

www.rusi.org



Посібник з оцінки ризиків фінансування розповсюдження зброї масового знищення

Ноемі Тамбе

Червень 2023

192 years of independent thinking on defense and security

The Royal United Services Institute (RUSI) is the world's oldest and the UK's leading defense and security think tank. Its mission is to inform, influence and enhance public debate on a safer and more stable world. RUSI is a research-led institute, producing independent, practical and innovative analysis to address today's complex challenges.

Since its foundation in 1831, RUSI has relied on its members to support its activities. Together with revenue from research, publications and conferences, RUSI has sustained its political independence for 192 years.

The views expressed in this publication are those of the author(s), and do not reflect the views of RUSI or any other institution.

Published in 2023 by the Royal United Services Institute for Defence and Security Studies.



This work is licensed under a Creative Commons Attribution – Non-Commercial – No-Derivatives 4.0 International Licence. For more information, see <http://creativecommons.org/licenses/by-nc-nd/4.0/>.

June 2023

Royal United Services Institute
for Defence and Security Studies
Whitehall
London SW1A
2ET United
Kingdom
+44 (0)20 7747 2600
www.rusi.org
RUSI is a registered charity (No.
210639)



Зміст

Подяки	iii
Короткий зміст	1
Вступ	2
I Підготовка до роботи	4
Роль приватного сектору	4
Що таке розповсюдження та фінансування розповсюдження?	4
Відмінності та подібності між ФР, ВК та ФТ	7
II Методологія оцінки ризиків ПФ	12
Категорії ризиків	12
Вразливість до ризику ФР та наступні кроки	21
III Категорії ризиків та фактори ризиків	25
Висновки	33
Про автора	34

Подяки

Автор висловлює подяку Дімплу Рабадіа та Маріо Менцу за рецензування та корисні коментарі до попередньої версії цього документа. Ми також дякуємо всім, хто щедро запропонував свій час для інтерв'ю з метою розробки цього посібника, а також команді RUSI Publications за редакторську роботу.

Короткий зміст

Потенційна участь приватного сектору в підтримці програм створення ЗМЗ є широкою. Розповсюджувачам потрібен доступ до приватного сектору, щоб генерувати кошти, переказувати їх та купувати товари подвійного призначення. Крім того, їм потрібно використовувати приватний сектор для торгівлі з компаніями і, зрештою, для імпорту товарів подвійного призначення до своєї юрисдикції. Таким чином, хоча уряди відіграють важливу роль у створенні нормативно-правової бази для боротьби з фінансуванням розповсюдження (ФР), вони потребують співпраці з приватним сектором для досягнення ефективної глобальної системи протидії фінансуванню розповсюдження (СРФ). Таким чином, приватний сектор, включаючи фінансові установи (ФУ), відіграє важливу роль у виявленні діяльності, яка може бути підозрілою, інформуванні відповідних органів, заморожуванні активів та застосуванні фінансових санкцій.

Цей посібник покликаний забезпечити підтримку приватного сектору в різних юрисдикціях у виявленні діяльності, яка може бути пов'язана з підвищеним ризиком, визначенні рівнів ризиків ФР, з якими стикається сектор, та розробці стратегій для подолання таких ризиків. Завдяки проведенню приватним сектором інституційних оцінок ризиків (ОР) національні органи влади отримують більш повне розуміння ризиків ФР на національному рівні. ОР ФР допоможе установам краще зрозуміти та визначити власну схильність до ризику, водночас дотримуючись законів та нормативно-правових актів у сфері СРФ.

Посібник описує способи, за допомогою яких фінансові установи повинні розуміти властиві їм ризики ФР, з якими вони стикаються через своїх клієнтів, пропоновані продукти та послуги, юрисдикції, в яких вони працюють, транзакції, використовувані канали доставки та кіберзагрози. У ньому пояснюється, як фінансові установи можуть оцінити ризики, притаманні цим категоріям, враховуючи ймовірність матеріалізації ризику, а також вплив цієї події.

Після оцінки притаманного ризику наступним кроком є оцінка залишкових ризиків ФР установи. Це досягається шляхом оцінки ефективності заходів контролю, які застосовує фінансова установа для подолання притаманних ризиків. Коли установа завершує оцінку ризиків фінансування розповсюдження зброї масового знищення, вона може виміряти свій залишковий ризик, а отже, і свою вразливість до ризику фінансування розповсюдження. Після цього установа може вирішити, чи приймати цей ризик, чи продовжувати зменшувати або намагатися запобігти таким вразливим місцям та схильності до ризику фінансування розповсюдження зброї масового знищення.

Посібник пояснює, що оцінка ризиків має бути динамічним процесом, і що фінансові установи повинні забезпечити виявлення існуючих та/або майбутніх вразливостей до ФР. Крім того, оцінка ризиків повинна здійснюватися на основі ризик-орієнтованого підходу, який забезпечує установам гнучкість у питаннях СРФ.

Вступ

Розповсюджувачам потрібен доступ до офіційної фінансової системи для збору та приховування коштів і закупівлі ЗМЗ. Щоб запобігти такій діяльності, низка Резолюцій Ради Безпеки ООН (РБ ООН) накладає міжнародно-правові зобов'язання, пов'язані з фінансуванням розповсюдження (ФР): Резолюція РБ ООН 1540 про нерозповсюдження ЗМЗ, Резолюція РБ ООН 2231 про виконання Спільного всеосяжного плану дій щодо Ірану та розширені вимоги Резолюцій РБ ООН щодо Північної Кореї.¹

Група з розробки фінансових заходів боротьби з відмиванням грошей (FATF), глобальний розробник стандартів боротьби з відмиванням коштів та фінансуванням тероризму, включила стандарти протидії фінансуванню розповсюдження (ФР) до свого мандату в 2012 році. У Керівництві з СРФ пояснюється, що розуміння ризиків ФР "позитивно вплине на здатність юрисдикції запобігати залученню, переміщенню та використанню коштів фізичними та юридичними особами, причетними до розповсюдження зброї масового знищення".²

З листопада 2020 року держави-члени FATF зобов'язані проводити національні оцінки ризиків (ОР) ФР. Фінансові установи (ФУ) та визначені нефінансові установи та професії також зобов'язані проводити оцінку ризиків фінансування розповсюдження зброї масового знищення на інституційному рівні з метою "виявлення, оцінки та вжиття ефективних заходів для зменшення ризиків відмивання коштів, фінансування тероризму та фінансування розповсюдження зброї масового знищення".³ Цю вимогу посилено в "Керівництві ФАТФ з оцінки та зменшення ризиків фінансування розповсюдження зброї масового знищення" від 2021 року, в якому зазначено:

Регулярне виявлення, оцінка та розуміння ризиків фінансування розповсюдження зброї масового знищення має важливе значення для посилення здатності країни або приватного сектору запобігати залученню, зберіганню, переміщенню та використанню коштів, а отже, й інших фінансових активів визначеними фізичними та юридичними особами, причетними до розповсюдження зброї масового знищення (ЗМЗ). Впровадження [цільових фінансових санкцій], пов'язаних з розповсюдженням та його фінансуванням, має важливе значення для посилення режиму протидії фінансуванню розповсюдження зброї масового знищення (СРФ).⁴

¹ Anagha Joshi, Emil Dall and Darya Dolzikhova, 'Guide to Conducting a National Proliferation Financing Risk Assessment', RUSI, May 2019.

² FATF, 'FATF Guidance on Counter Proliferation Financing: The Implementation of Financial Provisions of United Nations Security Council Resolutions to Counter the Proliferation of Weapons of Mass Destruction', 2018, p. 4.

³ FATF, 'International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation: The FATF Recommendations', 2012, Recommendation 1, p. 10.

⁴ FATF, 'Guidance on Proliferation Financing Risk Assessment and Mitigation', June 2021, p. 7.

Національна імплементація вимог CPF, включаючи оцінку ризиків ФР, буде оцінена під час наступного раунду взаємних оцінок.⁵

Цей посібник розроблено з метою надання підтримки приватному сектору в різних юрисдикціях у виявленні та визначенні рівнів ризиків ФР, з якими він стикається, а також у розробці стратегій для подолання таких ризиків відповідно до Рекомендацій ФАТФ 1, 2, 7 та 15.⁶ ОР має дотримуватися ризик-орієнтованого підходу (РОП), який забезпечить установам гнучкість у застосуванні заходів з CPF. Ризик-орієнтований підхід не є політикою, що забезпечує безвідмовну роботу, і не перешкоджає установам взаємодіяти з клієнтами або встановлювати ділові відносини, які можуть мати вищий рівень схильності до ризику ФР. Скоріше, передбачається, що установи будуть керувати та спрямовувати свої зусилля у сферах, які становлять вищі ризики ФР.

У Розділі I цього посібника обговорюється роль приватного сектору в CPF та пояснюється ФР, тоді як у Розділі II пропонується можливий підхід до оцінки ризиків ФР, що охоплює категорії ризиків, притаманні таким категоріям ризику, засоби контролю для зменшення притаманних їм ризиків, ефективність контролю та залишковий ризик. У Розділі III фактори ризику зіставляються з категоріями ризиків і документується, яке відношення до ФР має кожен з цих факторів ризику. У ньому також викладено критерії для визначення вразливості юрисдикцій до ризиків у сфері ФР.

