RUSI EUROPE

Project craaft

Collaboration, Research & Analysis Against the Financing of Terrorism

Аналітична записка (Occasional Paper)

КРОК ЗА КРОКОМ
(Bit by Bit)

Вплив нових технологій на ризики фінансування тероризму

Стівен Раймер, Метью Редхед

КРОК ЗА КРОКОМ

Вплив нових технологій на ризики фінансування тероризму

Стівен Раймер, Метью Редхед

Аналітична записка RUSI, Квітень 2022 року

RUSI EUROPE

Project craaft

Collaboration, Research & Analysis Against the Financing of Terrorism

Штаб-квартира RUSI Europe розташована в Брюсселі. Організація вивчає, просуває, обговорює та висвітлює всі питання, що стосуються міжнародної оборони та безпеки в Європі та за її межами. RUSI Europe тісно співпрацює зі своєю міжнародною материнською організацією RUSI шляхом обміну експертними знаннями та налагодження взаємин із міжнародними заінтересованими сторонами.

191 рік незалежної аналітики у сфері оборони та безпеки

Королівський об'єднаний інститут оборонних досліджень (RUSI) є найстарішим у світі та провідним у Великій Британії аналітичним центром у сфері оборони та безпеки. Його місія полягає в інформуванні, впливі та посиленні суспільних дискусій задля створення безпечнішого й більш стабільного світу. RUSI є дослідницьким інститутом, який готує незалежний, практичний та інноваційний аналіз для вирішення складних викликів сучасності.

Від часу свого заснування у 1831 році RUSI спирається на підтримку своїх членів у здійсненні діяльності. Разом із надходженнями від досліджень, публікацій та конференцій це дозволило RUSI протягом 191 року зберігати політичну незалежність.

Цей проєкт фінансовано за рахунок Фонду внутрішньої безпеки – Європейського Союзу.

Опубліковано у 2022 році Королівським об'єднаним інститутом оборонних та безпекових досліджень.

Аналітична записка RUSI, квітень 2022 року. ISSN 2397-0286 (онлайн).

Зміст

Подяки

Автори висловлюють подяку Тому Кітінджу, Олівії Кірні, Аланні Путце та Кінзі Редловській за їхню підтримку цього дослідницького проєкту, а також Джеммі Роджерс за організацію вебінару, під час якого було представлено та обговорено початкові результати цього дослідження у контексті онлайн-краудфандингу. Дослідження, представлене у цій публікації, є частиною проєкту CRAAFT (Collaboration, Research and Analysis Against the Financing of Terrorism — «Співпраця, дослідження та аналіз у сфері протидії фінансуванню тероризму»).

Про проект CRAAFT

Проєкт CRAAFT є науково-дослідною та комунікаційною ініціативою, спрямованою на зміцнення та координацію спроможностей ЄС і сусідніх країн у сфері протидії фінансуванню тероризму. Проєкт CRAAFT фінансується Фондом внутрішньої безпеки Європейського Союзу та реалізується консорціумом під керівництвом RUSI Europe у співпраці з Амстердамським університетом, братиславським аналітичним центром GLOBSEC і Міжнародним центром з питань протидії тероризму (ICCT), розташованим у Гаазі. Детальніше: projectcraaft.eu

Виконавчий підсумок

Потенційна роль, яку нові технології — від фінансових технологій до соціальних мереж — можуть відігравати у фінансуванні тероризму (ФТ), стає дедалі більшою причиною занепокоєння у колах європейських законотворців. Орієнтовані на швидкість, ефективність і позитивний користувацький досвід, нові технології мають потенціал не лише полегшувати життя пересічних споживачів, а й зменшувати бар'єри, з якими стикаються особи що фінансують тероризм під час фінансування нападів та організаційної діяльності. Віртуальні активи (ВА) — особливо криптовалюти — стали основною сферою занепокоєння як новий вимір ризиків фінансування тероризму.

Водночас нещодавня увага до нових технологій як потенційного каналу фінансування тероризму не призвела до формування єдиної думки щодо масштабів цих ризиків. Дискусія з цього питання розділилася на дві основні позиції: перша виходить із найгірших сценаріїв, припускаючи, що інновації полегшать діяльність осіб, що фінансують тероризм; друга вважає, що нові технології не є ані більш, ані менш ризикованими, ніж уже наявні технології чи традиційні фінансові інструменти.

Розбіжності у поглядах значні, а діалог між цими двома позиціями складно врегулювати через відмінні базові припущення. У першому випадку політики та представники традиційного фінансового сектору, стикаючись із новизною та невизначеністю, вважають найбезпечнішим підходом виходити з того, що теоретичні вразливості та притаманні ризики є реальними, доки не буде доведено протилежне. У другому — ті, хто створює та впроваджує нові технології, схильні вважати, що ризики не слід припускати без доказів, а необхідно їх підтвердити. Для обох сторін ключовим є розуміння сутності та якості наявних доказів.

На тлі цієї дискусії ця записка досліджує, чи створюють нові технології нові ризики фінансування тероризму у Європі або ж посилюють наявні. Попри труднощі зі збиранням даних щодо чутливих терористичних справ, усе ж вдалося сформувати чіткіше уявлення: нові фінансові технології дійсно застосовувалися для закупівлі та фінансування нападів, але з упевненістю це підтверджено лише у незначній частині випадків. Так само платіжні платформи, краудфандинг у соціальних мережах та віртуальні активи стали інструментами ширшого організаційного фінансування, однак вони були додані до вже усталених і традиційних методів, таких як готівка, використання посередників чи компаній, що надають грошові послуги, а не замінили їх.

Загалом нові технології стали частиною діяльності з фінансування тероризму в межах Європи, але менш революційним чином, ніж побоювалися багато політиків.

Вступ

У 1992 році британець із південного Лондона Бабар Ахмад, працюючи гуманітарним працівником на Балканах, став свідком жахливого насильства, вчиненого проти боснійських мусульман.[1] Згодом він створив вебсайт, основною метою якого було публікувати матеріали про конфлікти в Боснії та Чечні, але який також закликав надавати підтримку, фінансову та іншу, руху «Талібан» в Афганістані.[2] Відтоді використання інтернету для фінансування тероризму розвивалося паралельно з поширенням нових інтернет-технологій. Онлайн-чати поступилися місцем платформам миттєвого обміну повідомленнями, так само як спеціалізовані вебсайти були витіснені соціальними мережами як засобом охоплення широкої аудиторії прихильників.

Особливе занепокоєння сьогодні викликає низка технологій, які, взаємодіючи з фінансовою системою, розглядаються як такі, що становлять окремі ризики фінансування тероризму. Ризики, пов'язані з віртуальними активами (ВА), широко обговорювалися, так само як і потенціал онлайн-краудфандингових платформ для використання у ФТ.[3] Менш чітко окресленими залишаються ризики, що походять від продуктів і послуг фінансових технологій (FinTech), зокрема «челенджер-банків» (challenger banks) та постачальників платіжних послуг, які є основою значної частини сучасної фінансової системи.

Соціальні медіа (такі як соціальні мережі та платформи для розміщення контенту) і засоби онлайн-комунікації також можуть бути використані зловмисниками для підтримки діяльності з фінансування тероризму. Інші інновації, зокрема вебсайти електронної комерції, фігурували в оперативному плануванні самостійно діючих терористів у Європі, наприклад, під час придбання деталей для саморобного вибухового пристрою, використаного під час теракту на «Манчестер Арені» у 2017 році.[4] Водночас ризики, пов'язані з віртуальними активами, краудфандингом, фінансовими технологіями та соціальними медіа, охоплюють ширший спектр протиправної діяльності, включаючи збір пожертв, переміщення та приховування коштів.

Ця записка має на меті зробити внесок у наявну базу знань щодо рівня реальної загрози, яка виникає внаслідок зловживання новими технологіями, ставлячи питання про те, наскільки нові технології створюють нові або посилюють наявні ризики фінансування тероризму у Європі. Наразі спостерігається певна зацикленість на уявних вразливостях нових технологій, але, на основі зростаючої, хоча й досі обмеженої, бази доказів, ця загроза видається

---

1. Robert Verkaik, 'The Trials of Babar Ahmad: From Jihad in Bosnia to a US Prison via Met Brutality', *The Observer*, 19 March 2016.
2. Michael Jacobson, 'Terrorist Financing and the Internet', *Studies in Conflict and Terrorism* (Vol. 33, No. 4, 2010), pp. 353–63.
3. Tom Keatinge, David Carlisle and Florence Keen, 'Virtual Currencies and Terrorist Financing: Assessing the Risks and EBAluating Responses', May 2018, <https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf>, accessed 24 March 2021; Stephen Reimer and Matthew Redhead, 'Following the Crowd: Clarifying Terrorism Financing Risk in European Crowdfunding', Research Briefing No. 7, Project CRAAFT, 2021.
4. Stephen Reimer and Matthew Redhead, 'A New Normal: Countering the Financing of Self-ActiBAting Terrorism in Europe', *RUSI Occasional Papers* (May 2021), p. 13.

перебільшеною. Хоча нові технології створили нові можливості для фінансування тероризму, вони є радше додатковими інструментами до вже наявного «набору», а не повною його заміною. Це особливо важливо з огляду на те, як часто дискусія про небезпеки нових технологій призводила до рефлексивних заходів протидії фінансуванню тероризму (ПФТ), які не завжди відповідають реальному рівню виявлених ризиків.

Ця записка складається з чотирьох розділів. Розділ I містить оглядову дискусію щодо нових технологій, розглянутих у цьому дослідженні, та вступ до поведінкових моделей і цілей фінансування тероризму. Розділ II аналізує загрози ФТ, що походять від фінансових і нефінансових технологій, тоді як у Розділі III розглянуто реакцію на ці загрози з боку державного та приватного секторів. Розділ IV оцінює поточний стан загрози та заходів реагування, а у завершальній частині наведено низку рекомендацій для Європейської комісії щодо того, як ефективніше відстежувати еволюцію загрози та вдосконалювати заходи реагування на рівні ЄС та держав-членів.

Методологія

Цей проєкт тривав з січня 2021 року до березня 2022 року та розпочався з цільового огляду англомовних джерел, включаючи наукові статті, дослідницькі звіти аналітичних центрів і публікації в медіа, зокрема новинні матеріали та авторські колонки, що відображають поточну політичну дискусію у цій сфері. Терористична діяльність, натхненна ісламістським та ультраправим екстремізмом, розглядалася в міжнародному контексті, з огляду на транснаціональний характер інтернет-технологій і обмежену кількість літератури, присвяченої виключно Європі. Виявлені під час огляду прогалини у дослідженнях лягли в основу формулювання дослідницьких питань та загального дизайну цього дослідження.

Збір даних здійснювався у двох форматах:

- Було проведено **двадцять п’ять експертних консультацій** у дистанційному форматі через обмеження на міжнародні подорожі, запроваджені у зв’язку з коронавірусом. Експерти з державного та приватного секторів — переважно, але не виключно, із Західної Європи — взяли участь у напівструктурованих інтерв’ю щодо їхнього досвіду оцінки масштабів зловживання новими технологіями для фінансування тероризму та заходів реагування на це.
- Було проведено два проекти зі **збору даних з відкритих джерел**, у межах яких зафіксовано деталі загалом 261 унікальної події, пов’язаної з терористичними інцидентами або діяльністю в Європі в період з січня 2015 року до листопада 2021 року.
    - Перший проект був зосереджений виключно на фінансуванні планування нападів (операційне фінансування), включаючи здійснені, зірвані та заплановані атаки.[5] Було зафіксовано 212 нападів або змов, з яких 137 випадків (65%) стосувалися ісламістських екстремістів, далі йшли представники крайнього лівого крила (36 випадків, або 17%), крайнього правого крила (36 випадків, або 17%), екстремісти, підтримувані державами (2 випадки, або <1%), та екстремісти-націоналістичні сепаратисти (1 випадок, або <1%).

5. Події були зафіксовані у 19 країнах: Австрія, Бельгія, Болгарія, Хорватія, Данія, Фінляндія, Франція, Німеччина, Греція, Італія, Латвія, Литва, Нідерланди, Норвегія, Польща, Іспанія, Швеція, Швейцарія та Велика Британія.

- Другий проект був присвячений фінансуванню терористичних організацій (організаційне фінансування) та охоплював виключно випадки, що призвели до дій правоохоронних органів і потенційно також до судових проваджень проти окремих осіб.[6] Було зафіксовано 49 випадків, усі, крім двох, стосувалися ісламістських екстремістів.

Обмеження цього дослідницького підходу включають обмежений доступ до інформації, якою володіє державний сектор щодо реальних випадків використання нових технологій терористами або їхніми прихильниками для фінансування. Автори зіткнулися з низьким рівнем відгуку на запити про інтерв'ю від представників державного сектору, визнаючи, що проведення інтерв'ю в онлайн-форматі могло ускладнити для них повноцінну участь у дослідницькому процесі. Крім того, це могло відображати брак інформації для надання; один із керівників національного підрозділу фінансової розвідки (ПФР) зауважив, що обізнаність із цієї тематики серед європейських правоохоронних органів є низькою.[7]

Завдання зі збору даних з відкритих джерел ускладнювалися тим, що у публічно доступних звітах часто не наводилися фінансові та логістичні деталі подій, пов'язаних із фінансуванням, зазвичай через правові обмеження (наприклад, закони про захист приватності або інтереси збереження таємниці розслідувань) або через сприйняття такої інформації як нецікавої для громадськості. Ці обмеження можуть впливати на географічну репрезентативність, через що дані щодо окремих країн можуть бути як завищеними, так і заниженими. Часові рамки також спричинили викривлення в даних про організаційне фінансування: досліджуваний період (2015–2021 роки) не дав такої кількості випадків, пов'язаних із тероризмом правого спрямування, як очікувалося, можливо, через часовий розрив між самою подією та моментом, коли розслідування призводить до судового розгляду.

Звісно, ці обмеження залишають відкритою можливість того, що поширеність фінансування тероризму через деякі нові технології є вищою, ніж вдалося встановити у межах цього дослідження. Більший обсяг даних неминуче дав би змогу сформувати більш деталізовану картину, хоча малоймовірно, що така інформація призвела б до іншого висновку.

Розкриття понять: нові технології

Термін «нові технології» широко використовується, але має нечітке визначення,[8] і теоретично може стосуватися будь-якого нового інструмента, розробленого в недавньому минулому для будь-яких цілей — від обміну миттєвими повідомленнями до штучного інтелекту. Найбільш дотичним до сфери фінансування тероризму є сектор, відомий як «FinTech», у якому компанії використовують нові технології для надання базових, орієнтованих на роботу з великими обсягами даних, фінансових послуг швидко, безпечно та за низькою вартістю. Відмовляючись від традиційних посередників на користь онлайн-платформ, компанії фінансових технологій отримують доступ до ширшої потенційної аудиторії користувачів,

6. Події були зафіксовані у 12 країнах: Болгарія, Данія, Естонія, Франція, Німеччина, Ірландія, Італія, Нідерланди, Норвегія, Іспанія, Швеція та Велика Британія.
7. Інтерв'ю авторів із керівником підрозділу фінансової розвідки (ПФР) держави — члена ЄС, 26 липня 2021 року.
8. Наприклад, Рекомендація 15 FATF вимагає від країн «виявляти та оцінювати» ризики відмивання коштів і фінансування тероризму, пов'язані з новими технологіями та продуктами. Європейська комісія посилається на цю рекомендацію в проєкті регламенту щодо відстежуваності криптоактивів. Див.: European Commission, Regulation of the European Parliament and of the Council on Information Accompanying Transfers of Funds and Certain Crypto-Assets (Recast), липень 2021 року, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0422&from=EN, дата звернення: 16 березня 2022 року.

