількості неякісних SAR. Це, своєю чергою, може бути порушенням статті 8 Європейської Конвенції з прав людини, враховуючи обсяг персональних даних, які розкривають ці SAR.

Один з учасників підкреслив важливість того, щоб регуляторні органи або служби фінансової розвідки давали чіткі настанови про те, який вид обміну інформацією є допустимим, а який ні. Одним із наведених прикладів були настанови, оприлюднені у вересні 2025 року службою фінансової розвідки США — Мережею з протидії фінансовим злочинам (Financial Crimes Enforcement Network). Метою цих настанов є: "(i) роз'яснити, що Закон про банківську таємницю та нормативні акти щодо його впровадження (разом — "BSA"), як правило, не забороняють транскордонний обмін інформацією; та (ii) навести приклади інформації, яка зазвичай не розкриває факт подання звіту про підозрілу діяльність і, отже, обмін якою не заборонений BSA.

У Великій Британії настанови щодо заходів з обміну інформацією, передбачених ECCTA, описаних вище, були оприлюднені у жовтні 2024 року Міністерством внутрішніх справ, Міністерством фінансів (HM Treasury) та офіційним урядовим реєстром британських компаній (Companies House) за участі інших міністерств і відомств, а також оновлені у жовтні 2025 року. Метою цих настанов є сприяння суб'єктам регулювання у "використанні нових положень щодо обміну інформацією, передбачених статтями 188 і 189".

Обидва ці документи-настанови було охарактеризовано як приклад доброї практики, на який регулятори інших країн могли б орієнтуватися. Такі настанови дають змогу банкам та іншим установам розуміти, якою інформацією вони можуть обмінюватися як на національному, так і на міжнародному рівні відповідно до чинного законодавства.

Використання технологій для забезпечення обміну інформацією

В Україні банки вже використовують цифрову платформу для обміну ознаками ризику в режимі реального часу без передачі персональних даних. Платформа Української міжбанківської асоціації членів платіжних систем дозволяє обмінюватися ознаками шахрайства, типологіями та оновленнями щодо нових ознак шахрайської діяльності в банківському секторі.

Міжнародні учасники згадали про технологічні рішення, які дозволяють забезпечити ширший обмін інформацією.

© Королівський Об'єднаний інститут оборонних досліджень

Один з учасників описав успішний досвід використання захищених каналів для забезпечення обміну інформацією між банками (зокрема транскордонного) із дотриманням вимог GDPR. Реалізація таких рішень залежить від багатьох факторів, зокрема:

- Тісна координація між усіма відповідними групами всередині установи дозволяє узгоджено охоплювати всі технологічні, юридичні та операційні аспекти.
- Розуміння того, яку інформацію можна передавати в межах відповідної юрисдикції (юрисдикцій).
- Чітко визначений варіант використання (наприклад, об'єднання баз даних номерів шахрайських рахунків, обмін повідомленнями між слідчими з установ-учасниць або спільні розслідування).
- Належним чином оформлена угода про правила використання між учасниками.
- Лідерство з боку невеликої групи банків або банківської асоціації, здатної протестувати концепцію перед її ширшим впровадженням.

Один з учасників процитував користувача платформи, який описав, як координація дій між одним із найбільших банків Скандинавії та одним із найбільших банків Балтійського регіону дозволила вчасно заблокувати рахунок грошового мула та повернути жертві телефонного шахрайства €100200.

Інший учасник звернув увагу на зростання кількості операторів платіжних систем, які застосовують рішення RegTech для відстеження потоків коштів грошових мулів між учасниками платіжних систем у режимі реального часу. Такі можливості відстеження підвищують імовірність повернення коштів до того, як вони будуть зняті готівкою, переказані за кордон або конвертовані у віртуальні активи, після чого їхнє повернення стає значно складнішим. До юрисдикцій, які впровадили можливості відстеження для систем швидких платежів, належать Велика Британія та Малайзія.

Як один із варіантів також було згадано федеративне навчання, що дає змогу забезпечити спільну протидію використанню грошових мулів без необхідності обміну персональними даними. Хоча існують різні способи реалізації, федеративне навчання зазвичай означає тренування моделі машинного навчання на основі окремих наборів даних, що можуть належати різним установам. За словами одного з учасників, стаття 75 AMLR може слугувати правовою підставою для федеративного аналізу клієнта, який може мати рахунки в кількох установах. Наприклад, третя сторона може проаналізувати федеративні дані (необроблені дані або сигнали про ризики) з різних установ, щоб виявити закономірності, які можуть бути непомітні для кожної установи окремо.