Цей документ слід читати разом з "Посібником з проведення національної оцінки ризиків фінансування розповсюдження зброї масового знищення", розробленим RUSI.⁷ Разом ці посібники допоможуть установам зрозуміти типи загроз та вразливостей, з якими стикаються їхні юрисдикції у сфері фінансування розповсюдження.

⁵ FATF, 'Public Statement on Counter Proliferation Financing', press release, 23 October 2020, <<https://www.fatf-gafi.org/publications/financingofproliferation/documents/statement-proliferation-financing-2020.html>>, accessed 15 October 2022; see also FATF, 'Procedures for AML/CFT/CPF Mutual Evaluations',

⁶ Recommendation 1 requires countries, FIs, 'designated non-financial businesses and professions', and virtual asset service providers to identify, assess and understand their PF risks, and take commensurate action to mitigate these risks. Recommendation 2 requires effective national cooperation and coordination mechanisms to combat PF. Recommendation 7 requires the implementation of UNSCR-based targeted financial sanctions on PF (for instance, asset freezes) and requires ensuring that 'no funds and other assets are made available, directly or indirectly, to or for the benefit of, any person or entity designated by, or under the authority of, the [UNSC] under Chapter VII of the Charter of the United Nations'. Recommendation 15 (revised in June 2021) requires the conducting of a PF risk assessment and mitigation to be established in respect of virtual asset activities and service providers; see FATF, 'International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation'.

⁷ Joshi, Dall and Dolzikova, 'Guide to Conducting a National Proliferation Financing Risk Assessment'.

I. Підготовка до роботи

У цьому розділі підкреслюється важливість приватного сектору у сфері протидії фінансуванню розповсюдження зброї масового знищення, надається визначення розповсюдження та ФР, а також окреслюються відмінності та схожість між ФР, відмиванням коштів (ВК) та фінансуванням тероризму (ФТ).

Роль приватного сектору

Для розробки ЗМЗ розповсюджувачам потрібен доступ до приватного сектору, щоб отримувати гроші, переказувати їх, купувати товари подвійного призначення⁸, торгувати з компаніями і, зрештою, імпортувати товари подвійного призначення до своєї юрисдикції. Отже, потенційна участь приватного сектору в підтримці програм створення ЗМЗ є широкою. Таким чином, "приватний сектор" у цьому контексті означає не лише фінансові установи, але й "включає виробників товарів подвійного призначення або чутливих технологій, які можуть бути вразливими до перенаправлення з метою розповсюдження, а також постачальників транспортних послуг, які використовуються розповсюджувачами для переміщення цих товарів".⁹

Дійсно, хоча уряди відіграють важливу роль у створенні нормативно-правової бази для боротьби з фінансуванням розповсюдження зброї масового знищення, вони потребують співпраці з приватним сектором для досягнення ефективної глобальної системи протидії фінансуванню розповсюдження зброї масового знищення. Приватний сектор, у тому числі фінансові установи, відіграє важливу роль у виявленні підозрілої діяльності, інформуванні відповідних органів, заморожуванні активів та застосуванні фінансових санкцій. Завдяки проведенню приватним сектором інституційних ОР, національні органи влади отримують все більш повне розуміння ризиків ФР на національному рівні.

Що таке розповсюдження та фінансування розповсюдження?

Розповсюдження в цьому контексті - це "виробництво, придбання, володіння, розробка, експорт, перевантаження, посередництво в операціях з, транспортування, передача, накопичення або використання ядерної, хімічної або біологічної зброї, засобів її доставки та пов'язаних з нею матеріалів (включаючи технології та товари

⁸ Dual-use goods are goods, software and/or technologies that can be used for both commercial and military purposes. Such goods include nuclear materials, electronics, computers, sensors and lasers, for example. The export, transit and brokering of dual-use items is controlled to preserve international peace and security and prevent the proliferation of WMD. For more on dual-use goods, see Joshi, Dall and Dolzikova, 'Guide to Conducting a National Proliferation Financing Risk Assessment'; see also John Varesi, 'Wassenaar Arrangement Control Lists', presentation to BIS 2018 Annual Conference on Export Controls and Policy,

2018, <<https://www.bis.doc.gov/documents/bis-annual-conference-2018/2212-multilateral-regime-control-lists-wassenaar-nsg-ag-mtcr-rev-13may2018/file>>, accessed 10 December 2022.

⁹ Joshi, Dall and Dolzikova, 'Guide to Conducting a National Proliferation Financing Risk Assessment', p. 34.

подвійного призначення, що використовуються в нелегітимних цілях)".¹⁰ Воно включає технології, товари, програмне забезпечення, послуги та експертизу.¹¹ "ЗМЗ" означає ядерну, хімічну, радіологічну або біологічну зброю,¹² тобто будь-яку зброю, що може спричинити масові жертви та руйнування.

Загрози застосування ЗМЗ походять як від державних груп (наприклад, Іран, Північна Корея та Сирія), так і від недержавних груп. Під "недержавними групами" мається на увазі будь-яка фізична або юридична особа, яка не дотримується правового порядку держави, такі як терористичні групи або мережі розповсюдження, що складаються з брокерів, фінансистів, постачальників або тих, хто здійснює перевантаження.¹³

Незважаючи на відсутність міжнародного консенсусу щодо визначення ФР, ФАТФ визначає ФР як "залучення, переміщення або надання коштів, інших активів чи інших економічних ресурсів, або фінансування, повністю або частково, фізичним чи юридичним особам з метою розповсюдження зброї масового знищення, включаючи розповсюдження засобів її доставки або пов'язаних з нею матеріалів (включаючи технології та товари подвійного призначення, що використовуються в нелегітимних цілях)".¹⁴

Центр нової американської безпеки визначив і задокументував три стадії ФР:

- **Збір коштів:** розповсюджувач отримує кошти з державного бюджету або від незаконної чи законної комерційної або злочинної діяльності, що здійснюється за кордоном державними суб'єктами або від їхнього імені.
- **Маскування та розміщення коштів у фінансовій системі:** розповсюджувачі покладаються на мережу підприємств, підставних компаній, непрозорих структур власності та брокерів, щоб забезпечити географічну відокремленість від країн, на які накладено санкції.
- **Закупівля матеріалів і технологій за рахунок цих коштів:** розповсюджувач отримує доступ до міжнародної фінансової системи для оплати товарів, матеріалів, технологій і логістики, необхідних для його програми щодо ЗМЗ.¹⁵

Таким чином, ФР не обмежується прямим фінансуванням ЗМЗ або товарів і технологій, схильних до розповсюдження, а охоплює широкий спектр видів діяльності. Для цілей цього посібника трьома категоріями діяльності, які можуть розглядатися як ФР і які можуть бути охоплені в рамках інституційних ОР з питань ФР, є:

- Фінансові продукти та послуги - такі як, наприклад, торгове фінансування - які можуть безпосередньо підтримувати торгівлю товарами, що можуть бути

¹⁰ FATF, 'Guidance on Proliferation Financing Risk Assessment and Mitigation', p. 8.

¹¹ Gibraltar Financial Intelligence Unit, 'Counter Proliferation Financing: Guidance Notes', June 2020, p. 4, <<https://www.gfiu.gov.gi/what-is-proliferation-financing>>, accessed 6 January 2023.

¹² The White House, 'National Security Strategy of the United States of America', December 2017, p. 8, <<https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf>>, accessed 10 April 2023.

¹³ For details of non-state groups involved in PF, see Al-Jazeera, 'Abdul Qadeer Khan: Nuclear Hero in Pakistan, Villain to the West', 10 October 2021, <<https://www.aljazeera.com/news/2021/10/10/abdul-qadeer-khan-nuclear-hero-in-pakistan-villain-to-the-west>>, accessed 31 January 2023.

¹⁴ FATF, 'Guidance on Proliferation Financing Risk Assessment and Mitigation', p. 8.

¹⁵ Jonathan Brewer, 'The Financing of Nuclear and Other Weapons of Mass Destruction Proliferation', Center for a New American Security, 24 January 2018, p. 4, <<https://www.cnas.org/publications/reports/the-financing-of-nuclear-and-other-weapons-of-mass-destruction-proliferation>>, accessed 31 January 2023.

використані або модифіковані для використання у розробці ЗМЗ.

- Доходи або активи, отримані або забезпечені в результаті законної або незаконної діяльності з фінансування закупівлі та розробки ЗМЗ, які необхідно буде розмістити у фінансовій системі та перемістити через неї.
- Фінансові та корпоративні мережі - такі як кореспондентські відносини - можуть підтримувати рух фінансів і товарів, що використовуються для розробки ЗМЗ.¹⁶

Таким чином, для цілей своїх ОР фінансові установи повинні враховувати, що ФР, визначене ФАТФ, може не охоплювати весь спектр фінансової діяльності, яка може сприяти розповсюдженню зброї масового знищення. Ця діяльність охоплюється трьома категоріями ФР, які задокументовані на Рисунку 1.

Рисунок 1: Категорії ФР



Джерело: Команда з CPF та Санкцій у Центрі досліджень фінансової злочинності та питань безпеки RUSI's

При проведенні оцінки ризиків ФР установи повинні враховувати три категорії ФР, показані на Рисунку 1, та виявляти схильність до ризику ФР, який можуть становити для установи їхні клієнти.