яких приваблює зручність здійснення фінансових операцій онлайн і «на ходу» завдяки розвитку мобільних технологій та стільникових мереж.[9] Компанії фінансових технологій розвинулися практично в усіх сегментах фінансової системи, зокрема:

- **Цифровий банкінг:** наразі в Європі діє кілька добре відомих онлайн- або «нео»-банків, таких як розташований у Німеччині N26, які пропонують широкий спектр тих самих послуг, що й традиційні роздрібні банки. В Європі також спостерігається зростання ринку обслуговування бізнесу серед цифрових банків.
- **Платіжні послуги:** компанії на кшталт Stripe (зі штаб-квартирами в Ірландії та США), які забезпечують принаймні одну частину інфраструктури, необхідної для обробки переказів коштів між фізичними особами, підприємствами та/або фінансовими установами — як у межах країни, так і на міжнародному рівні.
- **Кредитування**: надання онлайн-кредитів — як для конкретних покупок, так і у вигляді більш загальних особистих або бізнес-позик. Деякі інші провайдери, такі як розташована у Великій Британії Funding Circle, застосовують підхід «рівний-рівному» (peer-to-peer, P2P) для фінансування своїх кредитів, що дозволяє приватним особам безпосередньо надавати позики малим і середнім підприємствам з метою отримання прибутку.
- **Краудфандинг:** натхненний розвитком мікрофінансових проєктів у країнах, що розвиваються, а також краудсорсингом знань і послуг через інтернет,[10] краудфандинг передбачає використання фізичними особами та групами спеціалізованих онлайн-платформ для просування своїх ініціатив, безпосереднього збору коштів та оперативного їхнього переказу кінцевому одержувачу.[11] Багато таких платформ — часто званих «орієнтованими на віддачу» — допомагають бізнесу залучати капітал від інвесторів в обмін на дохід або частку в компанії. Окрім цього, розвинулися й платформи, засновані на пожертвах, для підтримки благодійних або інших неприбуткових ініціатив,[12] які, однак, можна також розглядати як різновид соціальних медіа, як зазначено нижче.
- **Інвестиції:** інвестиційна індустрія зазнала впливу зростання інтернет-застосунків, які дають змогу інвесторам керувати своїми портфелями безпосередньо або за підтримки автоматизованих «робо-радників», замість користування послугами традиційних брокерів.[13]

---

9. Див.: Henri Arslanian та Fabrice Fischer, The Future of Finance: The Impacts of FinTech, AI, and Crypto on Financial Services (Cham: Palgrave Macmillan, 2019); Niels Pedersen, Financial Technology: Case Studies in Fintech InnoBAtion (London: Kogan Page, 2021); Itay Goldstein, Wei Jiang та G. Andrew Karolyi, 'To FinTech and Beyond', Review of Financial Studies (т. 32, № 5, травень 2019), с. 1647–1661; Anne-Laure Mention, 'The Future of Fintech', Research-Technology Management (т. 62, № 4, 2019), с. 59–63.
10. Francesca Di Pietro, 'Deciphering Crowdfunding', in Theo Lynn et al. (eds), *Disrupting Finance: FinTech and Strategy in the 21st Century* (Cham: Palgrave Macmillan, 2019), p. 2.
11. Асоціація краудфандингу Великої Британії, What is Crowdfunding?, https://www.ukcfa.org.uk/what-is-crowdfunding/, дата звернення: 28 червня 2021 року.
12. Див.: Reimer and Redhead, 'Following the Crowd'.
13. Jake Frankenfield, 'Robo-Advisor', Investopedia, оновлено 21 Лютого 2022, <https://www.investopedia.com/terms/r/roboadvisor-roboadviser.asp>, дата звернення: 4 Березня 2022.

- **Страхування:** подібно до інвестиційної сфери, компанії фінансових технологій (FinTech) вийшли на ринок страхування з наміром використовувати великі дані та машинне навчання для вдосконалення оцінки ризиків і зниження страхових премій.[14]
- **Постачальники послуг, пов'язаних із віртуальними активами (VASPs):** сектор VASP сформувався внаслідок розвитку криптовалют, таких як біткоїн, що ґрунтуються на технології розподіленого реєстру (distributed ledger technology, DLT) або блокчейні.[15] З часу появи біткоїна у 2008 році відбулося зростання так званих «конфіденційних монет» (priBAcy coins), які мають посилені протоколи шифрування, та «стейблкоїнів» (stablecoins), прив'язаних до базового активу. Основна діяльність сектору VASP наразі охоплює зберігання криптовалют (у гаманцях) та їх купівлю-продаж (через біржі). Хоча зростає асортимент товарів і послуг, які можна придбати за допомогою криптовалют, у їхньому повсякденному використанні досі існують суттєві практичні обмеження.[16] Темна мережа (dark net) також залишається альтернативним середовищем для їх застосування, де вони є основною валютою.[17]

Серед цих «підсекторів» FinTech найбільш комерційно помітними в Європі є цифровий банкінг, платіжні послуги та кредитування. Згідно з опитуванням, проведеним у вересні 2020 року серед 50 провідних європейських FinTech-компаній за обсягом ринкової вартості, платіжні послуги очолили список із 14 представників, за ними йшли цифровий або нео-банкінг (11) та кредитування (7). Сектори інвестицій і страхування були представлені п'ятьма та двома компаніями відповідно, тоді як постачальники послуг, пов'язаних із віртуальними активами (VASPs), — яких часто вважають найбільш суперечливим підсектором FinTech, — мали лише трьох представників.[18]

Поза межами FinTech слід також враховувати фінансове значення соціальних медіа через їхню здатність забезпечувати обмін фінансовою інформацією способами, що можуть сприяти фінансуванню тероризму. Згідно зі спільним звітом 2019 року Азійсько-Тихоокеанської групи з питань відмивання грошей (APG) та Близькосхідної й Північноафриканської групи з фінансових заходів (MENAFATF) — двох регіональних органів типу FATF (FSRB), афілійованих із FATF, — соціальні медіа охоплюють чотири підсфери.[19]

---

14. Marshall Hargrave, 'Insurtech', Investopedia, updated 27 August 2020, <https://www.investopedia.com/terms/i/insurtech.asp>, дата звернення: 4 березня 2022 року.
15. Використовуючи розподілений реєстр у комп'ютерних мережах, блокчейн дає змогу зберігати інформацію про події чи діяльність (наприклад, фінансові транзакції) в окремих «блоках», які проходять верифікацію на вузлах мережі. Завдяки хронологічній структурі ланцюга неможливо змінити дані, що вже містяться в ньому, заднім числом.
16. Jacob Bernstein, 'What Can You Actually Buy with Bitcoin?', *New York Times*, 3 лютого 2021.
17. Chainalysis, 'The 2022 Crypto Crime Report', February 2022, p. 11, <https://go.chainalysis.com/rs/503-FAP-074/images/Crypto-Crime-Report-2022.pdf>, дата звернення: 4 березня 2022.
18. The survey was conducted by FinoBAte, a FinTech events management provider. A further eight firms provided a BAriety of different business supports services. See Scott Raspa, 'A Look at the Top 50 Fintech Companies in Europe', 4 September 2020, <https://finoBAte.com/a-look-at-the-top-50-fintech-companies-in-europe/>, дата звернення: 15 грудня 2021.
19. APG, 'APG/MENAFATF Social Media & Terrorism Financing Report', January 2019, p. 6, <http://www.apgml.org/methods-and-trends/news/details.aspx?pcPage=1&n=1142>, дата звернення 15 грудня 2021.

1. **Соціальні мережі:** сайти, такі як Facebook або Twitter, які дають змогу користувачам створювати чи поширювати соціальний контент, а також встановлювати зв'язок та взаємодіяти з іншими користувачами.
2. **Сервіси розміщення контенту:** сайти, які дають змогу користувачам створювати, завантажувати та переглядати контент, такі як YouTube або Vimeo.
3. **Краудфандингові сервіси:** сайти, які — на відміну від орієнтованих на віддачу платформ, згаданих вище — дають змогу користувачам фінансувати проєкт або ініціативу шляхом збору невеликих сум коштів від великої кількості людей (crowdsourcing).[20] Прикладами є GoFundMe та JustGiving.
4. **Сервіси інтернет-комунікацій:** також відомі як платформи миттєвого обміну повідомленнями, які дають змогу користувачам спілкуватися в режимі реального часу через інтернет, такі як WhatsApp або Signal. Все частіше такі сервіси використовують наскрізне шифрування для запобігання стеженню за розмовами. Деякі вже почали інтегровувати інтернет- або мобільні платіжні сервіси, наприклад WeChat Pay.[21]

20. Асоціація краудфандингу Великої Британії, What is Crowdfunding?.
21. WeChat Pay майже виключно використовується в Китаї, хоча платформи інтернет-комунікацій, що належать компанії Meta (материнській компанії Facebook, Instagram та WhatsApp), наразі пропонують платіжні послуги в деяких країнах, зокрема у Бразилії, Таїланді та США. Див.: Facebook Pay, Current ABAilability, https://pay.facebook.com/gb/aBAilability/, дата звернення: 16 грудня 2021 року.

I. Фінансування тероризму: цілі та види діяльності

Як і у випадку з «новими технологіями», концептуалізація фінансування тероризму та його реальні прояви також залишаються доволі нечіткими. Резолюція Ради Безпеки ООН 2462 (2019) щодо протидії фінансуванню тероризму визначає під ФТ залучення, переміщення, переказ та отримання коштів для терористів і терористами як практичне розуміння цього явища. Натомість FATF у своєму визначенні зосереджується на запланованому використанні коштів — «фінансуванні терористичних актів, а також терористів і терористичних організацій».[22]

Останні наукові публікації допомогли частково вирішити цю проблему, поєднавши як діяльність, яку здійснюють особи що фінансують тероризм, так і цілі, заради яких вона здійснюється, щоб надати більш комплексне уявлення про ФТ. Мартін Навіас виокремив три категорії дій (створення, переміщення та використання коштів)[23] — підхід, який нещодавно був уточнений Джесікою Девіс, що запропонувала консолідований перелік із шести ключових видів діяльності:

- Залучення коштів.
- Використання коштів.
- Зберігання коштів.
- Переміщення коштів.
- Управління коштами.
- Приховування коштів[24]

Цей більш всеохоплюючий підхід свідчить, що фінансування тероризму стосується не лише коротко- та середньострокових дій — залучення, використання та переміщення коштів, — але й довгострокових аспектів, пов'язаних з управлінням фінансовими ресурсами.

Крім того, дослідники також наголошують на відмінностях між цілями операційного та організаційного фінансування.[25] У першому випадку операційне фінансування забезпечує проведення реальних або потенційних нападів, покриваючи підготовчі заходи, такі як дослідження, розвідка та закупівля зброї чи інших матеріалів, а також безпосереднє здійснення нападу.

---

22. UNSCR 2462 (2019); FATF, 'International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations', оновлено у березні 2022 року.
23. Martin S Navias, *Finance & Security: Global Vulnerabilities, Threats and Responses* (London: C Hurst & Co., 2019), p. 49.
24. Jessica Davis, *Illicit Money: Financing Terrorism in the 21st Century* (London: Lynne Rienner, 2021), p. 5.
25. *Ibid.*, pp. 3, 5. Colin P Clarke, *Terrorism, Inc.: The Financing of Terrorism, Insurgency, and Irregular Warfare* (Santa Barbara, CA: ABC-CLIO, 2015), p. 4; Nick Ridley, *Terrorist Financing: The Failure of Counter Measures* (Cheltenham: Edward Elgar, 2012).

Організаційне фінансування, навпаки, зазвичай має ширший спектр цілей, охоплюючи витрати на утримання терористичної групи або мережі, вербування та підготовку кадрів, забезпечення добробуту бойовиків і, іноді, їхніх утриманців, створення та поширення пропаганди, а також — у деяких випадках — надання оперативної підтримки ширшим мережам пов'язаних або ідейно близьких учасників.

Поділ на операційне та організаційне фінансування є важливим для розуміння характеру фінансування тероризму, оскільки мета використання коштів не лише визначає види фінансової діяльності, що здійснюються, але й на більш детальному рівні впливає на вибір фінансових інструментів, які можуть бути задіяні. Наприклад, фінансування індивідуальних атак, як правило, потребує менших витрат, що зменшує необхідність у залученні, переміщенні чи використанні значних сум. Це особливо актуально нині в Європі, з огляду на поширеність «самостійного» тероризму, який Europol визначає як основну терористичну загрозу для континенту[26] і який становив 74% вибірки нападів та змов, розглянутих у цьому дослідженні.

Дослідження свідчать, що такі нападники зазвичай здійснюють менш витратні атаки, використовуючи на вигляд легальні й буденні джерела фінансування, як-от заробітну плату чи зловживання державними соціальними виплатами, або ж вдаючись до дрібної злочинності, наприклад, торгівлі наркотиками.[27]

Натомість організаційне фінансування, як правило, вимагає масштабного залучення коштів, значна частина яких має бути переведена через кордони та управлятися протягом тривалого часу, що надає особливої ваги переміщенню, управлінню, зберіганню та приховуванню коштів. Наприклад, фінансові операції «Хезболли» в Європі включали використання підставних компаній і злочинної діяльності для залучення, переміщення та приховування коштів.[28] «Хамас»[29], «Аш-Шабаб»[30] та інші ісламістські екстремістські угруповання збирали пожертви від прихильників, що проживають у Європі, які потім переводилися за її межі через готівкових кур'єрів, підставні компанії, банківські перекази, сервіси переказу грошей і вартості, такі як MoneyGram та Western Union, а також через традиційну систему переказу вартості — хавалу.[31]

Ультраправі угруповання, розташовані в Європі, діяли подібним чином, зокрема групи у Фінляндії та Швеції, які залучали кошти через членські внески та пожертви від своїх прихильників.[32]

Опосередковані канали організаційного фінансування стають дедалі більшою проблемою у сфері ФТ для Європи, коли кошти переказуються до зон конфліктів, але не призначені для безпосередньої фінансової підтримки операцій

26. Europol, European Union Terrorism Situation and Trend (Люксембург: Publications Office of the EU, 2021), також відомий як «TE-SAT 2021».
27. Reimer and Redhead, 'A New Normal'.
28. Matthew Levitt, 'The Lebanese Hizbullah Financing Threat in Europe', Research Briefing No. 1, Project CRAAFT, 2020.
29. US Department of Justice, 'Global Disruption of Three Terror Finance Cyber-Enabled Campaigns: Largest Ever Seizure of Terrorist Organizations' Cryptocurrency Accounts', press release, 13 August 2020, <https://www.justice.gov/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns>, accessed 9 January 2022.
30. Див.: Magnus Normark and Magnus Ranstorp, 'Understanding Terrorist Finance: Modus Operandi and National CTF-Regimes', Swedish Defence University, 18 December 2015.
31. Europol, 'TE-SAT 2021', с. 33.
32. *Ibid*., с. 31.

терористичного угруповання. Під час піку територіального контролю «Ісламської держави» в Іраку та Сирії присутність у зоні конфлікту іноземних бойовиків з Європи спонукала їхніх друзів і членів сімей переказувати кошти через неформальні канали для забезпечення добробуту своїх близьких. Відправники таких переказів дуже рідко поділяли ідеологічні погляди одержувачів, проте, надаючи кошти терористу, вони все ж ставали причетними до фінансування тероризму, що призвело до кількох обвинувальних вироків у Європі.

Наприклад, у 2019 році британське подружжя було визнане винним у фінансуванні тероризму за переказ £233 через ліванського посередника своєму синові в Сирії, який підтримував «Ісламську державу».[33]

Останнім часом подібні перекази здійснювалися зі Швейцарії, Швеції, Іспанії, Нідерландів та інших частин Європи з метою фінансування поїздок іноземних бойовиків назад до Європи або підтримки осіб, утримуваних у таборах для пов'язаних з «Ісламською державою» осіб, зокрема для оплати послуг контрабандистів людей та посередників з метою вивезення жінок і дітей, пов'язаних з «Ісламською державою», з таких місць утримання.[34]

Такі операції з вивезення стають можливими завдяки складним мережам, до яких входять терористичні угруповання, афілійовані з «Ісламською державою» та «Аль-Каїдою», зокрема Хайят Тахрір аш-Шам, що отримують прибуток від незаконної економічної діяльності у сфері контрабанди людей.[35]

Підсумовуючи, як базовий орієнтир для оцінки ступеня зміни ризиків, пов'язаних із новими технологіями, операційне фінансування тероризму в Європі переважно здійснюється шляхом самофінансування незначних сум через дрібну злочинність та «буденні» джерела. Натомість організаційне фінансування є більш складним і залежить від залучення коштів та їхнього переказу (зазвичай за межі Європи).