© Королівський Об'єднаний інститут оборонних досліджень

Тематичні дослідження

Учасники виділили два проєкти ДПП, координовані Європолом.

Європейська кампанія з протидії грошовим мулам (European Money Mule Action, EMMA)

Європейська кампанія з протидії відмиванню коштів за підтримки Європолу — це транскордонне державно-приватне партнерство, спрямоване на масштабне припинення діяльності мереж грошових мулів. У період з 2016 по 2024 рік правоохоронні органи та фінансові установи країн ЄС та країн, що не входять до його складу, провели низку скоординованих операцій, що призвели до арештів грошових мулів та їх вербувальників. Ефективність EMMA є результатом обміну інформацією між усіма партнерами, що дозволяє правоохоронним органам ідентифікувати мережі та приймати рішення щодо найбільш ефективної стратегії ліквідації. Операція EMMA у 2021 році призвела до 1803 арештів та виявлення понад 18 000 грошових мулів.

EMMA спирається на попередній досвід аналогічної державно-приватної ініціативи в Нідерландах. Зазначалося, що ця ініціатива суттєво скоротила кількість грошових мулів, зробивши країну менш привабливою для такої діяльності.

Робоча група з питань грошових мулів у межах EFIPPP

Фінансово-розвідувальне державно-приватне партнерство Європолу (EFIPPP) нещодавно започаткувало робочу групу з питань грошових мулів за участі представників державного та приватного секторів. Учасники від приватного сектору діляться даними про другий рівень руху коштів — тобто про те, куди спрямовуються доходи від шахрайства після першого переказу з рахунку жертви. Учасники не розкривають жодних персональних даних бенефіціарів (отримувачів), натомість надають інформацію про фінансові установи, у яких відкриті відповідні рахунки. Завдяки агрегованим даним від усіх учасників робоча група виявляє банки, які мають вищий рівень вразливості до діяльності грошових мулів (і які можуть не бути членами EFIPPP). Ці висновки стають основою для подальшої взаємодії з відповідними банками щодо їхніх слабких місць та якості їхніх механізмів контролю.

© Королівський Об'єднаний інститут оборонних досліджень

Превентивні заходи на ранніх етапах

Окрім виявлення та правозастосування, боротьба з діяльністю грошових мулів потребує заходів, що діють на ранніх етапах, тобто ще до спроби здійснення будь-якої фінансової операції. Учасники обговорили роль просвітницьких кампаній та зусиль із підвищення фінансової грамотності, а також заходи стримування.

Освітні заходи

Освіта та фінансова грамотність були визначені як ключові превентивні інструменти для зниження вразливості до вербування грошових мулів.

Учасники підкреслили, що обмежена обізнаність про ризики фінансових злочинів, особливо серед молоді, підвищує ризик вербування. З огляду на це, банки, державні органи та правоохоронні органи в Україні вжили заходів для інформування клієнтів про ризики та наслідки використання їхніх рахунків у протиправних цілях, зокрема:

- Банки реалізували низку освітніх ініціатив, орієнтованих на молоду аудиторію, включаючи інформаційну роботу в школах та проведення занять зі студентами та учнями віком від 14 років. Це, зокрема, передбачає демонстрацію навчальних відео, орієнтованих на конкретні категорії клієнтів, а також надання прямих рекомендацій щодо умов користування рахунками.
- Кампанія з підвищення обізнаності громадськості #FraudstersGoodbye зосереджена на ризиках шахрайства та використання грошових мулів, пов'язаних із передаванням банківських реквізитів третім особам. Кампанія містить інтерактивні освітні матеріали, розроблені для використання в системі державної освіти, і кілька учасників зустрічі відзначили їхнє активне впровадження на практиці. Важливо, що ця інформаційна кампанія реалізується у форматі партнерства між державним і приватним секторами за участі мобільних операторів, державних міністерств, банків та приватного бізнесу.

- Кіберполіція проводила лекції у закладах вищої освіти, а також навчальні заходи для прокурорів щодо методів вчинення високотехнологічних фінансових злочинів.

Представники з України наголосили на важливості визначення найбільш ефективних каналів для підвищення обізнаності, зокрема тих, через які здійснюється вербування, — таких як соціальні мережі та месенджери. Також було зазначено, що окремі групи населення можуть мати обмежений рівень довіри до банків або органів державної влади, що знижує ефективність офіційних кампаній, які реалізуються такими установами.