¹⁶ Joshi, Dall and Dolzikova, 'Guide to Conducting a National Proliferation Financing Risk Assessment', p. 18.

Відмінності та схожість між ФР, ВК та ФТ

В існуючій літературі з питань боротьби з ФР обговорюються відмінності та схожість між ФР, ВК та ФТ. Як і ФТ, ФР передбачає лінійний грошовий слід: кінцевою метою є не повернення відмитих коштів, а сприяння подальшій незаконній діяльності. Так само, як і ВК, ФР вимагає тактики приховування, наприклад, приховування відносин з кінцевими бенефіціарними власниками (КБВ), складної маршрутизації та перенаправлення міжнародних платежів, а також приховування як кінцевого використання, так і кінцевих користувачів товарів подвійного призначення. Проте, "природа ФР є багатогранною: це одночасно ризик фінансових злочинів, ризик санкцій та ризик для міжнародних заходів з протидії розповсюдженню".¹⁷¹⁷

Таблиця 1: ФР, ВК та ФТ: порівняння

	Фінансування розповсюдження	Відмивання коштів	Фінансування тероризму
Мета	<ul style="list-style-type: none"> Підтримка держав і недержавних суб'єктів у їхній незаконній розробці програм зі створення зброї масового знищення. 	<ul style="list-style-type: none"> Відмивання доходів, отриманих злочинним шляхом, з метою надання їм законного вигляду. 	<ul style="list-style-type: none"> Фінансування тероризму, терористів і терористичних організацій.
Використання формальних фінансових систем?	<ul style="list-style-type: none"> Так, а також транскордонна контрабанда готівки, золота або інших цінних товарів за допомогою "мулів" для підтримки державної та недержавної діяльності з розповсюдження. 	<ul style="list-style-type: none"> Так, а також неформальні фінансові канали, такі як "хавала", пункти обміну валют, кур'єри готівки та контрабанда. 	<ul style="list-style-type: none"> Так, а також неформальні фінансові канали, такі як "хавала", пункти обміну валют, кур'єри готівки та контрабанда.
Транзакції	<ul style="list-style-type: none"> Транзакції виглядають законними і відповідають традиційній комерційній діяльності, структуровані, як і в ВК, для приховування зв'язку з державними та недержавними суб'єктами, залученими до ФР, або для приховування кінцевого використання чи кінцевого споживача придбаних товарів подвійного призначення. 	<ul style="list-style-type: none"> Складна мережа транзакцій з використанням коштів, нерухомості, підставних або фіктивних компаній, офшорних центрів та складних структур юридичних осіб (включаючи, наприклад, трасти та фонди). 	<ul style="list-style-type: none"> Різноманітні методи, включаючи використання традиційних платіжних методів і банківської діяльності, неформальні системи переказу коштів, контрабанда готівки та дорогоцінних металів і каміння.
Джерела фінансування	<ul style="list-style-type: none"> Часто засновані на державних програмах, які стимулюють діяльність зі збору коштів, що є традиційно законною але вважається нелегітимною через зв'язок, наприклад, з Іраном та/або Північною Кореєю. 	<ul style="list-style-type: none"> Злочинна діяльність. 	<ul style="list-style-type: none"> Нелегальна та легальна діяльність. Наприклад, кошти можуть надходити від пожертвувань, від роботи за наймом або від злочинної діяльності.

¹⁷ Ibid., p. 5.

	Фінансування розповсюдження	Відмивання коштів	Фінансування тероризму
Розмір транзакцій	<ul style="list-style-type: none"> • Середній 	<ul style="list-style-type: none"> • Від малого до великого 	<ul style="list-style-type: none"> • Малі та середні
Види діяльності та сектори	<ul style="list-style-type: none"> • Складне структурування для приховування походження фінансування, а також того, для чого в кінцевому підсумку призначені кошти/активи. • Створення корпоративних мереж, які сприяють, але не можуть бути самостійно залучені до діяльності ФР. Структури кінцевої бенефіціарної власності, зв'язків та контролю є непрозорими • Вплив на всі сектори. Наприклад, закупівля товарів подвійного призначення, таких як деталі двигунів, залучення коштів через мережу закордонних підприємств, використання будівельних компаній або рибного промислу. 	<ul style="list-style-type: none"> • Складне структурування та мережа транзакцій, які можуть передбачати використання підставних компаній. • Це може бути, наприклад, бізнес з високим обігом готівки (наприклад, ресторани, цілодобові магазини та манікюрні салони), акції на пред'явника¹⁸ та використання офшорів. • Вплив на всі сектори. Наприклад, придбання предметів розкоші за кошти, отримані злочинним шляхом. 	<ul style="list-style-type: none"> • Численні, різноманітні методи, наприклад, офіційні банківські системи, неофіційні системи переказу коштів, контрабанда цінностей (дорогоцінних металів і каміння, антикваріату) та готівки. • Вплив на всі сектори. Наприклад, закупівля зброї (в тому числі ножів) та транспортних засобів (включаючи компанії з прокату автомобілів).
Грошовий слід	<ul style="list-style-type: none"> • Лінійний: рух фінансів та/або торгівля товарами, чутливими до розповсюдження, між державними та недержавними суб'єктами. 	<ul style="list-style-type: none"> • Круговий: кошти, як правило, зрештою повертаються до особи, яка їх колись згенерувала, коли кошти достатньо віддалилися від злочину. 	<ul style="list-style-type: none"> • Лінійний: кошти використовуються для підтримки і фінансування терористів та їхньої діяльності, а також їхньої інфраструктури шляхом збору, зберігання, переміщення та використання коштів. Жоден з цих етапів не обов'язково пов'язаний з насильством.
Виявлення	<ul style="list-style-type: none"> • Спеціально визначені установи та/або громадяни, юрисдикції, що викликають занепокоєння з точки зору розповсюдження, торгівля товарами, чутливими з точки зору розповсюдження, та відома діяльність, пов'язана з отриманням доходів для розповсюдження. 	<ul style="list-style-type: none"> • Підозрілі транзакції, такі як депозити, нехарактерні для статків або очікуваної діяльності клієнта. 	<ul style="list-style-type: none"> • Підозрілі відносини, наприклад, транзакції між, здавалося б, непов'язаними сторонами.

¹⁸ Bearer shares are shares that are not registered and are owned by the individual or entity that holds the physical share.

	Фінансування розповсюдження	Відмивання коштів	Фінансування тероризму
Транскордонна діяльність?	<ul style="list-style-type: none"> • Так. Ймовірно, до цього залучені громадяни або юридичні особи, пов'язані з юрисдикціями, що викликають занепокоєння з точки зору розповсюдження, а також з країнами, що мають слабе законодавство у сфері експортного контролю або зі слабким виконанням законів у цій сфері. Використання мереж організованої або транснаціональної злочинності, зокрема їхніх транспортних коридорів та посередників у їхніх мережах для переміщення товарів та/або коштів. 	<ul style="list-style-type: none"> • Так. Ймовірно, використання менших банків-кореспондентів, розташованих у країнах зі слабким законодавством у сфері боротьби з відмиванням коштів. 	<ul style="list-style-type: none"> • Так. Ймовірно, пов'язане з використанням мереж організованої або транснаціональної злочинності, зокрема їхніх транспортних коридорів та посередників у цих мережах.

Sources: Author generated, drawing on Jonathan Brewer, 'Study of Typologies of Financing of WMD Proliferation', Project Alpha, Centre for Science and Security Studies, King's College London, 13 October 2017, p. 35, <<https://www.kcl.ac.uk/csss/assets/study-of-typologies-of-financing-of-wmd-proliferation-2017.pdf>>, accessed 16 November 2022; see also Joshi, Dall and Dolzikova, 'Guide to Conducting a National Proliferation Financing Risk Assessment', p. 18; Jersey Financial Services Commission, 'Comparison: Terrorism Financing, Money Laundering and Financing the Proliferation of Weapons of Mass Destruction', 14 April 2022, <<https://www.jerseyfsc.org/industry/guidance-and-policy/comparison-terrorist-financing-money-laundering-and-financing-the-proliferation-of-weapons-of-mass-destruction/>>, accessed 16 November 2022.

II. Методологія оцінки ризиків ФР

Фінансові установи можуть включити ОР ФР у свої існуючі ОР у сфері ПВК/ФТ. Це дасть змогу підрозділам установ із протидії фінансовим злочинам (ПФЗ) легко додавати категорії ризиків ФР, фактори ризику та методології оцінювання до існуючих систем оцінки ризиків ВК/ФТ. Однак, деякі юрисдикції можуть зобов'язати установи мати окремі системи оцінки ризиків фінансування розповсюдження. Це питання слід обговорювати з відповідними наглядовими та регуляторними органами.

Крім того, при розробці ОР ФР в установі, фінансовим установам наполегливо рекомендується враховувати національні оцінки ризиків ФР (НОР), доступні в їхній юрисдикції або такі, що мають відношення до їхньої юрисдикції. НОР з ВК та ФТ можуть бути хорошим джерелом інформації, оскільки ФР, як правило, виникає не у вакуумі, а використовуючи існуючі в юрисдикції загрози та вразливості від ВК та ФТ. Слід також ознайомитися зі звітами групи експертів ООН щодо Північної Кореї.