Потенційний вплив нових технологій на фінансування тероризму

З'явившись у цьому середовищі, нові технології отримали потенціал змінити усталені практики фінансування тероризму подібно до того, як вони трансформували легальну фінансову діяльність. У науковій літературі, а також під час напівструктурованих інтерв'ю, ця ідея про здатність нових технологій трансформувати ФТ висловлювалася у трьох основних формах:

- **Нові канали:** поява нового спектра постачальників фінансових послуг може надати особам що фінансують тероризм нові шляхи для здійснення ФТ. Наприклад, розвиток офіційних краудфандингових платформ та неформального краудфандингу, заснованого на соціальних медіа, має потенціал створити нові способи переміщення та залучення коштів.[36]

33. Crown Prosecution Service, 'Sally Lane and John Letts Sentenced for Sending Money to Daesh Supporting Son', <https://www.cps.gov.uk/cps/news/sally-lane-and-john-letts-sentenced-sending-money-daesh-supporting-son>, дата звернення: 9 грудня 2021 року.
34. Europol, 'TE-SAT 2021', p. 32.
35. Audrey Alexander, 'Cash Camps: Financing Detainee Activities in Al-Hol and Roj Camps', Combating Terrorism Center at Westpoint, вересень 2021 року, с. 23–27.
36. See Reimer and Redhead, 'Following the Crowd'; Jacobson, 'Terrorist Financing and the Internet'; Martin Rudner, '"Electronic *Jihad*": The Internet as Al Qaeda's Catalyst for Global Terror', *Studies in Conflict and Terrorism* (Vol. 40, No. 1, 2017), с. 10–23; інтерв'ю авторів із посадовцем банківського сектору ЄС, 27 серпня 2021 року.

- **Підтримка «техніки» ФТ:** наприклад, віртуальні активи (ВА) часто вважаються ідеальним інструментом для протиправної діяльності завдяки своїй безкордонній та P2P-природі, швидкості, низьким транзакційним витратам і передбачуваній анонімності, що потенційно може сприяти підготовці атак або організаційному фінансуванню.[37]
- **Зменшений рівень нагляду:** з огляду на відносну незрілість багатьох FinTech-компаній у розбудові систем протидії фінансовим злочинам та у розумінні ризиків ФТ, з якими вони стикаються, існує ймовірність, що такі платформи можуть створювати середовище для діяльності осіб що фінансують тероризм за умов слабшого контролю у сфері протидії фінансовим злочинам, ніж у традиційному фінансовому секторі, який має значно більший досвід дотримання вимог AML/CTF.[38]

Існує значний рівень невизначеності та занепокоєння щодо того, наскільки ці теоретичні ризики вже реалізувалися або можуть реалізуватися на практиці. В інтерв'ю для цього проєкту один із керівників національного правоохоронного органу зазначив, що серед колег у різних країнах Європи спостерігається обмежене розуміння реальної природи цих ризиків, а також наявне глибинне побоювання, що вони можуть виявитися неготовими до використання нових технологій у якийсь непередбачуваний спосіб.[39]

На цьому етапі ця записка переходить до аналізу поточного стану доказової бази щодо зловживання новими технологіями особами що фінансують тероризм в Європі.

37. Zachary K Goldman et al., 'Terrorist Use of Virtual Currencies: Containing the Potential Threat', Center for a New American Security, травень 2017 року; Nikita Malik, *Terror in the Dark: How Terrorists Use Encryption, the Darknet, and Cryptocurrencies* (London: Henry Jackson Society, 2018); Iwa Salami, 'Terrorism Financing with Virtual Currencies: Can Regulatory Technology Solutions Combat This?', *Studies in Conflict and Terrorism* (Vol. 41, No. 12, 2017), pp. 968–89; Nicholas Ryder, 'Cryptoassets, Social Media Platforms and Defence Against Terrorism Financing Suspicious Activity Reports: A Step into the Regulatory Unknown', *Journal of Business Law* (Vol. 8, 2020), т. 8, 2020), с. 668–693. Для критичного аналізу див.: Malcolm Campbell-Verduyn, 'Bitcoin, Crypto-Coins, and Global Anti-Money Laundering Governance', *Crime, Law and Social Change* (Vol. 69, No. 1, 2018); Keatinge, Carlisle and Keen, 'Virtual Currencies and Terrorist Financing'.
38. Інтерв'ю авторів із старшим консультантом з питань фінансових злочинів у FinTech, 7 травня 2021 року; інтерв'ю авторів з уповноваженим з питань повідомлення про відмивання коштів (MLRO) європейського постачальника платіжних послуг/FinTech, 28 липня 2021 року; інтерв'ю авторів з аналітиком європейського підрозділу фінансової розвідки (ПФР), 13 серпня 2021 року; інтерв'ю авторів із посадовцем банківського сектору ЄС, 27 серпня 2021 року; Michael Carter, Microlending and Crowdfunding: A Growing Terrorist Financing Risk, KYC360, 28 липня 2017 року, https://www.riskscreen.com/kyc360/article/microlending-and-crowdfunding-aml-risk/ , дата звернення: 22 березня 2021 року.
39. Інтерв'ю авторів із керівником підрозділу фінансової розвідки (ПФР) держави — члена ЄС, 26 липня 2021 року.

II. Нові технології та ризики фінансування тероризму

Дискусія щодо ризиків фінансування тероризму, пов'язаних із новими технологіями, має тенденцію поляризуватися навколо двох позицій: перша — поширена серед представників державного сектору[40] — розглядає передбачувані вразливості нових технологій як беззаперечну та нагальну загрозу; друга — більш властива тим, хто працює з новими технологіями, або науковцям і дослідникам, що мають змогу займати більш довгострокову перспективу[41], — вважає, що ці ризики не обов'язково є більшими, ніж ті, що походять від уже наявної фінансової системи.

Відсутність консенсусу частково зумовлена ролями та інтересами учасників обговорення, а також рівнем їхньої фактичної обізнаності з реальними випадками ФТ або з новими технологіями. Однак це також відображає нестачу узгодженої доказової бази, що робить можливим ширший спектр відмінних оцінок.

На базовому рівні очевидно, що деякі нові технології використовуються як для операційних, так і для організаційних цілей фінансування тероризму терористами з різними ідеологіями. В операційному аспекті в низці випадків фігурували постачальники платіжних послуг і соціальні медіа, тоді як для організаційного фінансування у дослідженнях та медіа особливо відзначаються соціальні медіа, краудфандингові платформи та віртуальні активи (ВА) як інструменти залучення та переміщення коштів.

Втім, існує дуже мало доказів того, що нові технології мали трансформаційний вплив на ФТ у Європі станом на сьогодні. З кількісної точки зору схеми ФТ досі переважно ґрунтуються на перевірених методах, а у випадках, коли нові технології все ж з'являються, вони, як правило, застосовуються у поєднанні з традиційними підходами.

Однак ці висновки слід супроводити застереженням щодо рівня впевненості в наявній доказовій базі. Із проведених інтерв'ю з практиками — як у державному, так і в приватному секторі — стало очевидно, що багато хто вважає свої знання недостатніми, аби з упевненістю описати масштаби та характер зловживань.[42] Це застереження вказує на необхідність вдосконалення доказової бази щодо всіх типів ФТ шляхом кращої класифікації та систематичної звітності за типологіями ФТ. Детальніше це питання розглянуто в Розділі III.

Операційне фінансування

Використання нових технологій для операційного фінансування привернуло значну увагу у грудні 2015 року, коли Сайєд Різван Фарук отримав позику у розмірі 28 500 доларів США від P2P-кредитної компанії Prosper Marketplace, лише за два тижні до того, як він разом із дружиною

40. Інтерв'ю авторів із керівником підрозділу фінансової розвідки (ПФР) держави — члена ЄС, 26 липня 2021 року; інтерв'ю авторів із посадовцем банківського сектору ЄС, 27 серпня 2021 року.
41. Інтерв'ю авторів з уповноваженим з питань повідомлення про відмивання коштів (MLRO) європейського постачальника платіжних послуг/FinTech, 28 липня 2021 року.
42. Інтерв'ю авторів із керівником підрозділу фінансової розвідки (ПФР) держави — члена ЄС, 26 липня 2021 року; інтерв'ю авторів із посадовцями на рівні ЄС, 7 червня 2021 року; інтерв'ю авторів із старшим співробітником служби комплаєнсу великого постачальника платіжних послуг, 27 липня 2021 року; інтерв'ю авторів із керівником напряму комплаєнсу з питань фінансових злочинів великого постачальника платіжних послуг, 24 липня 2021 року.

Ташфін Малік здійснили політично мотивовану стрілянину на різдвяній вечірці в Сан-Бернардіно, штат Каліфорнія. Американська влада тоді зазначила, що ця позика могла бути використана для придбання набоїв, компонентів для кількох саморобних вибухових пристроїв та для тренувальної стрільби на стрілецькому полігоні.[43]

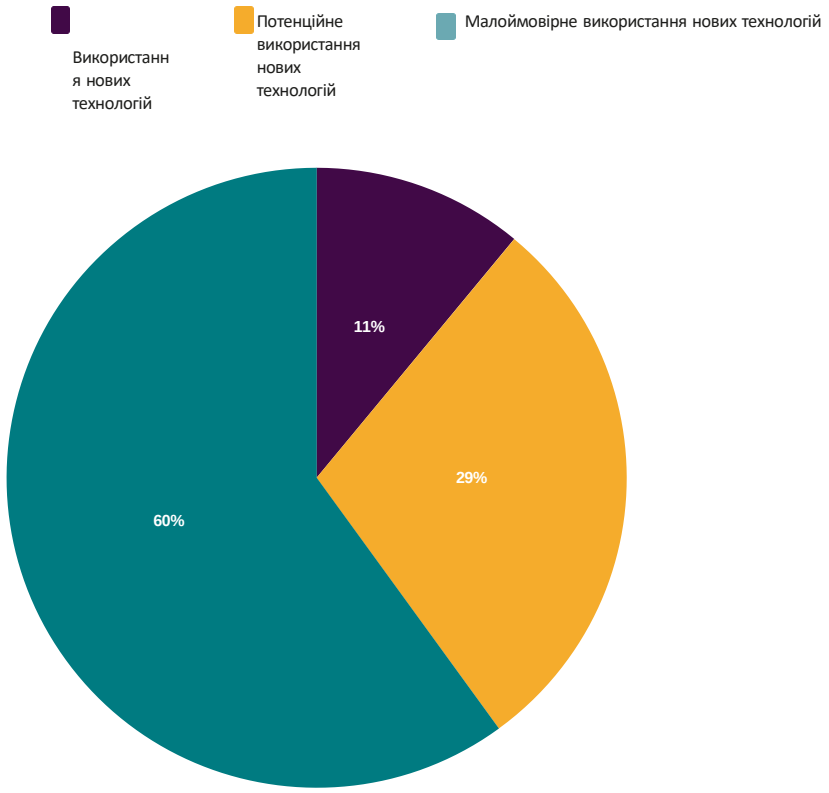
Приклад Сан-Бернардіно демонструє потенціал нових технологій у процесі залучення коштів для підготовки нападів. Водночас він залишається рідкісним випадком у США і, на підставі результатів збору даних з відкритих джерел у межах цього дослідження, не відображає й поточної ситуації в Європі.

У межах дослідження було проаналізовано 212 операційних випадків, що мали місце в Європі з січня 2015 року. Корисну інформацію щодо фінансових і логістичних аспектів планування атак вдалося отримати у 65 випадках (31%). Хоча дані про фінансування та управління цими змовами часто було складно визначити повною мірою, стало очевидно, що в більшості випадків нові технології не відігравали помітної ролі в операційному фінансуванні тероризму:

- У 60% випадків з високою ймовірністю нові технології не використовувалися з низки причин: у звітах зазначалося, що предмети, пов'язані з нападом, належали нападнику ще раніше або були придбані за готівку чи за допомогою звичайних банківських платіжних методів.
- У 29% випадків у звітах зазначалося, що певні фінансові технології потенційно могли бути використані для придбання предметів онлайн або в магазині, але не було зрозуміло, чи йшлося про традиційні банківські продукти, чи про сервіси, надані «челенджер-банком» або постачальником платіжних послуг.

43. James Rufus Koren та Jim Puzzanghera, Loan to San Bernardino Shooter Draws Scrutiny to Online Lending Industry, Los Angeles Times, 11 грудня 2015 року; BBC News, San Bernardino Shooting: What We Know So Far, 11 грудня 2015 року.

Рисунок 1: Використання нових технологій у плануванні нападів у Європі, 2015–2021 роки



Джерело: на основі 65 випадків з дослідження авторів.

З огляду на відносно невелику кількість випадків із чіткими доказами залучення нових технологій, у цій записці детальніше розглянуто кілька прикладів.

Приклад 1: Покупки у «темній мережі» за криптовалюту

У двох випадках використання нових технологій для придбання компонентів для нападів європейські самостійно діючі терористи купували зброю в «темній мережі» (dark net), використовуючи криптовалюту. Алі Давід Зонболі, терорист ультраправого спрямування з Німеччини, натхненний норвезьким терористом Андерсом Брейвіком, у 2016 році застрелив дев'ять осіб у Мюнхені. Після нападу 32-річного німця заарештували за спробу продати автоматичну зброю та пістолет агентам під прикриттям, з якими він познайомився в «темній мережі». Пізніше він зізнався, що також продав Зонболі пістолет Glock 17 і 350 набоїв під час двох зустрічей у місті Марбург. Матеріали коштували Зонболі 4 350 євро, які він сплатив у біткоїнах.

Невдала спроба Стівена Бішопа, спрямована на підрив мечеті на півдні Лондона, так само виявила спроби придбати у «темній мережі» компоненти для зброї, зокрема детонатор. Хоча у звітах не зазначено, чи було цей предмет придбано за фіатну валюту чи за віртуальні активи, цілком імовірно, що за останні, зважаючи на те, що вони є основною валютою для продажу незаконних товарів на маркетплейсах «темної мережі».

Ще в одному випадку відомо, що Стефан Баллієт, нападник на синагогу в Галле у жовтні 2019 року, отримав пожертву в біткоїнах від невстановленої особи перед здійсненням нападу, хоча зброю, яку він використав, він виготовив на 3D-принтері.

Джерела: Daniel Koehler, The Halle, Germany, Synagogue Attack and the Evolution of the Far-Right Terror Threat, CTC Sentinel (т. 12, № 11, грудень 2019); Ruth Bender та Christopher Alessi, Munich Shooter Likely Bought ReactiBAted Pistol on Dark Net, Wall Street Journal, оновлено 24 липня 2016 року; Reuters, German Admits Selling Gun to Munich Attack Shooter, 28 серпня 2017 року; Kim Sengupta, The Dark Web is a Dangerous New Frontier for Those Who Try to Keep Terrorists at Bay, The Independent, 26 серпня 2016 року; Lizzie Dearden, Man Planned to Bomb London Mosque in "Revenge" for Manchester Arena Attack, The Independent, 9 квітня 2019 року; Wimbledon Times, Man Arrested at His Mother's Morden Home Plotted to Blow Up Mosque in a Suicide Mission, a Court Heard, 6 листопада 2018 року; Sven Röbel, Halle-Attentäter wurde von Unbekanntem finanziell unterstützt [«Нападника в Галле фінансово підтримала невідома особа»], Spiegel Panorama, 11 жовтня 2019 року.

Приклад 2: Сервіси онлайн-платежів

Три випадки демонструють використання FinTech-компаній, що надають платіжні послуги, для придбання компонентів для нападів.

Два випадки у Великій Британії стосувалися використання облікових записів PayPal для здійснення покупок: Мохаммед Рехман, який планував атакувати Лондонське метро або торговий центр Westfield у 10-ту річницю терактів 7/7, придбав прекурсори хімічних речовин та інші матеріали на eBay; підліток Хайдер Ахмед планував напад із використанням мисливського ножа, який він купив через PayPal за £25, але його план було зірвано після того, як мати знайшла та конфіскувала зброю.

У 2019 році вибух СВП (саморобного вибухового пристрою) у Ліоні, Франція, був профінансований за рахунок доходу, який нападник отримав від надання приватних онлайн-уроків через платформу Udemy. Дохід з платформи надходив на рахунок нападника в Payoneer — постачальника фінансових послуг, що спеціалізується на забезпеченні платежів для продавців товарів і послуг на онлайн-маркетплейсах. Компоненти СВП, придбані на Amazon, були оплачені платіжною карткою, прив'язаною до рахунку Payoneer. Цей випадок демонструє високий рівень обізнаності нападника у використанні нових технологій як для залучення, так і для витрачання коштів з метою підготовки до терористичної діяльності. Додатково встановлено, що нападник мав три рахунки у платіжній системі PayPal та зберігав криптовалютні активи на рахунку у криптовалютній біржі Coinmama.