Робота Організації економічного співробітництва та розвитку (ОЕСР) у сфері фінансової грамотності, зокрема її звіт "Застосування поведінкових інсайтів у програмах та ініціативах із фінансової грамотності та навчання інвесторів", була відзначена як корисна для розробки ефективніших програм, адаптованих до різних вікових груп. Поведінкові інсайти можуть бути основою для розробки ініціатив із фінансової грамотності, виходячи за межі простого надання інформації та включаючи переконання, стимулювання та інші поведінкові втручання, здатні впливати на прийняття фінансових рішень. Цифрові інструменти, зокрема рішення на основі штучного інтелекту, також можуть сприяти створенню більш персоналізованих повідомлень і дозволяють адаптувати освітній контент до форматів і платформ, якими зазвичай користується молода аудиторія.

Насамкінець, учасники наголосили на важливості оцінювання впливу освітніх та інформаційних заходів, зокрема шляхом проведення опитувань та інтерв'ю з самими грошовими мулами.

Стримування

Деякі учасники висловили занепокоєння через те, що вироки за кримінальними справами для грошових мулів сприймаються як рідкісні або занадто м’які. Це може послаблювати ефект стримування та сприяти уявленню, що особи, які надають свої рахунки у користування, майже не стикаються з правовими наслідками, особливо якщо йдеться про перші випадки або незначні суми.

Ще одним фактором, що сприяє м’якості вироків, є складність доведення в певних справах наявності необхідного злочинного умислу — тобто усвідомлення особою того, що її рахунок буде використано для злочинних цілей.

На цьому тлі деякі учасники стверджували, що до Статті 200 Кримінального кодексу України, яка стосується незаконних дій із платіжними інструментами, слід внести зміни для посилення її дієвості та ефекту стримування. Інші учасники застерігали від небажаних наслідків підходу, зосередженого на

© Королівський Об'єднаний інститут оборонних досліджень

засудженні грошових мулів. Було висловлено занепокоєння щодо ризику винесення великої кількості вироків, особливо серед молоді, та впливу, який це може мати на її майбутній доступ до фінансової системи взаємодію з нею.

Роль державно-приватного партнерства в освіті

Учасники також обговорили потенційну роль державно-приватних партнерств у забезпеченні скоординованої та ефективної комунікації з громадськістю для підвищення обізнаності. Як було зазначено раніше, Литовський Центр передового досвіду з питань протидії відмиванню коштів (Centre of Excellence in AML) збирає дані від банків, а потім використовує їх для регулярної публічної комунікації, включаючи пресрелізи та постійну взаємодію з національним телебаченням і онлайн-медіа, щоб підтримувати високий рівень обізнаності населення про фінансові загрози.

Учасники дійшли спільної думки: для того, щоб кампанії з підвищення обізнаності були ефективними, партнерства мають виходити за межі банків та державних органів і залучати також організації громадянського суспільства та компанії-власники соціальних мереж. Взаємодія з цими додатковими зацікавленими сторонами може допомогти у розповсюдженні навчальних матеріалів по каналах, які найчастіше використовуються групами ризику.

© Королівський Об'єднаний інститут оборонних досліджень

Наступні кроки

Як зазначено в цьому звіті, окремі елементи державно-приватного співробітництва вже існують в Україні. Однак ефективність цих зусиль залежатиме від готовності зацікавлених сторін перейти від ситуативної (ad hoc) взаємодії та обговорень до системного, операційного та стійкого партнерства як наступного кроку.

Для розбудови таких партнерств міжнародні експерти рекомендували опиратися на перевірені канали співпраці, можливо, у межах вузького кола установ, і розпочати з чітко визначених практичних кейсів, таких як боротьба з грошовими мулами. Вони також закликали українські зацікавлені сторони розширювати кордони та розглядати партнерство як повторюваний процес, який з часом потребуватиме коригувань.

194 роки незалежного мислення про оборону та безпеку

Королівський Об'єднаний інститут оборонних досліджень (RUSI) — найстаріший у світі та провідний у Великій Британії аналітичний центр з питань оборони та безпеки. Його місія — інформувати, впливати та сприяти більш змістовному громадському обговоренню безпечнішого та стабільнішого світу. RUSI — це науково-дослідний інститут, який проводить незалежний, практичний та інноваційний аналіз, направлений на вирішення складних викликів сьогодення.

З моменту заснування RUSI в 1831 році його діяльність підтримують його члени. Завдяки доходам від досліджень, публікацій і конференцій RUSI зберігає свою політичну незалежність протягом 194 років.

© 2026 Королівський Об'єднаний інститут оборонних досліджень

RUSI зареєстрований як благодійний фонд в Англії та Уельсі

Реєстраційний номер благодійної організації: 210639

Номер платника ПДВ: GB752275038