Насамкінець, слід зазначити, що матриці, наведені нижче, є рекомендаційними, і фінансові установи повинні будуть відкалібрувати їх, щоб відобразити, серед іншого, існуючі методології оцінки, схильність до ризику та типи здійснюваного контролю. Методологія ОР повинна бути затверджена відповідними зацікавленими сторонами в межах ФУ.

Категорії ризиків

Відповідно до посібника ФАТФ для банківського сектору¹⁹, фінансові установи повинні ідентифікувати ризики ФР, з якими вони стикаються. Ці ризики можна класифікувати наступним чином:

- Клієнти.
- Продукти та послуги, що пропонуються.
- Юрисдикції, в яких працює та з якими співпрацює.
- Транзакції.
- Канали доставки, що використовуються.
- Кіберзагрози для систем і програмного забезпечення, що використовуються.²⁰

¹⁹ FATF, 'Guidance for a Risk-Based Approach: The Banking Sector', October 2014, p. 13, <<https://www.fatf-gafi.org/media/fatf/documents/reports/Risk-Based-Approach-Banking-Sector.pdf>>, accessed 2 February 2023.

²⁰ North Korea engages in malicious cyber activities to collect intelligence, threaten its perceived enemies and raise revenue. Dolzikova and Joshi note that 'North Korea has adapted its operations to take advantage

Кожна з цих категорій ризику буде оцінена на ризик ФР шляхом аналізу основних факторів ризику (це більш детально розглянуто в Розділі 3) та оцінки залишкового ризику ФР, який вони становлять. Ці дані потім включаються до оцінки ризиків ФР фінансових установ. Наприклад, розгляд факторів ризику клієнта зазвичай включає "ділову активність/професію/галузь" та "організаційно-правову форму". Аналогічно, фактори ризику продуктів та послуг можуть включати "кореспондентські банківські відносини" або "торгівлю за відкритими рахунками".

Притаманні ризики

Притаманні ризики - це ризики ФР, з якими стикається установа, до врахування застосованих заходів контролю та стратегії їх зниження. Після визначення категорій ризику, фінансові установи повинні оцінити властивий ризик цих категорій, розглядаючи ймовірність матеріалізації ризику, а також вплив події, якщо вона відбудеться. Як правило, така оцінка проводиться на основі п'яти рівнів впливу, які співвіднесені з п'ятьма рівнями ймовірності (див. Таблицю 2).

Наприклад, команда ПФЗ може, проаналізувавши типології ФР або ознайомившись зі звітами групи експертів ООН, виявити, що в "категорії ризику продукту" торгівля на відкритих рахунках може бути використана для ФР. Таким чином, ймовірність використання цього продукту для здійснення ФР може бути класифікована як "можливе". Тоді команда ПФЗ оцінить вплив як "значний", якщо виявлений ризик матеріалізується і призведе до порушення санкцій, шкоди репутації та фінансових втрат внаслідок падіння цін на акції та регуляторних штрафів.²¹

Перехресне посилання на вплив ("значний") та ймовірність ("можлива") використання продукту для здійснення ФР (див. Таблицю 2) створює "середньо-високий" рейтинг притаманного ризику ФР для продукту. Після цього команда ПФЗ повинна розглянути, чи зменшують існуючі заходи контролю притаманний ризик і, таким чином, призводять до залишкового ризику, який відповідає толерантності або апетиту до ризику установи, чи все ж таки потрібно впроваджувати додаткові пом'якшувальні заходи, щоб зменшити ризик виникнення події.

of the now-ubiquitous use of computer-based systems and telecommunications technology by financial institutions, as well as the expanding popularity of cryptocurrencies, to evade sanctions and generate revenue for the regime. Detailed information on North Korean cyber or crypto operations is not widely available, as cyber attacks can be hard to trace and attribute. However, the August 2019 PoE report estimated that, to date, North Korea had illegally acquired \$2 billion through cyber means. Some of the best-known cyber operations which are widely suspected to have been carried out by North Korean actors include the 2016 Bank of Bangladesh heist (which attempted to steal nearly \$1 billion from the bank's account at the Federal Reserve Bank of New York). See Darya Dolzikova and Anagha Joshi, 'The Southern Stratagem: North Korean Proliferation Financing in Southern and Eastern Africa', RUSI Occasional Papers (April 2020), p. 30.

²¹ For example, in 2019, Standard Chartered bank paid \$657 million to the US Department of the Treasury's Office of Foreign Assets Control to resolve sanctions violations, mainly relating to Iran. There were additional sanctions violations relating to Cuba, Sudan, Burma, Syria and Zimbabwe. See US Department of the Treasury, 'U.S. Treasury Department Announces Settlement with Standard Chartered Bank', press release, 9 April 2019, <<https://home.treasury.gov/news/press-releases/sm647>>, accessed 10 May 2023.

**Посібник з оцінки ризиків фінансування
розповсюдження зброї масового знищення
Ноемі Тамбе**

Таблиця 2: Притаманні ризики

		Вплив				
		Несуттєвий	Малий	Помірний	Великий	Суттєвий
		Властивий ризик				
Ймовірність	Певна	Середньо-низький	Середньо- низький	Середньо-високий	Середньо-високий	Екстремальний
	Майже певна	Середньо-низький	Середньо- низький	Середньо-високий	Високий	Високий
	Можлива	Низький	Середньо- низький	Середньо-низький	Середньо-високий	Середньо-високий
	Маловірогідна	Низький	Низький	Середньо-низький	Середньо-високий	Середньо-високий
	Дуже мала	Низький	Низький	Низький	Середньо-низький	Середньо-високий

Джерело: Створено автором. Адаптовано з різних систем та посібників з управління ризиками на підприємстві. Фінансові установи можуть адаптувати цю таблицю до своїх внутрішніх процесів.

Торгівля за відкритими рахунками та фінансування розповсюдження

З роками світова торгівля товарами та послугами розширювалася, як і торгівля за відкритими рахунками:

Умови відкритого рахунку [передбачають], що покупець і продавець погоджуються з умовами контракту, а товари поставляються покупцеві з подальшим чистим або взаємозаліковим платежем через банківську систему. За таких умов відкритого рахунку, якщо тільки фінансова установа не надає кредитні кошти, участь фінансової установи буде обмежена чистим платежем, і вона, як правило, не знатиме про основну причину платежу. Оскільки фінансова установа не бачить транзакції, вона не може здійснити нічого, окрім стандартної перевірки чистого або взаємозалікового платежу на предмет відмивання грошей та санкцій.

Таким чином, торгівля за відкритими рахунками дозволяє відвантажувати і доставляти товари до настання терміну платежу, при цьому експортер надсилає товаросупровідні документи безпосередньо імпортеру. У цьому процесі банк не бере участі. Як наслідок, хоча банк має доступ до файлів належної перевірки клієнтів (CDD) своїх прямих клієнтів - перевіряючи інформацію про бенефіціарних власників, господарську діяльність та минулі транзакції - він не має ключової інформації, що стосується товарів, які відвантажуються, особи та юрисдикції покупця або продавця, назви судна, судноплавної компанії або маршрутів транспортування. Це також стосується банків-посередників, які мають лише інформацію про платника та одержувача в електронному платіжному повідомленні. Імпортер та експортер товарів використовують банк лише як засіб переказу грошей.

ФУ, які пропонують торгівлю за відкритими рахунками, можуть не:

- Розуміти, чи є товар, що відвантажується, товаром подвійного призначення.

- Знати, хто перевозить товар.
- Знати, чи перебуває судно або особи, які беруть участь у торгівлі, під санкціями.
- Знати, чи пункт призначення вантажу знаходиться у підсанкційній або високоризиковій юрисдикції,.

Таким чином, хоча імпортер та/або експортер можуть бути розповсюджувачами, транзакції можуть не бути позначені як підозрілі і виглядати законними.

На відміну від торгівлі за відкритими рахунками, акредитиви вимагають від банків отримання документації, включаючи дані про контрагентів, одержувачів та інформацію про відвантаження. Це дає змогу ФУ використовувати цю інформацію для проведення ретельної належної перевірки, виокремлення певної інформації та перевірки транзакції та пов'язаних з нею даних. Наприклад, поставки, що фінансуються за допомогою документарного акредитива, дозволяють банкам, які фінансують транзакцію, мати доступ до інформації, що стосується товарів, які відвантажуються, ідентифікаційних даних та юрисдикції покупця і продавця, назви судна і судноплавної компанії, а також маршрутів доставки.

Примітка: Акредитив - це банківська гарантія того, що належний платіж буде отримано протягом обумовленого терміну. Якщо установа-платник не може виконати платіж установі-отримувачу, банк зобов'язується погасити повну суму платежу.

Source: Wolfsberg Group, ICC and BAFT, 'The Wolfsberg Group, ICC and BAFT Trade Finance Principles', 2017, p. 7, <https://www.icc-france.fr/wp-content/uploads/2021/04/TradeFinance_icc-wolfsberg-trade-finance-principless-2017.pdf>, accessed 30 May 2023.

Ідентифікація засобів контролю та оцінка ефективності засобів контролю

Після оцінки притаманних ризиків наступним кроком є оцінка залишкових ризиків ФР установи, тобто ризиків, які залишаються після застосування заходів контролю та стратегій пом'якшення для подолання притаманних ризиків. Слід зазначити, що заходи контролю, спрямовані на зменшення ризиків ВК та ФТ, також допомагають фінансовим установам зменшити ризики ФР, з якими вони можуть зіткнутися.