Джерела: BBC News, '"Silent Bomber" Couple Found Guilty of London Terror Attack Plan', 29.12.2015; Peter Stubley, 'Wife of Suspected ISIS Terrorist "Used Payday Loans to Fund His Bomb-Making Purchases on eBay"', The Mirror, 02.12.2015; BBC News, 'Redhill Man Haider Ahmed Jailed Over Knife Terror Plot', 28.06.2019; France 24, 'Lyon Blast Suspect Appears Before Anti-Terror Judge', 31.05.2019; відеоінтерв'ю авторів із представниками компетентних органів Франції, липень 2020 року.

Як показано у прикладах, немає підстав вважати, що нові технології відігравали провідну роль у фінансуванні більшості терористичних атак у Європі останніх років. Зокрема, віртуальні активи (ВА) не стали поширеним інструментом для придбання зброї. Попри занепокоєння щодо рівня анонімності, який вони можуть забезпечувати під час покупок у даркнеті, ВА — принаймні у випадку з найбільш розповсюдженими криптовалютами — водночас формують публічний реєстр транзакцій, що, ймовірно, стримує їхнє більш масове використання. Більше того, технологічні навички, необхідні для орієнтування у даркнеті та успішного здійснення покупок з використанням ВА, у більшості випадків перевищують можливості переважної частини терористів, які самостійно планують атаки. Використання платіжних платформ для придбання товарів таки фіксується, однак слід зазначити, що зловмисники зверталися не стільки до новітніх ринкових рішень, скільки до більш усталених сервісів — насамперед PayPal.

Також майже немає ознак, що терористи масово переходили на цифровий банкінг або намагалися фінансувати атаки за рахунок кредитування чи краудфандингових платформ, за аналогією з випадком у Сан-Бернардіно. Водночас, з огляду на значну кількість випадків, які складно класифікувати через брак інформації, такі висновки слід робити з певною обережністю.

44. Інтерв'ю авторів із Кейлою Айзенман, дослідницею з питань лістингу активів у Coinbase та асоційованою науковою співробітницею RUSI, 14 травня 2021 року.

Організаційне фінансування

В академічному середовищі та засобах масової інформації значно активніше обговорюється роль, яку нові технології можуть відігравати у фінансуванні терористичних організацій. У цьому контексті ключовими є віртуальні активи (ВА), краудфандинг на основі пожертв, соціальні мережі та постачальники платіжних послуг. Найбільш поширеними типологіями, що досліджуються, є роль нових платформ у залученні та переміщенні коштів[45].

Існує значна кількість доказів того, що терористичні угруповання різних ідеологічних напрямів активно просувають використання віртуальних активів (ВА). Так, у 2014 році «Ісламська держава» почала закликати своїх прихильників використовувати Bitcoin, хоча є дані, що останнім часом вона перейшла до заохочення використання «конфіденційних» (приватних) монет, таких як Monero[46]. Інші ісламістські екстремістські угруповання також просували використання ВА для збору коштів — зокрема, Mujahideen Shura Council у 2016 році та Хамас у березні 2019 року[47]. Деякі ультраправі угруповання у США та Європі пішли аналогічним шляхом: наприклад, скандинавські організації Nordic Resistance Movement та Nordic Strength збирали онлайн-пожертви у ВА[48].

Водночас, як і у випадку з операційним фінансуванням, варто проявляти обережність, щоб уникнути надто гучних та передчасних висновків. Щодо найбільш обговорюваної технології — віртуальних активів (ВА) — залишається незрозумілим, який саме реальний вплив вони мали. Зокрема, повідомлялося, що операція уряду США у серпні 2020 року призвела до вилучення активів у ВА на мільйони доларів, які належали ісламістським екстремістським угрупованням[49], однак в інших випадках відсутні ознаки того, що такі групи отримали значну вигоду від збору коштів у ВА.

Наприклад, згадана вище кампанія Mujahideen Shura Council змогла зібрати еквівалент лише 500 доларів США[50]. Останні дослідження компаній, що спеціалізуються на аналітиці блокчейнів, таких як Chainalysis, також показують, що попри використання терористичними угрупованнями криптовалют, їм не вдається повністю убезпечити активи від правоохоронних органів, які дедалі ефективніше відстежують та вилучають кошти[51].

---

45. Див. Reimer та Redhead, «Following the Crowd».
46. Stan Higgins, 'ISIS-Linked Blog: Bitcoin Can Fund Terrorist Movements Worldwide', CoinDesk, updated 11 September 2021, <https://www.coindesk.com/markets/2014/07/07/isis-linked-blog-bitcoin-can-fund-terrorist-movements-worldwide/>, accessed 9 January 2022; Andrey Shevchenko, 'ISIS-Affiliated News Website to Collect Donations with Monero', CoinTelegraph, 25 June 2020, <https://cointelegraph.com/news/isis-affiliated-news-website-to-collect-donations-with-monero>, accessed 9 January 2022.
47. Antonia Ward, 'Bitcoin and the Dark Web: The New Terrorist Threat?', RAND, 22 January 2018, <https://www.rand.org/blog/2018/01/bitcoin-and-the-dark-web-the-new-terrorist-threat. html>, accessed 9 January 2022; Tom Wilson and Dan Williams, 'Hamas Shifts Tactics in Bitcoin Fundraising, Highlighting Crypto Risks: Research', *Reuters*, 26 April 2019.
48. Europol, 'TE-SAT 2021', p. 31.
49. US Department of Justice, 'Global Disruption of Three Terror Finance Cyber-Enabled Campaigns'.
50. Ted Knutson, 'Terrorists Trying Multiple Times to Raise Funds Via Crypto – Without Much Success, Congress Told', *Forbes*, 7 September 2018.
51. Chainalysis, 'The 2022 Crypto Crime Report', p. 93.

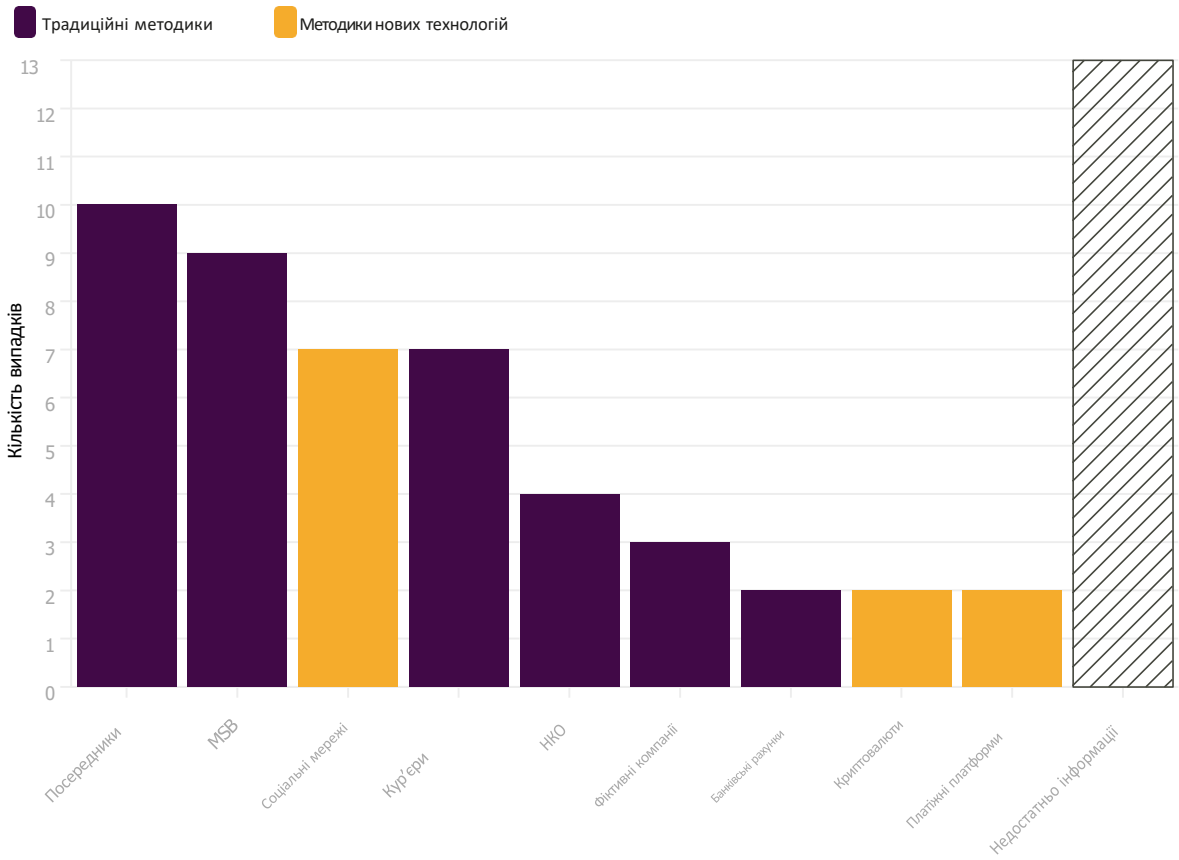
Окрім віртуальних активів (ВА), двоє опитаних експертів, обізнаних із низкою європейських справ щодо фінансування тероризму, відзначили, що інші нові технології — зокрема постачальники платіжних послуг — почали з'являтися у схемах фінансування організацій дедалі частіше. Водночас вони оцінили, що роль платіжних платформ усе ще є відносно обмеженою порівняно з використанням традиційної фінансової системи або альтернативних систем переказу вартості, таких як ісламські банківські інструменти, зокрема хавала. Як і у випадках операційного фінансування, більш імовірною була поява на ринку вже усталених платіжних платформ, наприклад PayPal [52].

Такий багатогранний погляд значною мірою підтвердився і під час кількісного аналізу справ щодо фінансування терористичних організацій, проведеного в межах цього дослідження. Було виявлено 49 справ[53], переважно пов'язаних із ісламістськими екстремістами, які намагалися перевести кошти з європейських країн до держав Близького Сходу та Північної Африки, часто для підтримки іноземних бойовиків або членів їхніх сімей. Із цих 49 справ у 36 було наявно достатньо матеріалів для формування висновків щодо використаних методів ФТ; загалом було ідентифіковано 52 методології, причому в окремих випадках поєднувалося декілька методів.

52. Інтерв'ю авторів із посадовцями інституцій ЄС, 7 червня 2021 року.

53. Як і у вибірці з 212 виявлених випадків операційного фінансування, вибірка з 49 випадків фінансування діяльності організацій майже напевно є неповною. Неможливо визначити, скільки випадків операційного фінансування відбулося у досліджуваний період, але не було зафіксовано у звітах. Як зазначено у розділі «Методологія», можна очікувати, що проміжок часу між випадком фінансування діяльності ультраправих організацій та розслідуванням, яке призводить до судових дій (і, відповідно, до висвітлення у ЗМІ чи в інших публічних джерелах, використаних у цьому дослідженні), може бути однією з причин такого неповного охоплення.

Рисунок 2: Методики фінансування діяльності терористичних організацій, виявлені у 49 європейських справах



Умовні позначення: фіолетовий — «традиційні методикиї»; жовтий — «методики, що використовують нові технології».

Джерело: створено авторами.

Очевидно, що «традиційні» способи фінансування діяльності організацій значно переважали ті, що передбачають використання нових технологій. Трійку найпоширеніших методик склали: використання «посередників» для сприяння або безпосереднього здійснення переказу коштів (10 випадків, 20%), компанії, що надають послуги з грошових переказів (money service businesses, MSB) (дев'ять випадків, 18%) та хавала (сім випадків, 14%). Значну роль також відігравали перевізники готівки (шість випадків, 12%), які іноді, судячи з описів справ, фактично збігалися з категорією «посередників».

FinTech траплявся значно рідше: випадки з використанням онлайн-платіжних сервісів та криптовалют становили найменшу частку ідентифікованих методик, хоча приклади застосування ВА були відносно недавніми (див. Приклад 3).

Приклад 3: Криптовалюта та фінансування діяльності організацій

У вересні 2020 року французькі правоохоронні органи заарештували 29 осіб за фінансування джихадистських угруповань у Сирії за допомогою купонів на криптовалюту номіналом від 10 до 150 євро, придбаних у ліцензованих кіосках по всій Франції. Оплачені готівкою або банківською карткою без необхідності пред'явлення документа, що посвідчує особу, реквізити купонів передавалися контактам у Сирії через зашифровані месенджери. Одержувачі могли використати їх для зарахування коштів на власні біткойн-гаманці. Після цього інциденту Франція оголосила про запровадження нових правил ідентифікації клієнтів (know-your-customer, KYC), які поширюються на всіх постачальників послуг, пов'язаних із криптовалютами.

У Великій Британії Гішам Чаудгарі (засуджений у вересні 2021 року) у 2018 році отримав десятки тисяч фунтів стерлінгів від контактів, пов'язаних з «Ісламською державою», і мав завдання конвертувати ці кошти у криптовалюту (Bitcoin), а потім передати їх для використання угрупованням. Повідомлялося, що у 2018 році Чаудгарі придбав біткойнів на суму 17 000 фунтів, з яких 16 000 було переведено невстановленим отримувачам. У 2019 році він придбав і передав приблизно 35 000 фунтів у біткойнах. За повідомленнями, кошти призначалися для організації звільнення прихильників «Ісламської держави» з таборів утримання та їх транспортування до районів, підконтрольних угрупованню.

Джерела: France 24, «France Arrests 29 in Anti-Terror Syria Financing Sting», 29.09.2020; Gabriel Vedrenne, «Cryptocurrency "Coupons" Funded Syrian Jihadism, French Authorities Claim», Moneylaundering.com, 02.10.2020, https://www.moneylaundering.com/news/cryptocurrency-coupons-funded-syrian-jihadism-french-authorities-claim/, дата звернення: 18.12.2021; Vish Gain, «France Announces Strict Cryptocurrency KYC Rules to Fight Money Laundering and Terrorist Financing», AML Intelligence, 11.12.2020, https://www.amlintelligence.com/2020/12/france-announces-strict-cryptocurrency-kyc-rules-to-fight-money-laundering-and-terrorist-financing/, дата звернення: 18.12.2021; BBC News, «Hisham Chaudhary: Oadby Terrorist Who Funded IS with Bitcoin Jailed», 03.09.2021.

Водночас, попри відносно незначну роль FinTech у вузькому розумінні, варто зазначити, що використання соціальних мереж траплялося значно частіше — у семи випадках, коли екстремісти поширювали інформацію, яка дозволяла залучати або переміщувати кошти, — методика, що вже добре задокументована за межами Європи[54].

З метою маскування своєї діяльності особи що фінансують тероризм часто заявляють, що збирають кошти на законні благодійні або гуманітарні цілі, коли звертаються по пожертви через соціальні мережі[55]. Такий підхід було зафіксовано, зокрема, в Іспанії у 2021 році, коли троє осіб спрямували кошти, зібрані для неприбуткової організації, на фінансування діяльності «Аль-Каїди»[56]. У таких випадках отримані пожертви зазвичай надходять через традиційні платіжні методи, такі як банківські перекази[57], хоча трапляються приклади використання передплачених карток та криптовалют[58].

Ці випадки демонструють важливу роль, яку інтернет-технології можуть відігравати у процесах залучення та управління коштами в межах фінансування терористичних організацій[59], а також їхню здатність легко поєднуватися з іншими підходами. Так, один неназваний підсудний у Швеції, якого судили за терористичними звинуваченнями у лютому 2017 року, використав Facebook для публікації реквізитів банківських рахунків відомих терористів[60]. Ще один приклад — справа Мохаммеда Ікбала Голамауллі та Назімабі Голамауллі, засуджених у Лондоні в листопаді 2016 року: вони надсилали кошти своєму племіннику Заффіру в Сирію через кур'єра, однак домовленості щодо переказу обговорювали у WhatsApp. Ще один випадок поєднання соціальних мереж та інших методів описаний у Прикладі 4.

53. Jessica Davis, 'New Technologies but Old Methods in Terrorism Financing', Research Briefing No. 2, Project CRAAFT, 2020.
54. Rudner, '"Electronic *Jihad*"'.
55. Europol, 'Three Arrested in Spain for Terrorist Financing', 26 March 2021, <https://www.europol.europa.eu/media-press/newsroom/news/three-arrested-in-spain-for-terrorist-financing>, дата звернення: 18.12.2021.
56. APG/MENAFATF, 'Social Media and Terrorism Financing', 2019, <http://www.apgml.org/news/details.aspx?n=1142>, дата звернення: 14.01.2022.
57. FATF, 'Financing of the Terrorist Organisation Islamic State in Iraq and the LeBAnt (ISIL)', лютий 2015 року, с. 24–25; Міністерство юстиції США, 'Global Disruption of Three Terror Finance Cyber- Enabled Campaigns'.
58. Jacobson, 'Terrorist Financing and the Internet'; UN Office on Drugs and Crime (UNODC), 'The Use of the Internet for Terrorist Purposes', 2012, <https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf>, дата звернення: 19.03.2021.
59. Eurojust, 'Terrorism Convictions Monitor' (No. 30, April 2018), p. 24, <https://www.eurojust.europa.eu/sites/default/files/Publications/Reports/2018-04_TCM-30_EN.pdf>, дата звернення: 14.01.2021.

Приклад 4: «Justice for Sisters»: онлайн-краудфандинг та опосередковане фінансування діяльності організацій

Кампанія під назвою «Justice for Sisters» («Справедливість для сестер») улітку 2019 року продемонструвала тенденцію ісламістських екстремістів використовувати прикриття гуманітарної діяльності для збору коштів перед їх транснаціональним переміщенням. Кампанія зібрала тисячі євро через онлайн-краудфандинг у форматі «pop-up» у соціальних мережах, нібито на потреби жінок, утримуваних у таборі Аль-Хол у північній Сирії.

Організатори поширювали у Telegram-каналах, пов'язаних з «Ісламською державою», відео, фотографії та письмові свідчення німецькою, англійською та арабською мовами, часто апелюючи до добробуту малолітніх дітей задля стимулювання пожертв. Донорів скеровували на кілька рахунків PayPal MoneyPool, сума на кожному з яких не перевищувала 1 800 євро (поріг, після якого власника рахунку зобов'язують надати додаткову ідентифікаційну інформацію для проведення належної перевірки відповідно до законодавства ЄС).

За повідомленнями, кошти згодом переводилися через німецького посередника до Туреччини за системою хавала, а далі — до власників крамниць усередині табору в Сирії. Щоб уникнути виявлення PayPal, донорам давали інструкції не використовувати ісламські терміни в призначенні платежу; зокрема, кампанії позначали як «Honeymoon in Vienna» («Медовий місяць у Відні») та іншими подібними фразами.

Ще одна нова типологія фінансування тероризму, пов'язана із соціальними мережами, передбачає отримання терористичними угрупованнями та окремими екстремістами рекламних доходів від сервісів розміщення контенту. Том Кітінджі та Флоренс Кін звернули увагу на те, що розміщення терористичного контенту може приносити прибуток завдяки показу брендованої реклами у відео[61].

Один із таких випадків було виявлено у 2017 році, коли реклама брендів, серед яких Mercedes Benz та британська мережа супермаркетів Waitrose, з'являлася у публікаціях, розповсюджуваних «Ісламською державою»[62]. Цю стратегію збору коштів також перейняли ультраправі, які отримують можливість монетизувати поширення екстремістської ідеології на таких платформах, як Instagram, TikTok, YouTube, Twitch та DLive[63].

60. Tom Keatinge and Florence Keen, 'Social Media and Terrorist Financing: What Are the Vulnerabilities and How Could Public and PriBAte Sectors Collaborate Better?', Global Research Network on Terrorism and Technology, Paper No. 10, RUSI, 2019, <https://static.rusi.org/20190802_grntt_paper_10.pdf>, дата звернення: 31.01.2022.
61. Alexi Mostrous, 'Big Brands Fund Terror Through Online Adverts', *The Times*, 9 February 2017.
62. Комітет Палати представників Конгресу США з фінансових послуг, 'Memorandum: February 25, 2021, NSIDMP Hearing Entitled, "Dollars Against Democracy: Domestic Terrorist Financing in the Aftermath of the Insurrection"', 22 February 2021, <https://financialservices.house.gov/ uploadedfiles/hhrg-117-ba10-20210225-sd002.pdf>, дата звернення: 18.03.2021;
63. Megan Squire, 'Monetizing Propaganda: How Far-Right Extremists Earn Money by Video Streaming', конференція

Оцінка

На основі зібраних даних можна зробити висновок, що більшість підсекторів FinTech не фігурували у випадках операційного чи організаційного фінансування тероризму в Європі з 2015 року. Свідчення їх використання переважно відсутні у відкритій інформації про планування атак, хоча постачальники платіжних послуг трапляються у низці справ і — разом із цифровими банками — могли б фігурувати частіше, якби було доступно більше матеріалів справ.

У досліджуваний період більш помітну роль у фінансуванні діяльності ісламістських екстремістів відігравали усталені платіжні платформи та віртуальні активи (ВА), однак основу залучення та переміщення організаційних коштів і надалі складали традиційні засоби — кур'єри, посередники, компанії з надання послуг грошових переказів (MSB) та хавала.

Водночас найбільше значення мала роль соціальних мереж, які виконували промоційну та організаційну функції у процесах збору й управління коштами, іноді у поєднанні з «основними» традиційними методиками. Як зазначає Девіс, нові технології частіше з'являються у контексті вже існуючих методів ФТ, а не як самостійні трансформаційні інструменти[64].

Отримані результати порушують два важливі запитання:

1. Чому терористи наразі не використовують FinTech, особливо нових постачальників, більш активно?
2. Наскільки ймовірно, що наявність прихованих або недоступних доказів може призвести до інших висновків?

Щодо першого запитання, видається малоймовірним, що терористи-одинаки, які діють у Європі, потребують фінансових інновацій для здійснення тих не надто складних атак, до яких вони наразі вдаються. Ножі, тупі предмети та багато компонентів саморобних вибухових або запальних пристроїв можна безперешкодно придбати у відкритому інтернеті (або у звичайних магазинах) з використанням уже наявних традиційних банківських рахунків та/або FinTech першого покоління, наприклад PayPal[65]. Для осіб що нінансують тероризм ситуація може бути подібною, особливо серед ісламістських екстремістів, які користуються перевіреними платіжними механізмами, такими як хавала, що є складними для відстеження.

Попередні дослідження у цій сфері справді підкреслювали, що існують вагомі підстави не очікувати значних змін у підходах через специфіку процесу ухвалення рішень терористами. Дослідження з поведінкових фінансів, проведене Пітером Дж. Філліпсом та Бенджаміном МакДермідом, свідчить про наявність серйозних підстав вважати, що рішення осіб що фінансують тероризм будуть «інертними» та систематично зміщеними на користь старих, більш знайомих і — що особливо важливо — перевірених та надійних способів переказу коштів[66].

В іншому дослідженні Том Кітінджі та Керстін Даннер встановили, що фінансова інноваційність терористів є найчастіше зумовлена необхідністю

64. Davis, 'New Technologies but Old Methods in Terrorism Financing'.
65. See Reimer and Redhead, 'A New Normal'.
66. Peter J Phillips and Benjamin McDermid, 'FinTech, Terrorism-Related Fund Transfers and Behavioural Finance', *Dynamics of Asymmetric Conflict* (Vol. 14, No. 3, 2021), pp. 226–46.

«та є реакцією на зовнішні чинники»[67]. Іншими словами, якщо попередні підходи, як і раніше, демонструють ефективність, то стимулів змінювати їх майже немає.

Існують також інші можливі причини, які слід враховувати, розглядаючи труднощі переходу до використання нових технологій. Як зазначалося в попередньому розділі, існує припущення, що FinTech є більш уразливим для терористів та інших злочинців через нижчі стандарти належної перевірки. Водночас, визнаючи, що багато нових FinTech-компаній, ймовірно, справді є вразливими на ранніх етапах свого розвитку, коли системи та процедури ще нові, цей стан не триває безкінечно.

Посадова особа, відповідальна за звітування про відмивання коштів (money laundering reporting officer, MLRO) у великій FinTech-компанії, опитана в межах цього дослідження та раніше залучена до роботи в традиційному фінансовому секторі, зазначила, що після досягнення певного етапу на «кривій зрілості» суттєвої різниці у стандартах між «старими» та «новими» технологіями немає. Керівник глобальної консалтингової компанії з питань комплаєнсу, яка тісно співпрацює з FinTech-фірмами, теж висловив подібну думку[68].

Підсумовуючи, усталені FinTech-компанії не обов'язково є більш сприятливим середовищем для терористів, ніж традиційні фінансові установи.

Нарешті, існує питання складності використання та доступності, що особливо стосується віртуальних активів (ВА). Використання ВА для придбання товарів з метою підготовки атаки у відкритому інтернеті все ще є складним завданням, а робота в даркнеті вимагає додаткових технічних навичок і впевненості. Нікіта Малік також раніше зазначала, що передбачувана анонімність користувачів криптовалют не є гарантованою, оскільки публічно доступний блокчейн транзакцій дозволяє особам з достатніми комп'ютерними знаннями «відстежити цифровий слід анонімних трейдерів»[69].

Том Кітінджі, Девід Карлайл та Флоренс Кін також підкреслювали складність використання ВА для цілей організаційного фінансування тероризму через труднощі з їх конвертацією назад у фіатну валюту для використання в традиційній економіці[70]. Імовірно, саме з цих причин, наприклад, Національна оцінка ризиків Великої Британії за 2020 рік зазначає, що хоча спостерігається незначне зростання використання ВА терористами[71], поширеним таке використання вважати вкрай малоймовірно[72].

Друге запитання, безумовно, є значно складнішим. Видається малоймовірним, що багато секторів FinTech наразі експлуатуються у великому масштабі, проте все ж існують підстави для пильного спостереження за за тими «масовими» постачальниками

67. Tom Keatinge and Kerstin Danner, 'Assessing InnoBAtion in Terrorist Financing', *Studies in Conflict and Terrorism* (Vol. 44, No. 6, 2021), pp. 455–72.
68. Інтерв'ю авторів із MLRO (посадовою особою, відповідальною за звітування про відмивання коштів) у FinTech-компанії, що надає платіжні послуги, 27.05.2021; інтерв'ю авторів із старшим консультантом з фінансових злочинів у FinTech, 07.05.2021..
69. Malik, *Terror in the Dark*.
70. Keatinge, Carlisle and Keen, 'Virtual Currencies and Terrorist Financing'; Salami, 'Terrorism Financing with Virtual Currencies'.
71. Рівень ризику для ВА було підвищено з низького до середнього для фінансування тероризму у період між 2017 та 2020 роками, що пояснюється зростанням доступності на тлі вдосконалення технологій ВА.
72. See HM Treasury and Home Office, *National Risk Assessment of Money Laundering and Terrorist Financing 2020* (London: The Stationery Office, 2020).

які залучені до процесів використання та переказу коштів, особливо у підсекторах цифрового банкінгу та платіжних послуг[73].

Ще однією сферою, що потребує обережності, є масштаби минулого використання віртуальних активів (ВА). Згідно з доказами, представленими під час судового розгляду, Гішам Чаудгарі повідомив своїм контактам у Telegram, що «Ісламська держава» використовувала криптовалюту «роками» для організаційного фінансування[74]. Можливо, це була випадкова репліка, однак вона заслуговує на подальший аналіз.

Як показує подальший розгляд поточних заходів із протидії фінансуванню тероризму (ПФТ), більш комплексний збір даних буде необхідним для вироблення більш точного та релевантного підходу до оцінки реальних ризиків у сфері FinTech.

73. Інтерв'ю авторів із керівником підрозділу комплаєнсу з питань протидії фінансовим злочинам у великій компанії — постачальнику платіжних послуг, 24.07.2021.
74. James Rodger, 'Sales Consultant with "Saviour Complex" Jailed for Funding ISIS with Bitcoin', *Birmingham Mail*, 3 September 2021.

III. Поточні заходи реагування

Роль нових технологій у фінансуванні тероризму була підкреслена FATF у жовтні 2015 року в її звіті «Emerging Terrorist Financing Risks» («Нові ризики фінансування тероризму») поряд із «традиційними» питаннями, такими як використання компаній, що надають послуги грошових переказів (MSB), перевізників готівки та системи хавала[75].

Відтоді ця тематика привернула увагу ключових учасників системи протидії фінансуванню тероризму (ПФТ) в ЄС. Законодавці оновили регулювання, що стосується віртуальних активів (ВА) та краудфандингу, а представники усталених сегментів фінансового сектору намагалися зменшити ризики, скорочуючи співпрацю з окремими клієнтами з FinTech, особливо з постачальниками послуг, пов'язаних із віртуальними активами (VASP).

Однак, як показано в розділі II, ризики, з якими стикаються різні сегменти сектора FinTech, суттєво відрізняються та, згідно з наявними даними, ймовірно є більш незначними, ніж багато хто побоюється. У певному сенсі віртуальні активи (ВА) стали своєрідним «страшилом» сектора FinTech і «першочерговою» темою для обговорення потенційних нових ризиків ФТ у розмовах із посадовцями та експертами з комплаєнсу[76].

Водночас, це, ймовірно, є переоцінкою значення ВА у FinTech загалом, а також і поточних ризиків ФТ. Цифровий банкінг та постачальники платіжних послуг становлять більшу частину ринку FinTech і, навіть попри відсутність очевидно високих ризиків ФТ, можуть становити більший інтерес у разі наявності більш обґрунтованої доказової бази.

Крім того, нинішній підхід ЄС не враховує питання, пов'язані із соціальними мережами — новою технологією, яка формально не належить до FinTech, але вже містить помітні ризики ФТ, що поки що не були належним чином усунені.

У цьому розділі буде проаналізовано стан поточних заходів реагування на ймовірні зловживання новими технологіями з метою фінансування тероризму з метою визначення загального рівня ризику. Якщо, наприклад, застосовувані нині заходи пом'якшення ризиків та інші відповіді є адекватними та пропорційними характеру загрози, як це викладено в розділі II, то ступінь, у якому поява нових технологій змінила наявні ризики, буде обмеженим.

У подальшому буде здійснено оцінку заходів реагування як з боку державного, так і з боку приватного секторів.

ЄС та протидія фінансуванню тероризму

Відповідно до рекомендацій FATF, регуляторний підхід ЄС до протидії фінансуванню тероризму (CTF) повністю інтегрований у його систему протидії відмиванню коштів (AML) та викладений у шести послідовних версіях Директиви ЄС щодо протидії відмиванню коштів (AMLD), остання з яких була оприлюднена у жовтні 2018 року.

---

75. FATF, 'Emerging Terrorist Financing Risks', October 2015, pp. 30–39.
76. Інтерв'ю авторів із керівником підрозділу ПФР держави-члена ЄС, 26.07.2021; інтерв'ю авторів із посадовцями інституцій ЄС, 07.06.2021; інтерв'ю авторів із старшим консультантом з питань фінансових злочинів у сфері FinTech, 07.05.2021.

Кожна версія встановлює перелік мінімальних стандартів, яких мають дотримуватися держави-члени, хоча новий план Європейської комісії у сфері AML, оприлюднений у липні 2021 року, передбачає створення єдиного та уніфікованого підходу для всіх держав-членів[77].

Хоча вимоги AMLD з часом стали ширшими та детальнішими, основні елементи залишилися здебільшого незмінними. Правопорушення, пов'язані з фінансуванням тероризму (ФТ), були криміналізовані, а на приватний сектор покладено обов'язок виконувати роль «воротаря» фінансової системи. Компанії, що працюють у фінансовому секторі або на його периферії, мають здійснювати різні рівні перевірки клієнтів (customer due diligence, CDD), щоб ідентифікувати потенційно відомих осіб що фінансують тероризм та відстежувати поведінку клієнтів для виявлення незвичних дій, які можуть бути пов'язані з ФТ. Якщо така діяльність видається підозрілою, зобов'язані суб'єкти повинні подати відповідні повідомлення про підозрілі операції (suspicious transaction reports, STRs) до національного ПФР для подальшого передання правоохоронним або іншим компетентним органам[78].

Окрім регуляторної основи, в ЄС діє низка інституцій, що мають певні повноваження у сфері ПВК/ФТ (AML/CTF). З точки зору нагляду, три Європейські наглядові органи (European Supervisory Authorities, ESA), серед яких найважливішим є Європейський банківський орган (European Banking Authority, EBA)[79], мають мандат підтримувати обмін наглядовою інформацією з питань AML/CTF.

Поліцейське агентство Europol також відіграє важливу роль як розвідувальний центр у сфері ПФТ, у структурі якого функціонують: Європейський центр з протидії тероризму (European Counter-Terrorism Centre, ECTC), європейський сегмент Програми відстеження фінансування тероризму ЄС–США (Terrorist Finance Tracking Program, TFTP), а також Європейське державно-приватне партнерство у сфері фінансової розвідки (European Financial Intelligence Public/PriBAte Partnership, EFIPPP). Останнє об'єднує національні правоохоронні органи, регуляторів та провідні фінансові установи для стратегічного обміну розвідувальною інформацією щодо всіх предикатних правопорушень у сфері ПВК/ФТ [80].