Так, під час започаткування та в рамках поточних ділових відносин, фінансові установи традиційно отримують та зберігають інформацію про клієнтів, щоб зрозуміти, оцінити та задокументувати ризики ВК та ФТ. Для розуміння, оцінки та документування ризиків ФР слід також збирати наступну інформацію:

- Хто є клієнтом, а також особи кінцевих бенефіціарних власників, істотних контролерів, установ-посередників у ланцюжку власності та підписантів (щоб встановити, чи є зв'язок з підсанкційною особою або юрисдикцією).
- Чим займається клієнт, в якому секторі він працює та який характер його бізнесу.
- Ідентифікаційні дані сторін, з якими клієнт веде бізнес, а також будь-яких інших

відповідних пов'язаних сторін.

- Чи має клієнт справу з товарами подвійного призначення, ядерними, дослідницькими або військовими товарами.
- Мета ділових відносин.
- Очікувана активність за рахунком.

Крім того, розуміння того, чи купує, продає, імпортує або експортує клієнт товари подвійного призначення або інші підконтрольні товари (ядерні або військові), має важливе значення для протидії фінансуванню розповсюдження. Більш конкретно, установи повинні знати:

- Чи має покупець ліцензію на торгівлю такими товарами.
- Чи є зв'язок з юрисдикцією, до якої застосовано санкції, або з територією, яка межує з юрисдикцією, до якої застосовано санкції.
- Чи передбачає торгівля перевантаження товарів.

Аналогічно, фінансові установи перевірятимуть нових та існуючих клієнтів (а також пов'язаних осіб та/або контрагентів) за санкційними списками, негативними згадками у ЗМІ та контрольними списками з метою виявлення будь-яких зв'язків з юридичними особами, громадянами або політично значущими особами (PEP), до яких застосовано санкції. Будь-які попередження та фактичні збіги повинні оброблятися відповідно до існуючих процесів ескалації, що діють у ФУ. Клієнти (та відповідні пов'язані сторони) повинні підлягати постійній перевірці протягом усього періоду їхніх відносин або життєвого циклу торгівлі. На додаток до "перевірки імен", необхідно здійснювати перевірку всіх транскордонних платежів (вхідних та вихідних), щоб забезпечити дотримання відповідних санкційних норм.

Крім того, інструменти моніторингу операцій фінансових установ повинні включати типології, що вказують на діяльність, пов'язану з фінансуванням розповсюдження. У разі виявлення таких операцій має бути проведено розслідування відповідно до існуючих у фінансовій установі процесів, спрямованих на виявлення ухилення від санкцій та/або фінансування розповсюдження. Про будь-які підозри, що виникають, необхідно повідомляти відповідні органи, що застосовують санкції, а також підрозділи фінансової розвідки, залежно від вимог юрисдикції.

Нарешті, всі співробітники повинні пройти відповідне навчання, що буде відповідати їхнім функціям та юрисдикціям. Зокрема, співробітники, які започатковують відносини з клієнтами, здійснюють оцінку ризиків, поточний моніторинг або перевірку імен та транзакцій, повинні пройти цільову підготовку з питань ризиків, типологій та індикаторів ризиків ФР.

Підсумовуючи, існуючі засоби контролю, які допомагають фінансовим установам зменшити ризики ФР, включають:

- Механізми управління.
- Управлінська інформація.
- Політика протидії ФР.
- Механізми належної перевірки клієнта (CDD)/Знай свого клієнта (KYC) (включаючи постійну належну перевірку та посилену належну перевірку).

- Механізми перевірки власних працівників (Know Your Employee)
- Оцінка ризиків клієнтів.
- Перевірка публічно відомих осіб, санкцій та контрольних списків спостереження.
- Можливість заморожувати активи визначених установ та/або громадян.
- Моніторинг транзакцій.
- Незалежне тестування засобів контролю та забезпечення якості існуючих систем і засобів контролю.
- Процеси затвердження нових продуктів, включаючи, де це можливо, рішення комітетів.
- Навчання персоналу.
- Обмеження щодо діяльності на певних ринках.
- Повідомлення про підозрілу діяльність.
- Загальнокорпоративні ОР.

Наведений вище перелік не є вичерпним, і існують додаткові елементи, які слід запровадити, і які будуть націлені конкретно на ФР. До них відносяться:

- Калібрування інструментів моніторингу транзакцій для відображення існуючих сценаріїв ФР.²²
- Перегляд звітів групи експертів ООН щодо Північної Кореї та Ірану з метою виявлення фізичних та юридичних осіб, пов'язаних з ФР, та додавання їх до внутрішніх списків спостереження.
- Перегляд звітів групи експертів ООН щодо Північної Кореї та Ірану з метою виявлення нових типологій та тенденцій у сфері ФР.²³
- Проведення тренінгів з експортно-імпортного контролю для співробітників.
- Проведення тренінгів для працівників щодо товарів подвійного призначення.

Ефективність засобів контролю визначається двома аспектами: чи добре розроблений засіб контролю для зменшення притаманних ризиків і чи належним чином він використовується для зменшення цих ризиків. Поєднання ефективності розробки та операційної ефективності засобів контролю вказує на те, чи є контроль неефективним, частково ефективним, ефективним або високоефективним (див. Таблицю 3). Визначення того, чи засоби контролю ефективно розроблені та функціонують, повинно ґрунтуватися на тестуванні контролів.

²² For more on PF typologies, see Brewer, 'Study of Typologies of Financing of WMD Proliferation'; FATF, 'FATF Guidance on Counter Proliferation Financing'.

²³ Security Council Report, 'UN Documents for DPRK (North Korea): Sanctions Committee Documents', <https://www.securitycouncilreport.org/un_documents_type/sanctions-committee-documents/?ctype=DPRK%20%28North%20Korea%29&cbtype=dprk-north-korea>, accessed 18 May 2023; Security Council Report, 'UN Documents for Iran: Sanctions Committee Documents', <https://www.securitycouncilreport.org/un_documents_type/sanctions-committee-documents/?ctype=Iran&cbtype=iran>, accessed 5 January 2023.

Таблиця 3: Ефективність контролю

		Операційна ефективність			
		Неефективна	Частково ефективна	Ефективна	Високо ефективна
Ефективність розробки	Неефективна	Неефективний	Неефективний	Неефективний	Неефективний
	Частково ефективна	Неефективний	Неефективний	Частково ефективний	Ефективний
	Ефективна	Неефективний	Частково ефективний	Ефективний	Ефективний
	Високоєфективна	Неефективний	Ефективний	Ефективний	Високоєфективний

Джерело: Створено автором. Адаптовано з різних систем та посібників з управління ризиками на підприємстві. Фінансові установи можуть адаптувати цю таблицю до своїх внутрішніх процесів.

Наприклад, у наведеному вище прикладі, коли торгівля на відкритому рахунку була оцінена як така, що має середньо-високий притаманний ризик, ФУ має оцінити ефективність наявних засобів контролю для зменшення ризиків неправомірного використання відповідних продуктів у цілях ФР.

Заходи контролю та зниження ризиків, які зазвичай використовуються для зменшення ймовірності настання та впливу ризику ФР, пов'язаного з фінансуванням за допомогою відкритих рахунків, включають:

- Належна перевірка як клієнтів, так і інших відповідних сторін транзакцій для розуміння профілю клієнта (включаючи очікувану діяльність) та виявлення незвичної та потенційно підозрілої діяльності.
- Перевірка назв/імен, організацій, осіб, постачальників і країн за списками офіційних санкцій і заборонених осіб з метою виявлення санкцій або інших проблем, пов'язаних з відносинами або транзакціями.
- Моніторинг завершених або поточних транзакцій для виявлення наявності незвичної або потенційно підозрілої діяльності відповідно до відомих типологій ФР.²⁴

²⁴ Wolfsberg Group, ICC and BAFT, 'The Wolfsberg Group, ICC and BAFT Trade Finance Principles', p. 70.

Тематичне дослідження Chinpo Shipping

Наприкінці 1990-х років Північна Корея заснувала компанію Ocean Maritime Management (ОММ), яка надавала послуги з перевезення зброї, що відіграла центральну роль у ядерній програмі країни. До того, як у 2014 році Рада Безпеки ООН (РБ ООН) внесла ОММ до списку санкцій, вона створила глобальну мережу підставних компаній і посередників для обходу санкцій ООН. До неї входила "Chinpo Shipping", судноплавна компанія з оптового імпорту/експорту, заснована в 1970 році Тан Ченг Хое, що базується в Сінгапурі.

У 2014 році РБ ООН додала ОММ до списку спеціально визначених організацій за сприяння у перевезенні в липні 2013 року звичайних озброєнь з Куби до Північної Кореї. Поставка здійснювалася на судні "Chong Chon Gang", де під мішками з цукром були виявлені наступні предмети: два літаки МіГ-21 і двигуни до них; шість трейлерів із зенітними ракетами типу земля-повітря SA-2 і SA-3; боєприпаси, гвинтівки і прилади нічного бачення; і загалом 240 тонн військового спорядження.