Робота з ФТ та новими технологіями

Законодавці ЄС визначили віртуальні активи (ВА) та постачальників послуг, пов'язаних із віртуальними активами (VASP), як найбільш ризикові нові фінансові технології з точки зору фінансування тероризму[81]. Автори формулювань нового плану Європейської комісії у сфері AML/CTF назвали появу ВА однією з головних причин необхідності реформ. Оголошуючи нові заходи 20 липня 2021 року, Європейська комісія зазначила, що реформує систему для того, щоб врахувати «нові та такі, що з'являються, виклики, пов'язані з технологічними

77. European Commission, 'Questions and Answers: Anti-Money Laundering and Countering Financing of Terrorism (AML/CFT)', 20 July 2021, <https://ec.europa.eu/commission/presscorner/detail/en/qanda_21_3689>, accessed 10 December 2021.
78. See Matthew Redhead, 'Deep Impact? Refocusing the Anti-Money Laundering Model on Evidence and Outcomes', *RUSI Occasional Papers* (October 2019).
79. Дві інші установи — Європейський орган з нагляду за страховою діяльністю та пенсійним забезпеченням (European Insurance and Occupational Pensions Authority, EIOPA) та Європейське управління з цінних паперів і ринків (European Securities and Markets Authority, ESMA).
80. RUSI, 'Survey Report: Five Years of Growth in Public–PriBAte Financial Information-Sharing Partnerships to Tackle Crime', August 2020, pp. 79–81, accessed 13 December 2021.
81. Authors' interview with European banking official, 27 August 2021.

Інноваціями, з особливим акцентом на «віртуальні валюти»[82]. Не дивно, що в ЄС спостерігається послідовне прагнення забезпечити охоплення ширшого кола VASP режимом AML/CTF. Це почалося з включення VASP, які працюють на межі світу фіатних валют і ВА, таких як біржі обміну фіат–криптовалюта та кастодіальні гаманці, до п'ятої AMLD у травні 2018 року[83], а тепер у новому плані з AML запропоновано поширити його дію на всі інші типи VASP, включно з біржами обміну ВА–ВА[84].

Крім того, Європейська комісія запропонувала поширити дію Регламенту про переказ коштів 2015 року на VASP, щоб імплементувати нові вимоги, ухвалені FATF у червні 2019 року[85]. Відоме у фінансовій сфері як Travel Rule, це нововведення вимагатиме від усіх VASP збирати інформацію про ініціатора та одержувача для будь-якої транзакції, зменшуючи рівень анонімності для користувачів ВА в межах ЄС та їхніх безпосередніх контрагентів, потенційно — за межами ЄС[86].

Паралельно з активними діями щодо зменшення потенційних ризиків, пов'язаних із віртуальними активами (ВА), окремі інституції в системі ЄС визнали, що виклики, які нові технології можуть створювати для протидії фінансуванню тероризму, значно ширші, ніж лише ВА. Водночас потенційні ризики ФТ з боку інших секторів FinTech були більш непомітно інтегровані у вже наявні структури ПВК/ФТ.

Оскільки більшість основних підсекторів FinTech надають послуги, що повторюють функції традиційного фінансового сектору, вони, по суті, вже підпадають під вимоги ПВК/ФТ за замовчуванням. Водночас постачальники платіжних послуг на основі інтернет-технологій були спеціально включені до сфери дії 4AMLD у травні 2015 року[87].

Були й винятки, зокрема краудфандинг, який дотепер розглядається як окремий випадок. У травні 2014 року Франція ухвалила Указ 2014-559, спрямований на реєстрацію та базове регулювання краудфандингових платформ, що займаються інвестиціями та кредитуванням[88], однак ця практика не отримала широкого поширення серед інших держав-членів ЄС.

---

82. European Commission, 'Beating Financial Crime: Commission Overhauls Anti-Money Laundering and Countering the Financing of Terrorism Rules', 20 July 2021, <https://ec.europa.eu/commission/presscorner/detail/en/IP_21_3690>, дата звернення: 20.12.2021.
83. *Official Journal of the European Union*, 'Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 Amending Directive (EU) 2015/849 on the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing, and Amending Directives 2009/138/EC and 2013/36/EU', 19 June 2018, p. 2, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L0843&from=EN>, дата звернення: 13.12.2021.
84. European Commission, 'Beating Financial Crime'.
85. FATF, 'Updated Guidance for a Risk-Based Approach: Virtual Assets and Virtual Asset Service Providers', October 2021.
86. Це випливає з вимог, встановлених FATF. Див. там само.
87. *Official Journal of the European Union*, 'Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing, Amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and Repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC', 5 June 2015, p. 2, <https:// eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L0849&from=EN>, дата звернення: 13.12.2021.
88. Уряд Франції, «Ordonnance n° 2014-559 du 30 mai 2014 relative au financement participatif», https://www.legifrance.gouv.fr/loda/id/JORFTEXT000029008408/ .

ЄС ухвалив власний Регламент про краудфандинг для платформ із винагородою (return-based platforms) у жовтні 2020 року, запровадивши вимогу здійснювати перевірку клієнтів (CDD) щодо тих, хто шукає фінансування, хоча й не прямо з міркувань ПВК/ФТ[89].

У межах нового плану з ПВК Європейська комісія також пропонує включити платформи краудфандингу, заснованого на пожертвах (donation-based crowdfunding), до переліку зобов'язаних суб'єктів за правилами ПВК/ФТ. Підходи, засновані на прибутку (profit-based), не включені, оскільки, за оцінкою Комісії, чинний Регламент про краудфандинг «містить достатні запобіжники для провайдерів краудфандингових послуг, що підпадають під його сферу дії»[90].

Ще однією сферою, на яку варто звернути увагу, є реакція ЄС на діяльність у соціальних мережах. Підхід ЄС до протидії розповсюдженню терористичного контенту в інтернеті передбачає обмін оперативною розвідувальною інформацією для сприяння його видаленню. Наразі ЄС прагне посилити ці заходи, запроваджуючи додаткові законодавчі вимоги, що перегукуються із Законом про забезпечення мережевої дії (Netzwerkdurchsetzungsgesetz, NetzDG), ухваленим у Німеччині у вересні 2017 року, який зобов'язував провайдерів соціальних мереж видаляти терористичний контент зі своїх платформ[91].

Згідно з новим Регламентом ЄС щодо протидії поширенню терористичного контенту в інтернеті, ухваленим у травні 2021 року, постачальники послуг хостингу (hosting service providers, HSP) — компанії, які забезпечують онлайн-інфраструктуру для соціальних мереж та інших вебсайтів — повинні виявляти та видаляти контент, «який підбурює або спонукає когось до вчинення чи сприяння вчиненню терористичних злочинів»[92]. Водночас, хоча широке тлумачення цієї норми могло б охоплювати й інформацію, що поширюється з метою фінансування тероризму, прямо ця можливість у регламенті не зазначена.

Налаштування регулювання

Хоча прагнення ЄС реагувати на потенційні ризики ФТ, пов'язані з новими технологіями, не можна вважати помилковим, його політична реакція виявилася недостатньо диференційованою. Підхід ЄС полягав у тому, щоб інтегрувати більшість елементів сектора FinTech у вже наявну регуляторну систему ПВК/ФТ за замовчуванням або, у випадку онлайн-платежів та ВА, шляхом їхнього спеціального включення.

Це, безумовно, має очевидні переваги: прагнення до комплексного охоплення нових FinTech-сегментів може зменшити ризик масштабного перенесення діяльності осіб що фінансують тероризм у цей сектор. Водночас, з огляду на відносну незрілість значної частини цього сектору та

89. *Official Journal of the European Union*, 'Regulation (EU) 2020/1503 of the European Parliament and of the Council of 7 October 2020 on European Crowdfunding Service Providers for Business, and Amending Regulation (EU) 2017/1129 and Directive (EU) 2019/1937', 20 October 2020, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32020R1503&rid=4>, дата звернення: 21.12.2021..
90. *Там само.*
91. Міністерство юстиції Німеччини, «Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz – NetzDG)», https://www.gesetze-im-internet.de/netzdg/BJNR335210017.html, дата звернення: 13.12.2021.
92. EU Monitor, 'Regulation 2021/784 – Addressing the Dissemination of Terrorist Content Online', <https://www.eumonitor.eu/9353000/1/j9vvik7m1c3gyxp/vlivmgatiaxg>, дата звернення: 10.12.2021.

задекларованe ЄС прагнення сприяти його зростанню[93], застосування до нього повного обсягу регуляторних вимог може виявитися контрпродуктивним. Доцільнішим було б обрати більш калібрований підхід до ризиків у кожному підсекторі, а не очікувати впровадження стандартних процедур комплаєнсу з ПВК/ФТ повсюдно. У деяких випадках — наприклад, у низькоризикових сферах, таких як страхування або інвестиції — це могло б означати застосування м'якших вимог, тоді як в інших — наприклад, у сегменті нових платіжних сервісів — потребувало б більш суворих заходів комплаєнсу з фокусом на ризики ФТ[94].

Такий більш деталізований підхід уже застосовується в одному з підсекторів FinTech — краудфандингу: платформи з винагородою (return-based), що належать до низькоризикових, залишаються поза режимом ПВК/ФТ, тоді як платформи, що збирають пожертви і пов'язані з вищими ризиками, включаються до нього[95].

Звісно, контраргументом до деталізації є «ризик-орієнтований підхід» (risk-based approach, RBA). Протягом майже 20 років FATF та її члени наголошують, що компанії повинні застосовувати перевірку клієнтів (CDD) та інші заходи з урахуванням специфіки, щоб виявляти індивідуальні ризики та відповідно налаштовувати внутрішні політики, процедури та механізми контролю[96]. Теоретично це правильна порада. Однак на практиці її складно реалізувати, особливо коли компанії перебувають на ранніх етапах розвитку й не мають сформованої внутрішньої експертизи у сфері комплаєнсу — майже універсальна проблема для молодих FinTech-компаній[97]. Ба більше, така ситуація сприяє тим постачальникам, де ризики ФТ імовірно є нижчими, та ускладнює роботу тих, де вони вищі.

Якщо сектори з підвищеним рівнем ризику хочуть ефективно впоратися з цими викликами, є підстави для розробки більш детальних регуляторних настанов щодо ПВК/ФТ (а можливо, й інших заходів з протидії фінансовим злочинам) для FinTech-компаній на ранніх етапах розвитку.

Найбільш тривожною прогалиною в регуляторному режимі ЄС з ПВК/ФТ на сьогодні є становище соціальних мереж. За результатами цього дослідження, вони належать до числа найбільш проблемних нових технологій, що використовуються для організаційного фінансування тероризму. Проте вони не мають жодних зобов'язань у межах AMLD чи за консервативного тлумачення регламенту про терористичний контент. Очевидно, що цю ситуацію слід змінити, навіть якщо зміни не передбачатимуть повного віднесення соціальних мереж до категорії зобов'язаних суб'єктів за режимом ПВК/ФТ. Як зазначалося в попередніх дослідженнях RUSI, вимога до платформ соціальних мереж змінити умови надання послуг, розширивши визначення «терористичного контенту», не є складним завданням[98].

Крім того, логічним наступним кроком видається зобов'язання платформ соціальних мереж або хостинг-провайдерів шукати, виявляти та повідомляти не лише про підозріле поширення пропаганди, але й фінансову інформацію, навіть якщо це дещо розмиє межі секторних зобов'язань.

93. Європейська комісія, «Digital Finance», https://ec.europa.eu/info/business-economy-euro/banking-and-finance/digital-finance_en, дата звернення: 22 грудня 2021 р.
94. Інтерв'ю авторів із провідним консультантом FinTech з питань фінансових злочинів, 7 травня 2021 р.
95. Reimer and Redhead, 'Following the Crowd'.
96. FATF, 'Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing: High Level Principles and Procedures', червень 2007 р.
97. Інтерв'ю авторів із провідним консультантом FinTech з питань фінансових злочинів, 7 травня 2021 р.
98. Keatinge and Keen, 'Social Media and Terrorist Financing', p. 17.

Як зазначив один із європейських експертів з питань протидії тероризму, терористи зазвичай не переймаються діями в межах офіційних категорій, а беруть «те, що є під рукою, і використовують у спосіб, який їм зручний»[99]. Влада має продемонструвати таку саму гнучкість, щоб випереджати дії терористів.

Водночас будь-які такі зобов'язання спричинять додаткові виклики, оскільки модерація контенту пов'язана з ризиком хибнопозитивних і хибнонегативних результатів так само, як моніторинг транзакцій у фінансових установах. Розробка оптимальних правил модерації контенту для запобігання ФТ є непростим завданням для приватного сектору. Це ще одна причина, чому ефективна модерація потребує кращої співпраці між державними та приватними структурами щодо того, на що саме мають звертати увагу платформи[100].

Оцінка ефективності державного сектору

Існують глибші проблеми в оцінюванні реагування ЄС на фінансування тероризму у контексті нових технологій. Значна частина подальшого обговорення ґрунтується на припущенні, що ЄС інтегрує FinTech-компанії та інші сектори в загалом ефективний режим ПВК/ФТ. Однак це припущення можна поставити під сумнів. Модель передбачає, що суб'єкти приватного сектору здатні виявляти релевантну фінансову розвідку щодо ФТ та передавати її органам влади у вигляді звітів про підозрілі транзакції (STRs). Проте дослідження свідчать, що ця система надає вкрай мало цінної розвідувальної інформації, а також є надмірно бюрократизованою та несвоєчасною за термінами її подання[101].

Як і багато національних урядів, ЄС намагався вирішити цю проблему шляхом запровадження партнерства з обміну фінансовою розвідкою (financial intelligence sharing partnership, FISP) — EFIPPP, щоб забезпечити тіснішу стратегічну комунікацію між державним і приватним секторами. Це стало позитивним, хоча й обережним кроком уперед. Наразі представництво приватного сектору в EFIPPP переважно складається з традиційних фінансових установ, що мають транскордонні інтереси. Якщо партнерство прагне отримати більш реалістичне уявлення про фактичні ризики у секторах FinTech та соціальних мереж, воно має активніше залучати їх до співпраці — як через асоційоване членство, так і через участь у робочих групах. З огляду на все ще фрагментарний стан наявної розвідки щодо ризиків ФТ у цих секторах та серйозну стурбованість політиків ЄС стосовно таких технологій, як віртуальні активи (ВА), видається необхідним забезпечити їхню присутність у партнерстві.

Реакція приватного сектору

Оскільки реагування державного сектору на зловживання новими технологіями для фінансування тероризму значною мірою визначається занепокоєнням щодо теоретичних вразливостей, компанії приватного сектору здебільшого залишені самостійно формувати власну реакцію на сприйнятий ризик, стосовно якого вони отримали небагато офіційних рекомендацій. Такі заходи можуть бути зумовлені як необхідністю виконання зобов'язань і реагування на реальні загрози, так і побоюваннями щодо регуляторних та репутаційних ризиків.

99. Інтерв'ю авторів з європейським науковцем-експертом з протидії тероризму, 9 червня 2021 р.
100. Keatinge and Keen, 'Social Media and Terrorist Financing', pp. 15–16.
101. Matthew Redhead, 'The Future of Transaction Monitoring: Better Ways to Detect and Disrupt Financial Crime', SWIFT Institute Working Paper No. 2020-001, січень 2020 р., сс. 5–8.

Хоча деякі традиційні фінансові установи намагалися використати потенціал FinTech, створюючи партнерства з новими компаніями або власні дочірні FinTech-продукти[102], у традиційній індустрії існують різноманітні побоювання щодо ризиків, які можуть нести нові гравці. Особливе занепокоєння знову викликають віртуальні активи (ВА): класичні банки неохоче відкривають рахунки для криптовалютних бірж або проводять транзакції їхніх клієнтів, зазвичай обґрунтовуючи це побоюваннями щодо фінансових злочинів[103]. Замість того щоб управляти невизначеними ризиками, деякі традиційні установи просто вирішили повністю уникати таких відносин.

У США, де зростає занепокоєння щодо посилення крайньо правих рухів, є свідчення того, що деякі FinTech-компанії самі застосовують стратегію «де-ризингу»/уникнення, яка є поширеною серед усталених гравців. Багато краудфандингових кампаній, організованих крайніми правими групами, були видалені з основних платформ, таких як GoFundMe та Kickstarter, після мітингу «Unite the Right» у Шарлотсвіллі, штат Вірджинія, у 2017 році. Великі постачальники платіжних послуг, зокрема PayPal, Stripe, Apple Pay та Google Pay, також відмовилися приймати платежі на спеціально створених краудфандингових платформах [104]. Постачальники платіжних послуг, зокрема PayPal, також припинили обслуговування платформи GiveSendGo після заворушень у Капітолії США 6 січня 2021 року[105].