Під час судового процесу в Сінгапурі над засновником "Chinpo" Тан Чен Хо, експерт-свідок обвинувачення вказав, що така військова техніка може бути використана для захисту ядерних об'єктів Північної Кореї. Крім того, суд підтвердив, що ОММ доручив Chinpo Shipping сплатити від свого імені збори за прохід судна через Панамський канал (\$54,270 і \$72,017 за вихідний і вхідний прохід). Щоб приховати попередню діяльність "Chong Chon Gang", ОММ також доручив компанії "Chinpo" внести неправдиву назву судна - "South Hill 2" - у документацію про банківські перекази.

У 2015 році Окружний суд Сінгапуру визнав Тан Чен Хо винним у двох злочинах: порушенні санкцій ООН і наданні фінансових послуг, які можуть бути обґрунтовано використані для сприяння програмі Північної Кореї з її ядерних та балістичних ракет. Під час судового процесу з'ясувалося, що Тан Чен Хо мав тісні зв'язки з Північною Кореєю: його офісне приміщення "Chinpo" було безкоштовно надано посольству Північної Кореї; він був контактною особою з питань працевлаштування північнокорейських робітників у сінгапурських компаніях; він виступав посередником у вирішенні конфлікту між північнокорейськими та сінгапурськими компаніями; також він був фінансовим агентом багатьох північнокорейських організацій, в тому числі й ОММ.

Банк Китаю, який надавав Чінпо банківські послуги, не зміг впровадити надійні перевірки KYC і CDD. Він не виявив ані тісних зв'язків "Chinpo" з північнокорейцями в Сінгапурі, ані її прямих зв'язків з Північною Кореєю. Зокрема, не було виявлено, що "Chinpo" ділилася своєю адресою з посольством Північної Кореї в Сінгапурі

Крім того, Окружний суд Сінгапуру встановив, що банк, можливо, не здійснював належного моніторингу транзакцій, що могло бути наслідком неякісних перевірок

КУС і CDD. Наприклад, у період з 2010 по 2013 рік кількість суден, що перевозили вантажі Chinpro, зменшилася з 57 до 4. Однак грошові перекази Chinpro за кордон у період з 2009 по 2013 рік склали понад 40 мільйонів доларів США. Такі операції не відповідають профілю такого судноплавного агента. Незрозуміло, чи постійний моніторинг транзакцій Банку Китаю висвітлював попередження про транзакції, і чи досліджували аналітики ці транзакції, щоб встановити, чи були вони легітимними.

Sources: James Martin Center for Nonproliferation Studies, 'Chinpro Shipping Case Study', November 2017, <<http://www.nonproliferation.org/wp-content/uploads/2017/12/op35-presentation-chinpro-shipping-case.pdf>>, accessed 10 May 2023; Colum Lynch, 'U.N. Panel: North Korea Used Chinese Bank to Evade Nuclear Sanctions', Foreign Policy, 7 March 2016.

Залишкові ризики: Поєднання оцінок притаманного ризику та ефективності контролю:

Якщо всі три заходи контролю оцінюються як ефективні, то накладання цієї оцінки на середньо-високий рівень притаманного ризику призведе до оцінки залишкового ризику на рівні середньо-низький (див. Таблицю 4). Важливо відзначити, що такі системи повинні бути гнучкими, а також те, що досвід і знання команди протидії фінансовим злочинам повинні підсилювати такі оцінки. Команди ПФЗ повинні застосовувати ризик-орієнтований підхід. Наприклад, у випадку, коли заходи контролю оцінюються як ефективні, група з ПФЗ може визначити, що залишковий ризик має бути середньо-високим через елементи, які не були якісно або кількісно враховані під час оцінки. Таким чином, "технічні оцінки, виконані аналітиками ризиків, можуть бути змінені, що дозволяє аналітикам використовувати евристичні методи, часто під впливом "інтуїції", або чутливості до певної теми або етики, при оцінці певних ризиків, пов'язаних з конкретною подією".²⁵ Такі фактори повинні бути чітко задокументовані та сформульовані, а також розглянуті та оцінені за допомогою належних механізмів управління (наприклад, комітетів з питань ризиків та аудиту) для обґрунтування рішень.

²⁵ Noémi També Bearpark, *Deconstructing Money Laundering Risk: De-Risking, the Risk-Based Approach and Risk Communication* (New York, NY: Springer, 2022), p. 23.

Таблиця 4: Залишковий ризик

		Притаманний ризик				
		Низький	Середньо-низький	Середньо-Високий	Високий	Екстремальний
		Залишковий ризик				
Ефективність контролю	Не ефективний	Низький	Середньо-низький	Середньо-високий	Високий	Екстремальний
	Частково ефективний	Низький	Середньо-низький	Середньо-високий	Високий	Екстремальний
	Ефективний	Незначний	Низький	Середньо-низький	Середньо-високий	Високий
	Високо-ефективний	Незначний	Незначний	Низький	Середньо-низький	Середньо-високий

Джерело: Створено автором. Адаптовано з різних систем та посібників з управління ризиками на підприємстві. Фінансові установи можуть адаптувати цю таблицю до своїх внутрішніх процесів.

Вразливість до ризику ФР та наступні кроки

Після того, як установи завершили свою ОР ФР, вони можуть виміряти свій залишковий ризик, а отже, і свою вразливість до ризику ФР (наприклад, з точки зору потенційного недотримання нормативних вимог або надмірної схильності до ризиків). Згодом установи можуть вирішити, чи приймати, надалі зменшувати або запобігати таким вразливим місцям та схильностям до ризику ФР.

Установи можуть захотіти посилити та вдосконалити існуючі засоби контролю для подолання виявлених притаманних ризиків, що мають найвищий рейтинг ("екстремальний" в Таблиці 2), а також змінити інші засоби контролю, які вважаються неефективними або частково неефективними. Діючи на основі ризик-орієнтованого підходу, установи повинні зосередити увагу на виявлених притаманних ризиках, що мають найвищий рейтинг. У цьому дусі установи можуть також вирішити переглянути певні заходи контролю, які можуть розглядатися як непропорційні з точки зору зниження притаманних ризиків, що мають нижчий рейтинг.

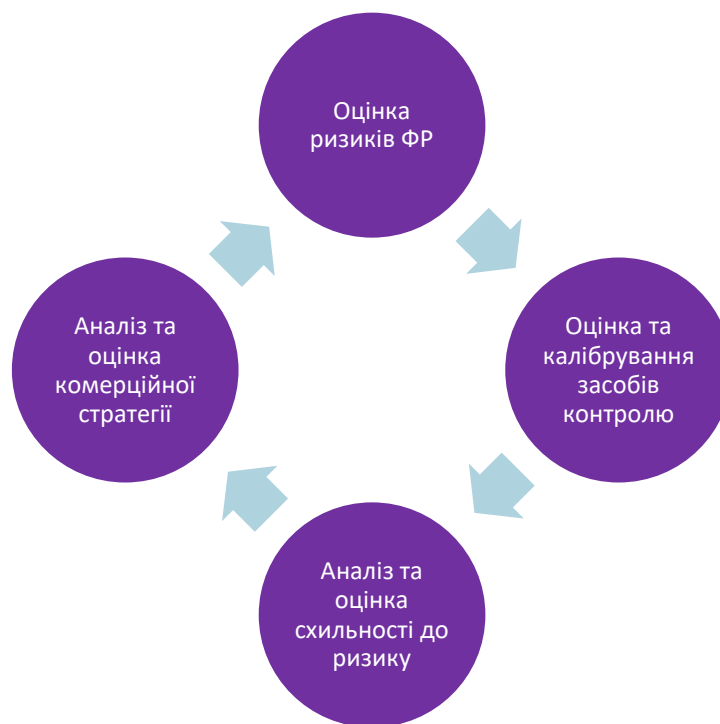
Крім того, ОР ФР допоможе установам краще зрозуміти та визначити свій апетит до ризику, водночас відповідаючи законам та нормативно-правовим актам з протидії фінансування розповсюдження. Таким чином, установи можуть вирішити переглянути та оцінити свої існуючі комерційні стратегії.

Це може призвести до того, що установа:

- Припинить здійснення певних видів діяльності в певних юрисдикціях.
- Припинить певні ділові відносини.
- Запуск нових комерційних підприємств.
- Розробка механізмів управління та контролю для посилення відповідності схильності до ризику

ОР має бути динамічним процесом, і описані вище підходи можуть бути використані в новій ОР ФР, щоб забезпечити виявлення існуючих та/або майбутніх вразливостей до ФР. Це проілюстровано на Рисунку 2 нижче

Рисунок 2: Цикл ОР



Джерело: Створено автором. Адаптовано з різних систем та посібників з оцінки ризиків.

Розуміння притаманних та залишкових ризиків ФР на практиці

Кейс Corman Construction and Commerce (CC&C) ілюструє притаманні ризики ФР клієнтів банків, які демонструють підвищені фактори ризику ФР. У доповіді групи експертів ООН за березень 2021 року зазначено, що CC&C є підставною компанією для групи компаній Mansudae Overseas Project, на яку ООН наклала санкції у 2017 році. Компанія була зареєстрована як сенегальська компанія з Чхве Сонг Чолом, відомим громадянином Північної Кореї, який у документах про правовий статус компанії вказаний як контролююча особа. У доповіді групи експертів ООН зазначається, що контракти та фінансові операції свідчать про те, що CC&C керувала кількома проектами в Дакарі (Сенегал).