У Європі, однак, підхід поки що видається менш проактивним. Майже всі FinTech-компанії та галузеві експерти, опитані в межах цього дослідження, відзначали, що компанії дуже серйозно ставляться до дотримання вимог ПВК/ФТ; водночас вони визнавали, що багато FinTech-компаній не розглядають ФТ як проблему, рівнозначну за важливістю шахрайству чи відмиванню коштів. Унаслідок цього базові ризики ФТ, пов’язані з платежами у юрисдикції підвищеного ризику, враховуються у сценаріях моніторингу транзакцій, проте більш складні сценарії не розробляються[106]. Крім того, деякі компанії, що стикаються зі складними ризиками ФТ, сприймають їх просто як частину загального ризику ведення бізнесу. Один з опитаних у межах цього дослідження P2P-кредиторів надавав краудфандинговий капітал

102. *Finextra*, ‘UK Banks Plan to Grow Partnerships with Fintech Firms in Wake of Pandemic’, 11 October 2021, <https://www.finextra.com/newsarticle/38992/uk-banks-plan-to-grow-partnerships-with-fintech-firms-in-wake-of-pandemic>, accessed 12 January 2022.
103. Lily Russell-Jones, ‘HSBC Bans UK Customers From Making Payments to Binance’, *City AM*, 4 August 2021.
104. Sheila Dang, ‘No Cash for Hate, Say Mainstream Crowdfunding Firms’, *Reuters*, 14 August 2017; BAnessa Romo, ‘Charlottesville Jury Convicts “Unite the Right” Protester Who Killed Woman’, *NPR*, 7 December 2018; Tom Keatinge, Florence Keen and Kayla Izenman, ‘Fundraising for Right-Wing Extremist Movements: How They Raise Funds and How to Counter It’, *RUSI Journal* (Vol. 164, No. 2, 2019), pp. 10–23.
105. Olivia Solon and Leticia Miranda, ‘“Too Little, Too Late”: Extremism Experts Criticize Payment Companies’, *NBC News*, 13 January 2021.
106. Інтерв’ю авторів із відповідальним працівником за дотримання вимог фінмоніторингу (MLRO) FinTech-компанії, що надає банківські послуги, 22 липня 2021 р.; інтерв’ю авторів із відповідальним працівником за дотримання вимог фінмоніторингу (MLRO) європейського постачальника платіжних послуг / FinTech, 28 липня 2021 р.; інтерв’ю авторів із керівником підрозділу з протидії фінансовим злочинам постачальника послуг, пов’язаних із віртуальними активами (VASP), 26 липня 2021 р.; інтерв’ю авторів із керівником підрозділу з дотримання вимог фінмоніторингу у великого постачальника платіжних послуг, 24 липня 2021 р.; інтерв’ю авторів із FinTech-компанією, що надає послуги у форматі «платежі як сервіс» (PaaS), 23 липня 2021 р.

компаніям-кредиторам, розташованим за межами Європи, які, у свою чергу, пропонували короткострокові позики до зарплати, автокредити чи бізнес-позики фізичним особам. Хоча P2P-кредитор, базований у Європі, міг проводити належну перевірку клієнта (CDD) стосовно іноземної компанії-кредитора, він був змушений довіряти, що та здійснює такі самі перевірки щодо кінцевих отримувачів[107].

Водночас деякі FinTech-компанії явно прагнуть застосовувати більш інноваційні підходи до управління ризиками ФТ, виходячи за межі стандартної моделі ПВК/ФТ. Їхня цифрова природа та відсутність обтяження застарілими багаторівневими системами дає змогу збирати дані про поведінку клієнтів, які традиційні фінансові установи не так просто агрегують чи відстежують, зокрема IP-адреси та геолокацію. Використовуючи цю інформацію, компанії динамічно оновлюють оцінки ризику ФТ клієнта на основі його поведінки. Наприклад, якщо клієнт часто входить у систему з місця, відмінного від задекларованого місця проживання, це може стати підставою для «червоного прапорця» з точки зору ФТ[108]. Так само деякі усталені FinTech-компанії інвестували ресурси в інструменти мережевого аналізу, що дає їм змогу проводити проактивний аналіз у сфері протидії ФТ, включаючи перевірку клієнтських баз на предмет потенційних зв'язків (отримувачів переказів) з терористами, ідентифікованими правоохоронними органами[109]. Аналіз розвідданих із соціальних мереж (SOCMINT) уже інтегрований у системи управління ризиками фінансових злочинів багатьох FinTech-компаній[110].

Також існує значний інтерес серед FinTech-компаній до участі в діяльності партнерств з обміну фінансовою розвідкою (FISP). Найдоступнішими для приєднання є приватні ініціативи, як-от глобальне FinTech Financial Crime Exchange (FFE), яке має багато європейських учасників[111] та заохочує проактивний обмін типологічною інформацією про ФТ та інші фінансові злочини. Водночас, хоча кілька FinTech-компаній, опитаних у межах цього дослідження, висловили сильне бажання долучитися до державних публічно-приватних FISP, у своїх юрисдикціях вони часто стикалися з тим, що ці структури функціонують як «закриті клуби», які надають перевагу співпраці між правоохоронними органами та великими усталеними фінансовими установами[112].

А що ж із соціальними мережами? Модерація контенту зазнала значного посилення після нападу крайньо правого екстреміста в Крайстчерчі (Нова Зеландія) у 2019 році, який злочинець записав та транслював наживо на платформах соціальних мереж. У відповідь було проголошено «Christchurch Call» — ініціативу урядів Нової Зеландії та Франції, спрямовану на заохочення технологічних компаній співпрацювати з урядами задля усунення терористичного контенту з інтернету. Ця ініціатива спиралася на вже наявну приватну співпрацю[113],

---

107. Інтерв'ю авторів із командою з комплаєнсу європейської P2P-платформи кредитування, 28 травня 2021 р.

108. Інтерв'ю авторів із відповідальним працівником за дотримання вимог фінмоніторингу (MLRO) великої FinTech-компанії, що надає платіжні послуги, 27 травня 2021 р.

109. *Там само.*

110. Tom Keatinge and Florence Keen, 'Social Media and Terrorist Financing: Time for a Focused Response', *RUSI Newsbrief* (Vol. 37, No. 4, October 2017); Tom Keatinge and Florence Keen, 'Social Media and (Counter) Terrorist Finance: A Fund-Raising and Disruption Tool', *Studies in Conflict and Terrorism* (Vol. 42, No. 1–2, 2019), pp. 178–205.

111. FINTRAIL, 'FinTech FinCrime Exchange', <https://fintrail.com/ffe>, дата звернення: 16 березня 2022 р..

112. нтерв'ю авторів із керівником підрозділу з дотримання вимог фінмоніторингу у великого постачальника платіжних послуг, 24 липня 2021 р.; інтерв'ю авторів із відповідальним працівником за дотримання вимог фінмоніторингу (MLRO) великої FinTech-компанії, що надає платіжні послуги, 27 травня 2021 р.; інтерв'ю авторів із відповідальним працівником за дотримання вимог фінмоніторингу (MLRO) FinTech-компанії, що надає банківські послуги, 22 липня 2021 р.

113. Global Internet Forum to Counter Terrorism (GIFCT) було створено у 2017 р. компаніями Facebook, Microsoft, Twitter та YouTube «з метою запобігти використанню цифрових платформ терористами та насильницькими екстремістами [шляхом] сприяння технічній співпраці між компаніями-учасниками, розвитку відповідних…».

дослідницькі програми, орієнтовані на проблематику радикалізації та профінансовані самими соціальними мережами[114], а також на використання модераторів контенту й автоматизованих систем його видалення.

Втім, ці ініціативи рідко зосереджувалися на проблемі використання соціальних мереж з метою фінансування тероризму[115].

Соціальні мережі, такі як Facebook, почали самостійно вживати заходів у випадках, коли їхніми платформами користуються не включені до офіційних списків, але неприйнятні екстремісти, зокрема з метою фінансування. Їхня політика щодо небезпечних осіб та організацій (Dangerous Individuals and Organizations policy) визначає, що користувачам дозволено говорити про створений самою платформою список «організацій з історією терористичної або насильницької кримінальної діяльності»[116]. Разом із витоком знімка самого списку[117], який містить чимало ісламістських екстремістських та крайньо правих угруповань, не включених до жодного офіційного списку терористичних організацій, видання The Intercept у жовтні 2021 р. опублікувало інструкції для модераторів контенту. Ці інструкції передбачають видалення публікацій, що «надають пряму (збір коштів, благодійні кампанії тощо) або непряму (відмивання коштів, бухгалтерські чи банківські послуги тощо) фінансову підтримку організації [зі списку]»[118]. Наскільки поширеним став цей підхід серед усіх соціальних мереж, наразі невідомо.

Оцінка реагування приватного сектору

Різні учасники традиційного фінансового сектору, а також секторів FinTech та соціальних мереж обрали три загалом відмінні підходи до управління ризиками ФТ: уникнення ризиків шляхом відмови від взаємодії; зниження пріоритетності цих ризиків у межах наявних комплаєнс-рамок; або спроби більш проактивного управління цими ризиками за допомогою нових інструментів та зовнішньої взаємодії.

У контексті відносно низьких або помірних ризиків ФТ, притаманних більшості секторів FinTech, про що свідчать результати цього дослідження, видається, що повна відмова від взаємодії є надмірною реакцією, навіть щодо таких суперечливих підсекторів, як постачальники послуг, пов'язаних із віртуальними активами (VASPs).

114. Global Network on Extremism and Technology — академічний дослідницький підрозділ GIFCT, що працює на базі Міжнародного центру вивчення радикалізації при Королівському коледжі Лондона.
115. Tech Against Terrorism hosted a rare CTF-focused event in October 2021. See Tech Against Terrorism, 'TAT & GIFCT E-Learning Session – Online Terrorist Financing: Assessing the Risks and Mitigation Strategies', <https://www.techagainstterrorism.org/event/tat-gifct-e-learning-session- online-terrorist-financing-assessing-the-risks-and-mitigation-strategies/>, accessed 14 January 2022.
116. Sam Biddle, 'Revealed: Facebook's Secret Blacklist of "Dangerous Individuals and Organizations"', *The Intercept*, 12 October 2021.
117. *The Intercept*, 'Facebook Dangerous Individuals and Organizations List (Reproduced Snapshot)', 12 October 2021, <https://theintercept.com/document/2021/10/12/facebook-dangerous-individuals-and-organizations-list-reproduced-snapshot/>, accessed 7 January 2022.
118. *The Intercept*, 'Facebook Praise, Support and Representation Moderation Guidelines (Reproduced Snapshot)', 12 October 2021, <https://theintercept.com/document/2021/10/12/facebook-praise-support-and-representation-moderation-guidelines-reproduced-snapshot/>, accessed 7 January 2022.

Подібні рішення по де-ризикінгу можуть ґрунтуватися на законних міркуваннях прибутковості та толерантності до ризику, проте після того, як П'ята директива ЄС з ПВК/ФТ (5AMLD) 2018 року поширила статус зобов'язаних суб'єктів і на VASPs, така вибіркова практика не може бути виправдана лише цими міркуваннями.

Водночас надто поблажливий підхід також може бути небезпечним. Низькі або помірні ризики не означають, що потенційне ФТ не відбувається, а самозаспокоєність може призвести до того, що компанії пропускатимуть очевидні проблеми — проблеми, які посилюються браком регуляторних орієнтирів щодо ризиків ФТ. Як зауважив старший фахівець з комплаєнсу глобального постачальника платіжних послуг, дуже легко дійти висновку: «ми не знаємо, як виглядає ФТ, тож ми його не бачимо, а отже, його не існує»[119].

Хоча FinTech-компанії стикаються з тією самою проблемою, що й усталені установи, вона може відчуватися особливо гостро, коли компанії є ще незрілими, невеликими та лише намагаються закріпитися на ринку. Для швидкозростаючих FinTech-компаній складно вчасно й у повному обсязі інвестувати у впровадження регуляторних технологій (RegTech) відповідно до темпів зростання, що може призвести до їхньої неготовності реагувати на нові ризики [120]. FinTech-компанії також можуть стикатися з більшими труднощами через те, що — як показує приклад згаданих вище P2P-кредиторів — вони зазвичай є меншими гравцями у великих екосистемах і мають обмежене розуміння практик та рівня надійності партнерських FinTech-компаній, з якими змушені взаємодіяти.

Попередній регуляторний підхід до нових фінансових компаній не передбачав надання підтримки в частині знань для окремих сегментів фінансового сектору. Проте поява численних FinTech-компаній із обмеженим досвідом у сфері комплаєнсу, ймовірно, свідчить про потребу змінити підхід — принаймні на початкових етапах зростання, — забезпечивши більш прямі початкові рекомендації з питань, зокрема, ПВК/ФТ, у процесі становлення таких компаній. Також доцільно, щоб уряди подбали про повну імплементацію інфраструктур, які підтримують належний комплаєнс, — наприклад, реєстрів загальноприйнятих KYC-даних, — аби менші компанії могли без зайвих труднощів отримувати необхідну інформацію для ефективного управління своїми ризиками.

Мабуть, найпозитивнішим аспектом реагування FinTech-компаній є зусилля тих із них, які намагаються використовувати більш інноваційні методи для виявлення ризиків ФТ. Використання кращих даних та доступних компаніям технологій є позитивним кроком, який має отримувати регуляторне заохочення та потенційне визнання. Крім того, очевидне прагнення багатьох FinTech-компаній ділитися розвідувальною інформацією та знаннями через FISP також є корисним. Водночас видається малоймовірним, що приватні партнерства, які не мають ключового внеску з боку правоохоронних органів і регуляторів щодо актуальних типологій, можуть бути настільки ж ефективними, як їхні публічно-приватні аналоги. Хоча питання членства FinTech-компаній у таких державних FISP не належить до компетенції приватного сектору, воно майже напевно принесло б користь обом сторонам.

---

119. Інтерв'ю авторів із старшим фахівцем з комплаєнсу великого постачальника платіжних послуг, 27 липня 2021 р.
120. Інтерв'ю авторів із відповідальним працівником за дотримання вимог фінмоніторингу (MLRO) FinTech-компанії, що надає банківські послуги, 22 липня 2021 р.; інтерв'ю авторів із керівником підрозділу з протидії фінансовим злочинам у великого постачальника платіжних послуг, 24 липня 2021 р.

Оцінювати реагування платформ соціальних мереж на проблему ФТ складно. Позитивним кроком є те, що принаймні деякі учасники галузі вважають своїм обов'язком видаляти не лише матеріали, безпосередньо пов'язані з фінансуванням тероризму, але й пропагандистський контент, навіть за відсутності чітких юридичних вимог робити це. Незалежно від того, чи мотивовані такі дії репутаційними міркуваннями, закриття облікових записів або видалення контенту, пов'язаного з ФТ, є безумовним суспільним благом.

Водночас цю діяльність слід здійснювати обережно та у спосіб, який не знищує потенційну розвідувальну цінність відповідних матеріалів. Системно зібрана розвідінформація з відкритих джерел у соціальних мережах (SOCMINT) могла б бути використана для виявлення типологій ФТ, що здійснюється через соцмережі, та для розроблення стратегій протидії ФТ, спрямованих на їхнє припинення[121]. Іншим ненавмисним наслідком підходу «видалення» може стати ефект витіснення, коли особи що фінансують тероризм починають діяти в менш видимих просторах, що скорочує можливості для збору розвідданих, які виникають унаслідок використання терористами нових технологій, і які могли б бути корисними для зусиль із протидії ФТ[122].

Активні та спеціалізовані канали обміну розвідувальною інформацією, що стосується ФТ, між підрозділами фінансової розвідки (ПФР), правоохоронними органами (LEA) та, за можливості, розвідувальними органами, є необхідними для забезпечення того, щоб ключові облікові записи в соцмережах залишалися відкритими в інтересах збору розвідданих та подальшого масштабного припинення діяльності мереж: видалення сьогодні може бути менш цінним, ніж широка операція із нейтралізації завтра.

Ще однією проблемою є те, що значна частина відповідних даних або розвідувальної інформації часто зберігається у компаній, розташованих у зарубіжних юрисдикціях, які діють у різних регуляторних умовах щодо обміну даними. Для Європи це особливо актуально, коли йдеться про потенційні розвіддані, що знаходяться у соціальних мережах, базованих у США. Втім, на всіх платформах, видалення контенту здійснене з метою збереження доброї репутації, не можуть бути довгостроковою гарантією зменшення ризиків ФТ і в окремих випадках навіть можуть мати зворотний ефект.

121. Keatinge and Keen, 'Social Media and Terrorist Financing'; Keatinge and Keen, 'Social Media and (Counter) Terrorist Finance'.
122. *Ibid.*; Davis, 'New Technologies but Old Methods in Terrorism Financing'; EBA Entenmann and Willem BAn den Berg, 'Terrorist Financing and Virtual Currencies: Different Sides of the Same Bitcoin?', International Centre for Counter-Terrorism – The Hague, 1 November 2018, <https://icct.nl/publication/terrorist-financing-and-virtual-currencies-different-sides-of-the-same-bitcoin/>, дата звернення: 7 січня 2022 р

IV. Ключові висновки та рекомендації щодо політики

Вісім ключових висновків цього дослідження супроводжуються відповідними рекомендаціями щодо політики для ЄС, його інституцій та агентств, а також для самих держав-членів. Виконання цих рекомендацій дасть змогу ЄС точніше налаштувати та покращити своє реагування на зловживання новими технологіями з боку осіб що фінансують тероризм, а також ефективніше використовувати унікальні можливості сектору FinTech для протидії ФТ.

Ключовий висновок 1: Більшість досліджених атак у Європі за останні шість років (74%) були здійснені терористами-одинаками. Там, де є публічно доступна інформація про фінансування атак, нові технології рідко фігурують у фінансуванні чи підготовці нападів, а коли й з'являються, то здебільшого це відомі платіжні платформи першого покоління (такі як PayPal), які є повсюдно поширеними в суспільстві. Найбільш показовою є відсутність віртуальних активів (ВА), які, попри занепокоєння щодо їх можливого зловживання для оплати незаконних товарів, фігурували лише в одному випадку.

- **Рекомендація 1(а):** Європейські наглядові органи (ESAs) мають заохочувати національних регуляторів, а також зобов'язані компанії у секторі FinTech до оновлення своїх оцінок ризиків ФТ та забезпечення того, щоб їхні політики, процедури й механізми контролю — особливо моніторинг транзакцій — були належним чином адаптовані до цієї реальності.
- **Рекомендація 1(б):** ESAs та Європол мають провести аналіз поширеності використання усталених платіжних платформ у контексті ФТ та типологій їхнього використання екстремістами, а також запросити цих постачальників послуг до співпраці у сфері генерування розвідувальної інформації з метою проактивного припинення діяльності. Така співпраця має здійснюватися у форматі серії воркшопів, щоб забезпечити довгострокове партнерство.

Ключовий висновок 2: Дослідження виявило більше прикладів використання нових технологій у сфері організаційного ФТ — для залучення та переказу коштів — ніж у фінансуванні операцій. Знову ж таки, фігурують усталені постачальники платіжних послуг, а також соціальні мережі як інструмент «тимчасового» краудфандингу. Крім того, є кілька більш помітних прикладів використання віртуальних активів (ВА) для збору коштів представниками різних ідеологічних напрямів. Водночас більшість підсекторів FinTech залишаються незалученими, а ознак того, що нові технології витіснили старі методи — такі як діяльність постачальників грошових послуг (MSB), система «хавала» та перевезення готівки кур'єрами, які й надалі домінують, — небагато. Скоріше, йдеться про паралельне використання старих і нових методів у прагматичних комбінаціях, що відповідають потребам осіб що фінансують тероризм.

- **Див. Рекомендацію 1(б):** За аналогією з Рекомендацією 1(б) вище, європейські регуляторні органи мають заохочувати національних регуляторів та зобов'язані компанії до оновлення своїх оцінок ризиків, пов'язаних з організаційним ФТ, у разі необхідності.

- **Рекомендація 2:** Європейський центр з протидії тероризму Європолу (ECTC) має підготувати та опублікувати аналіз того, як різні технології та методи використовуються у поєднанні. Такий звіт має містити деталі типологій, щоб допомогти зобов'язаним суб'єктам точніше налаштовувати свої механізми контролю для виявлення підозрілої діяльності.

Ключовий висновок 3: Попри зростаюче розуміння ризиків ФТ, пов'язаних із новими технологіями, це дослідження визнає, що все ще існують суттєві прогалини у знаннях, і необхідно провести додаткову роботу для їхнього заповнення, усунення неоднозначностей та розширення доказової бази. Потенційно можуть існувати приховані ризики організаційного фінансування, пов'язані з віртуальними активами (ВА), а також можливість того, що основні підсектори FinTech з високими обсягами клієнтів і транзакцій — онлайн-банкінг та постачальники платіжних платформ — можуть бути задіяними у ФТ значніше, ніж це очевидно зараз.

- **Рекомендація 3(а):** З метою виявлення цього «прихованого ризику» Європол має провести ретроспективний аналіз конфіденційної інформації щодо минулих випадків, щоб з'ясувати, чи окремі ключові сектори не були задіяні значніше, ніж це виглядає наразі.
- **Рекомендація 3(б):** У майбутньому Європол також має застосовувати більш суворий підхід до систематичного збору даних щодо ФТ для підготовки майбутніх звітів TE-SAT, щоб визначати частоту використання того чи іншого методу у фінансуванні операцій та організацій. Це має ґрунтуватися на централізовано розробленому шаблоні, а не наданні державами-членами правоохоронних органів лише фрагментарних або анекдотичних даних.

Ключовий висновок 4: Деякі заяви провідних політиків ЄС щодо ризиків, пов'язаних із новими технологіями, а також публічні меседжі від Європейської комісії, виглядають незбалансованими з огляду на реальний масштаб ситуації та рівень ризиків. Нові технології — це не лише віртуальні активи (ВА), а новизна не обов'язково означає високий ризик. Ба більше, така риторика суперечить окремим іншим задекларованим цілям ЄС. Надмірний акцент на вразливості секторів нових технологій як таких погано узгоджується з проголошеним Комісією прагненням сприяти цифровим та фінансовим інноваціям, тож необхідно досягти кращого балансу та активно його комунікувати.

- **Рекомендація 4:** Європейська комісія та керівники агентств ЄС мають публічно визнавати масштаби застосування нових технологій у фінансовій системі та різний рівень ризику в численних підсекторах. Загалом стратегія щодо фінансових інновацій повинна передбачати комплексний підхід як до можливостей, так і до ризиків, а Комісія має розробити комунікаційну стратегію, яка забезпечуватиме баланс між ними.

Ключовий висновок 5: Підхід ЄС, що передбачає інтеграцію більшості елементів FinTech у вже наявну структуру ПВК/ФТ, відповідає моделі, яка застосовується понад три десятиліття. Втім, йому бракує гнучкості та нюансованості: існують очевидні ризики, пов'язані з підходом «єдиного стандарту» до нових секторів, які легко можуть постраждати від надмірного регуляторного тиску. Більш м'який підхід — подібний до того, який був застосований до краудфандингу — був би більш доречним для підсекторів із нижчим рівнем ризику, таких як страхування чи інвестиції, особливо на ранніх етапах їхнього розвитку. Натомість підвищена увага та додаткова регуляторна підтримка мали б застосовуватися у підсекторах із великими обсягами операцій, таких як платіжні сервіси чи онлайн-банкінг.

- **Рекомендація 5(а):** Наразі відмова від стандартизованої інтеграції секторів FinTech у вже наявні Директиви ЄС з ПВК/ФТ (AMLD) неможлива. Втім, у середньостроковій перспективі новостворене Агентство з ПВК/ФТ, якщо воно буде створене відповідно до запропонованих планів, має переглянути застосування вимог ПВК/ФТ у своєму новому «Єдиному звідному регламенті» (Single Rulebook), щоб забезпечити чутливість до ризиків і реалій кожного підсектору. План з ПВК/ФТ надає ЄС можливість запровадити більш гнучкий підхід.
- **Рекомендація 5(б):** У короткостроковій перспективі європейські наглядові органи (ESAs) мають підготувати галузеві настанови у стилі ФАТФ щодо застосування ризик-орієнтованого підходу (RBA) до різних підсекторів FinTech. Настанови Європейського банківського органу (EBA) з факторів ризику (Risk Factor Guidance), востаннє оновлені у 2021 р., також слід переглянути[123]. Бажано, щоб обидва документи ґрунтувалися на прикладах типологій ФТ, розроблених на основі конкретних випадків Європолом (див. Рекомендацію 2).

Ключовий висновок 6: «Цифрова» природа багатьох FinTech-компаній відкриває нові можливості для їхнього внеску у заходи з протидії фінансуванню тероризму (ПФТ) поза межами режиму подання звітів про підозрілі транзакції (STRs), зокрема через обмін і проактивний аналіз деяких нефінансових даних, якими вони володіють, наприклад IP-адрес користувачів.

- **Рекомендація 6:** Національні підрозділи фінансової розвідки (ПФР) мають налагодити діалог із сектором FinTech у своїй юрисдикції для створення партнерств з обміну даними в межах подання повідомлень про підозрілу діяльність. Подібні підходи слід врахувати і під час формування Агентства ЄС з ПВК/ФТ.

Ключовий висновок 7: Платформи соціальних мереж не є «фінансовими інструментами», але їхні комунікаційні можливості дають змогу екстремістам поширювати фінансову інформацію або надавати вказівки, як і куди надсилати кошти. Це робить такі платформи корисними інструментами для ФТ — факт, який досі не врахований у чинному регулюванні ЄС щодо терористичного контенту в інтернеті. Цю прогалину необхідно усунути.

- **Рекомендація 7(а):** Відповідні нормативні акти ЄС щодо терористичного контенту мають бути прямо доповнені положеннями, які забороняють поширення фінансової інформації або інструкцій для цілей ФТ.
- **Рекомендація 7(б):** Платформи соціальних мереж повинні нести юридичну відповідальність за передання інформації, що стосується ФТ, до національного ПФР або, бажано, до національних правоохоронних чи розвідувальних органів, уповноважених на проведення розслідувань у сфері ПВК/ФТ.
- **Рекомендація 7(в):** Європол має створити захищений портал SOCMINT для подання інформації, пов'язаної з ФТ, від платформ соціальних мереж. Ці дані слід використовувати для інформування діяльності Європейського центру з протидії тероризму (ECTC), визначеної в Рекомендації 3.

Ключовий висновок 8: Партнерства з обміну фінансовою розвідувальною інформацією (FISP) стали корисним доповненням до вже існуючих механізмів обміну фінансовою інформацією в межах режиму ПВК/ФТ.

123. European Banking Authority, 'Guidelines on ML/TF Risk Factors (Revised)', <https://www.eba.europa.eu/regulation-and-policy/anti-money-laundering-and-e-money/revised-guidelines-on-ml-tf-risk-factors>, accessed 16 March 2022.

Наразі європейське FISP — EFIPPP, що функціонує як центр обміну стратегічною розвідкою та розробки типологій, — обмежило членство приватного сектору лише системно важливими фінансовими установами. Унаслідок цього втрачаються важливі можливості для діалогу між довгостроковими ключовими учасниками системи ПВК/ФТ та новими гравцями фінансового ринку.

- **Рекомендація 8:** EFIPPP має запросити до участі провідні європейські FinTech-компанії, особливо з підсекторів банківських та платіжних послуг, краудфандингу на основі пожертв, віртуальних активів (ВА), а також представників соціальних мереж і відповідних європейських галузевих асоціацій. Їхня участь — зокрема у новій «технологічній робочій групі» — має бути використана для підтримки роботи ESAs та Європолу з удосконалення регуляторних настанов і збору розвідувальної інформації щодо ризиків ФТ.

Висновки та перспективи на майбутнє

У цій записці розглянуто, наскільки нові технології створили нові ризики ФТ або ж посилили ті, що вже існували в Європі до появи FinTech. Відповідь на це питання виявилася складною, зокрема через проблеми з визначенням термінів: поняття «нові технології» використовувалося нечітко в дискусіях на цю тему, а увага часто зосереджувалася на найбільш «екзотичних» технологіях — віртуальних активах та постачальниках послуг, пов'язаних із віртуальними активами (VASPs), що звужувало висвітлення всієї сфери FinTech та інших дотичних секторів.

Тісно пов'язана з проблемою визначення є й проблема доказової бази. Через відсутність чіткого розуміння того, що саме може бути релевантним для ФТ, державні органи та зобов'язані суб'єкти приватного сектору не були достатньо ретельними у зборі доказів, які допомогли б прояснити рівень ризиків. У результаті наявна доказова база залишається недостатньою, а дискусія формується радше під впливом філософських припущень та гучних заголовків, ніж на основі всебічних даних.

З одного боку, існує група «песимістів», до якої здебільшого належать представники державного сектору та сектору традиційних фінансових послуг; вони наголошують на теоретичних ризиках нових технологій, і їхню позицію можна підсумувати так: «якщо щось може бути використано неправомірно — воно буде використано». У літературі «песимісти» стверджують, що нові технології:

- надають терористам нові канали для здійснення ФТ;
- підтримують їхню «техніку» ФТ завдяки низьким транзакційним витратам і нібито анонімності;
- ведуть до зниження рівня нагляду через нібито слабші механізми контролю фінансових злочинів.

З іншого боку, є «оптимісти», які здебільшого представляють сектори нових технологій та наголошують на обмеженій кількості матеріалів, що свідчать про підвищений ризик ФТ; можна сказати, що у деяких випадках тут простежується припущення: відсутність доказів розглядається як доказ відсутності ризику.

Щоб перевірити ці дві гіпотези, у цьому дослідженні було розглянуто наявну доказову базу максимально всебічно, водночас визнаючи обмеження, зумовлені новизною тематики. Загалом дослідження дозволяє звузити розрив між позиціями «песимістів» і «оптимістів»: ризики ФТ дійсно існують у певних нових технологіях, але вони не є загальними для всього сектору FinTech і проявляються сильніше в одних підсекторах, ніж в інших. Ба більше, ризики ФТ виходять за межі фінансового сектору. Соціальні мережі можуть підсилювати ці ризики, якщо використовуються паралельно зі старими та новими фінансовими методами для координації організаційних кампаній зі збору коштів.

Режим протидії ФТ в ЄС спирається на усталені базові елементи, які покладають на зобов'язані суб'єкти фінансового сектору та інших дотичних учасників роль охоронців і «воротарів» системи. Протягом останнього десятиліття політики ЄС намагалися інтегрувати різні елементи FinTech у вже наявні структури ПВК/ФТ, зобов'язуючи більшість — але не всі підсектори — дотримуватися відповідних вимог. Водночас інші сфери, зокрема соціальні мережі, продовжують розглядатися окремо. Така стратегія, хоч і узгоджується з підходом, підтриманим FATF, має низку проблем, які потребують вирішення.

У процесі реагування на ризики ФТ, що виникають у зв'язку з новими технологіями, існує небезпека припускати, що ці ризики — або їхня відсутність — є вродженими та незмінними. Проте ситуація, ймовірно, змінюватиметься з часом, особливо якщо нові технології отримають ширше поширення в суспільстві. Тому будь-які висновки, зроблені в межах цього дослідження, мають попередній характер і потребуватимуть повторного перегляду в майбутньому, що підкреслює важливість усунення прогалин у знаннях та підтримання якісної бази розвідувальної інформації.

Хоча це не породжує додаткових рекомендацій, але ще раз підкреслює значущість зусиль Європолу у сфері збору розвідданих та їхньої публікації в щорічних звітах TE-SAT, а також потребу — як зазначено в Рекомендації 3(б) — у більш системному та всебічному підході.

Про авторів

Stephen Reimer — науковий співробітник Центру досліджень фінансових злочинів і безпеки RUSI, спеціалізується на протидії фінансуванню тероризму та фінансуванню загроз загалом. Його нещодавні роботи зосереджені на фінансуванні тероризму терористами-одинаками в Європі, загрозах національній безпеці з боку нелегальних фінансових потоків та оцінюванні ризиків зловживання фінансуванням тероризму у неприбутковому секторі.

Matthew Redhead — автор публікацій з питань фінансових злочинів і національної безпеки, а також незалежний консультант із ризиків фінансових злочинів для секторів FinTech та RegTech. Раніше працював у фінансовій сфері та в уряді Великої Британії.