Крім того, вона мала рахунки у двох різних фінансових установах і регулярно здійснювала платежі на користь посольства Північної Кореї. CC&C і фінансові установи, які надавали CC&C банківські послуги, порушували санкції ООН, підтримуючи програми створення зброї масового знищення: перші - через діяльність зі збору доходів, а другі - через надання фінансових послуг та інфраструктури (див. рис. 1).

Крім того, у вересні 2019 року журналістське розслідування виявило, що в компанії працював щонайменше 31 громадянин Північної Кореї. Це було потенційним порушенням санкцій ООН, які забороняють країнам-членам ООН допускати нових північнокорейських працівників до своєї юрисдикції, а також вимагають, щоб усі наявні північнокорейські працівники були вислані з території країн-членів ООН до кінця 2019 року.

На основі даних групи експертів ООН неможливо встановити, чи свідомо фінансові установи, які надавали фінансові послуги компанії СС&С, порушували санкції ООН. Однак, наступні факти могли б свідчити про те, що СС&С має підвищені фактори ризику ФР:

- Географічний ризик:
 - Компанія працює в Сенегалі, юрисдикції, яка була визнана такою, що не відповідає Рекомендації 6 під час процесу взаємного оцінювання FATF у 2018 році.
 - Сенегал має історичні зв'язки з Північною Кореєю, дипломатичні відносини з якою існують з 1972 року. Крім того, північнокорейська компанія Mansudae Overseas Projects побудувала пам'ятник африканському відродженню в Дакарі.
- Клієнтський ризик:
 - Компанія контролюється громадянином Північної Кореї.
 - Юридична особа працює в будівельній галузі - секторі, який становить підвищений ризик ФР, оскільки може бути використаний для отримання доходів через експлуатацію праці та прибуток від оплати контрактів, що є частиною діяльності Північної Кореї зі збору доходів.
- Транзакційний ризик:
 - Компанія надсилає виручку до посольства Північної Кореї.

Після виявлення цих притаманних ризиків можна було б очікувати, що будуть застосовані наступні заходи контролю:

- Програма навчання співробітників для забезпечення належного рівня обізнаності про CPF у ФУ.
- Система CDD та KYC для встановлення кінцевого бенефіціарного власника та/або інших контролюючих осіб.
- Система CDD та KYC для виявлення того, що СС&С є підставною компанією для юридичної особи, на яку поширюються санкції.
- Система CDD та KYC для виявлення та оцінки географічного розповсюдження діяльності СС&С's та встановлення мети та характеру рахунку, включаючи очікувану діяльність.
- Перевірка санкцій та несприятливих даних зі ЗМІ для встановлення відповідності санкційним спискам.
- Моніторинг транзакцій для виявлення незаконних транзакцій, таких як ті, що

здійснюються на користь посольства Північної Кореї.

Належне впровадження цих засобів контролю показало б, що:

- Надання фінансових послуг та/або продуктів клієнтам СС&С є явним порушенням санкцій ООН.
- Тому залишкові ризики ФР, пов'язані з наданням банківських послуг такому клієнту, є серйозними.
- Щоб запобігти серйозним ризикам ФР не слід обслуговувати такого клієнта.

Sources: UN Security Council (UNSC), 'Security Council 1718 Sanctions Committee Amends 44 Entries on its Sanctions List', SC/14983, press release, 26 July 2022, <<https://press.un.org/en/2022/sc14983.doc.htm>>, accessed 10 May 2023; UNSC, 'UN Panel of Experts Report', S/2021/211, 4 March 2021, pp. 51, 53, 322, <https://www.securitycouncilreport.org/atf/cf/%7B65BF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/s_2021_211.pdf>, accessed 13 December 2022; Council of the European Union, 'Council Directive 2011/64/EU of 11 August 2017', Official Journal of the European Union (C 2016/849, 11 August 2017), <[https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52017XC0811\(11\)](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52017XC0811(11))>, accessed 13 December 2022; Ham Ji-ha and Kim Seonmyung, 'Despite UN Sanctions, North Koreans at Work in Senegal', VOA, 24 September 2019, <https://www.voanews.com/a/africa_despite-un-sanctions-north-koreans-work-senegal/6176412.html>, accessed 10 May 2023; Inter-Governmental Action Group against Money Laundering in West Africa, 'Anti-Money Laundering and Counter-Terrorist Financing Measures: Senegal: Second Round Mutual Evaluation Report', May 2018, <<https://www.fatf-gafi.org/en/publications/Mutualevaluations/Mer-senegal-2018.html>>, accessed 10 May 2023.

III. Категорії ризиків та фактори ризиків

Ґрунтуючись на більш повному розумінні методології ОР, у Таблиці 5 наведено п'ять категорій ризиків ФР, чиї притаманні ризики необхідно враховувати: клієнти; географічне розташування; продукти, послуги та транзакції; канали доставки та кіберзлочинність.

Можуть існувати й інші категорії ризиків, які установа може додати, щоб забезпечити належне охоплення усіх ризиків, з якими вона стикається. Наприклад, шахрайство може бути визначене як метод збільшення доходів, що використовується Північною Кореєю або Іраном у певній юрисдикції.

Потім фінансові установи повинні розглянути кожен ризик у порівнянні з "факторами ризику" (наведеними у другій колонці Таблиці 5), що відповідають їхній господарській діяльності. Значущість конкретних факторів ризику буде різною для різних установ. Наприклад, невелика страхова компанія не матиме таких самих ризиків, як міжнародна фінансова установа або постачальник послуг з віртуальних активів. Фактори ризику варіюватимуться залежно від типу ринків, які обслуговує установа, її клієнтів, продуктів, які вона пропонує, каналів доставки та платформ, що використовуються. Зверніть увагу, що Таблиця 5 не містить вичерпного переліку факторів ризику. У третій колонці Таблиці 5 фактори ризику співвіднесені з відповідними категоріями діяльності ФР, проілюстрованими на Рисунку 1 цього посібника.

У Таблиці 6 наведено критерії, які слід враховувати при оцінці ризиків ФР на які можуть наражатися юрисдикції.

**Посібник з оцінки ризиків фінансування
розповсюдження зброї масового знищення
Ноемі Тамбе**

Таблиця 5: Категорії ризику ФР та фактори ризику

Категорії ризику	Фактори ризику	Потенційні дії з фінансування розповсюдження зброї масового знищення
Ризик клієнта (включаючи тип юридичної особи)	<ul style="list-style-type: none"> • Резидентство та громадянство • Складна структура власності з декількома юрисдикціями та типами суб'єктів господарювання • Використання міжнародних корпоративних структур • Провайдери віртуальних валют або клієнти, які інвестують через таких провайдерів • Компанії з номінальними акціонерами 	<ul style="list-style-type: none"> • Використання вразливості країни до ФР внаслідок історичної спадщини, недосконалої нормативно-правової бази, соціально-політичних, економічних та технологічних чинників. • Юрисдикції, що надають рахунки або іншим чином сприяють фінансовій діяльності держав, що здійснюють розповсюдження. • Використання місцевих філій банків та фінансових установ, розташованих у країнах, що викликають занепокоєння з точки зору розповсюдження. • Використання складних структур (таких як багаторівневі трасти, фонди), номінальних директорів та/або акціонерів для приховування кінцевого бенефіціарного власника або істотного контролера та їхнього зв'язку з особами або юрисдикціями, що підпадають під санкції. • Використання криптовалют для уникнення офіційної фінансової системи. • Створення корпоративних мереж, які сприяють, але не можуть бути виключно задіяні в діяльності ФР. Непрозорість кінцевої бенефіціарної власності, зв'язків та структур контролю. • Використання підставних компаній, фіктивних компаній або брокерів для отримання продуктів і послуг торгового фінансування або як учасників "чистих" платежів. • Детальніше про критерії, які слід враховувати при оцінці вразливості юрисдикції, див. Таблицю 6
Діяльність / професія / галузь клієнта	<ul style="list-style-type: none"> • Бізнес з надання грошових послуг • Переробна промисловість • Сільське господарство • Наукові дослідження • Постачальники, покупці та торгові партнери у сфері технологій ЗМЗ/товарів подвійного призначення/ ядерної/ оборонної промисловості • Морська/ судноплавна 	<ul style="list-style-type: none"> • Використання університетів або дослідницьких центрів для закупівлі товарів подвійного призначення та/або для виплати коштів, включаючи іранські та сирійські установи. • Використання судноплавних компаній, брокерів та агентів для отримання страхових або інших фінансових послуг, пов'язаних з морськими перевезеннями. Часто поєднується з використанням підставних компаній з непрозорою структурою власності. • Обмінні пункти, що використовуються для грошових переказів на підтримку мереж розповсюдження, коли в переказах беруть участь фізичні або юридичні особи, які перебувають у власності або під контролем суб'єктів, що займаються розповсюдженням. Можуть також включати структуровані платежі організованим злочинним мережам, що займаються діяльністю, спрямованою на отримання прибутку. • Використання дипломатів, консульських працівників або дипломатичних чи консульських представництв Північної Кореї для створення мереж, у тому числі корпоративних, у країні. Ці мережі потім сприяють низці видів діяльності зі збору доходів²⁶, а також

²⁶ This guide does not offer a comprehensive list of activities that North Korean and Iranian nationals and entities have been reported to – or could theoretically – engage in to raise funds. There are several well-established or emerging patterns of fundraising activities,

Категорії ризику	Фактори ризику	Потенційні дії з фінансування розповсюдження зброї масового знищення
	<ul style="list-style-type: none"> • промисловість • Постачальники тіншових банківських послуг • Підприємства, що займаються обміном валют • Посольства та консульства • Політично значущі особи (PEPs) • Провайдери корпоративних послуг та посередники 	<p>просуванню фінансових продуктів або послуг, пов'язаних з торгівлею товарами.</p> <ul style="list-style-type: none"> • Використання політично значущих осіб, які є вразливими до корупції та можуть використовувати своє службове становище для отримання доступу до земельних прав, прав на видобуток корисних копалин або експлуатації бізнесу (наприклад, рибальства) з метою отримання доходів для країн та суб'єктів, що перебувають під санкціями. • Використання професійних посередників та корпоративних постачальників послуг для маскуванню учасників транзакцій та кінцевих користувачів, пов'язаних з ФР.
Географічний ризик	<ul style="list-style-type: none"> • Юрисдикції, відомі тим, що можуть порушувати міжнародні норми • Юрисдикції з високим рівнем ризику та треті країни з високим рівнем ризику • Країни, на які поширюються санкції або ембарго; країни, в яких відсутні належні закони та нормативно-правові акти у сфері ПВК/ФТ • Офшорні фінансові центри та податкові юрисдикції, що не співпрацюють • Юрисдикції, в яких спостерігається значний рівень корупції, організованої злочинності або іншої злочинної діяльності • Юрисдикції, в яких виявлено фінансування або підтримку терористичної діяльності 	<ul style="list-style-type: none"> • Використання місцевих філій банків та фінансових установ, розташованих у країнах, що викликають занепокоєння з точки зору розповсюдження. • Використання третіх країн зі слабкою системою ПВК або підвищеним ризиком корупції та хабарництва для проведення фінансових операцій, пов'язаних з товарами подвійного використання. • Використання офшорних юрисдикцій, які дозволяють легко створювати підставні та/або фіктивні компанії для маскуванню кінцевих бенефіціарів та/або кінцевих користувачів, пов'язаних з програмами створення зброї масового знищення. • Використання торговельних або інших економічних відносин з країнами, що мають зв'язки або значний вплив на країну, що розповсюджує зброю масового знищення. Часто цьому сприяє складна корпоративна мережа.

such as cybercrime and abuse of cryptocurrencies, provision of military assistance, construction of statues and monuments, illegal wildlife trade, and overseas labour across different types of industries. Revenue-raising activities will differ across jurisdictions, as they depend on jurisdictions' specific vulnerabilities. See Dolzikova and Joshi, 'The Southern Stratagem'.

Категорії ризику	Фактори ризику	Потенційні дії з фінансування розповсюдження зброї масового знищення
Ризик продуктів, послуг та операцій	<ul style="list-style-type: none"> • Платежі за відкритими рахунками/ акредитивами • Міжнародні платежі • Тіньовий банкінг • Кореспондентські банківські відносини • Іноземні рахунки • Надання послуг з дорогоцінними металами та камінням • Надання продуктів морського страхування • Надання послуг з торгівлі віртуальними активами 	<ul style="list-style-type: none"> • Використання продуктів і послуг торговельного фінансування та послуг "чистих" платежів при закупівлі товарів, чутливих з точки зору розповсюдження. • Використання фальшивих або шахрайських документів, пов'язаних з доставкою, митницею або платежами, для спрощення транзакцій або торгового фінансування. • Використання міжнародних електронних платежів з обмеженим наглядом за дотриманням вимог CDD щодо платників та одержувачів платежів. • Використання тіньової банківської діяльності, що характеризується обмеженим розкриттям вартості та характеру активів. • Використання кореспондентських відносин для переказу коштів через міжнародну фінансову систему розповсюджувачам та від розповсюджувачів для оплати товарів подвійного призначення або для переказу доходів від діяльності, пов'язаної з отриманням прибутку. • Використання рахунків в іноземній валюті для здійснення міжнародних платежів за товари подвійного призначення або для переказу доходів від діяльності, пов'язаної з отриманням доходів. • Купівля або продаж дорогоцінних металів та/або каміння для переміщення вартості між юрисдикціями або для отримання доходів, спрямованих на підтримку програм створення зброї масового знищення. • Надання морського страхування судноплавним компаніям, причетним до порушення санкцій. • Використання криптовалют для забезпечення анонімності та уникнення офіційної фінансової системи і пов'язаного з нею контролю, за допомогою якого легше виявити порушення санкцій.
Ризик каналу доставки	<ul style="list-style-type: none"> • Очне походження • Заочне походження 	<ul style="list-style-type: none"> • Використання засобів заочного відкриття рахунків для маскуванню особи кінцевого бенефіціарного власника. • Послуги, які можуть приховати бенефіціарну власність від компетентних органів (наприклад, ризик номінального директора)
Ризик кіберзлочинності	<ul style="list-style-type: none"> • Хакерство • Програми-вимагачі • ІТ-підрядники з доступом до конфіденційних матеріалів 	<ul style="list-style-type: none"> • Зламування рахунків з метою отримання цінності, що здебільшого використовується державними суб'єктами. • Використання систем зі шкідливим програмним забезпеченням, яке заморожує або шифрує пристрої, що розблоковуються після сплати викупу. • Використання кримінальних ІТ-співробітників, інфільтрованих в організації, що займаються підготовкою або розробкою тематики, потенційно пов'язаної зі зброєю масового знищення або товарами подвійного призначення.

Source: Author generated. The 'Potential Acts of Proliferation Finance' column is based on Joshi, Dall and Dolzikova, 'Guide to Conducting a National Proliferation Financing Risk Assessment'; see also Brewer, 'Study of Typologies of Financing of WMD Proliferation'.

Таблиця 6: Оцінка ризиків країни

Скоринг	Опис
Санкційний	<ul style="list-style-type: none"> • Країна перебуває під санкціями ООН (Північна Корея та Іран). • Країна перебуває під іншими санкціями (наприклад, Китай, Сирія, Росія та Пакистан). • Країна має значну корпоративну/торговельну мережу ФР з країною/країнами, що перебувають під санкціями. • Країна пропонує торгівельні судна під зручним прапором або зі зручним паспортом. • Країна входить до "списку країн високого ризику" FATF та/або "сірого списку" FATF. • Розвіддани свідчать про те, що країна може розглядати можливість розвитку ядерного потенціалу шляхом незаконних закупівель.
Середньо-високий	<ul style="list-style-type: none"> • Країна, відома порушеннями міжнародних норм, країна з низьким рівнем ефективності у звітах про взаємну оцінку, в тому числі за Безпосереднім Результатом 11.²⁷ • Географічна близькість до країни, що займається розповсюдженням. • Країна, названа групою експертів ООН/Офісом з контролю за іноземними активами/основними ЗМІ як така, що або торгує з державами, до яких застосовано санкції, або не має достатньої видимості/прозорості щодо торговельних схем. • Країна не відповідає на запити групи експертів ООН. • Країна не є учасницею Договору про нерозповсюдження ядерної зброї та/або зберігає чи вдосконалює, або, як очікується, зберігатиме чи вдосконалюватиме свій ядерний потенціал. • Держава, що розповсюджує ЗМЗ, має дипломатичну присутність в країні.
Середньо-низький	<ul style="list-style-type: none"> • Країна межує з державою, що займається розповсюдженням зброї масового знищення. • Країна має велику діаспору з держави, що викликає занепокоєння з точки зору розповсюдження. • У країні розташований фінансовий, торговий центр або перевалочний вузол, привабливий для тих, хто фінансує розповсюдження зброї масового знищення. • Юрисдикція є домом для виробничого сектору, який виробляє товари, що контролюються міжнародними режимами поставок, пов'язаними зі зброєю масового знищення та/або засобами її доставки. • Юрисдикція має слабкі механізми контролю та/або правозастосування у сфері ВК, ФТ та ФР.
Низький	<ul style="list-style-type: none"> • Країна має сильні механізми регулювання та правозастосування, які визнані ФАТФ, та/або не оцінюються в жодному зі звітів за категоріями ризику, та/або країна не включена до списків ФАТФ. • Країна має надійну систему реєстрації компаній. • Країна провела національну оцінку ризиків (НОР) щодо ВК/ФТ/ФР (зверніть увагу, що це є вимогою ФАТФ і може бути індикатором низького ризику), а також визначила та впровадила пом'якшувальні засоби контролю для вирішення питань високого ризику, порушених у НОР.

Source: Author generated, drawing on Jonathan Brewer, 'The Financing of WMD Proliferation: Conducting Risk Assessments', Center for New American Security, 30 October 2018.

Тематичне дослідження: Congo Aconde SARL

У 2018 році двоє північнокорейських бізнесменів, Пак Хва Сонг і Хван Кіл Су, заснували компанію Congo Aconde SARL, яка надає будівельні послуги в

²⁷'Immediate outcomes' assess to what extent a country meets the objectives of FATF standards. Immediate Outcome 11 requires preventing persons and entities involved in WMD proliferation from raising, moving and using funds. For more information, see FATF, 'Methodology for Assessing Technical Compliance with the FATF Recommendations and the Effectiveness of AML/CFT Systems', updated October 2021, <<https://www.fatf-gafi.org/en/publications/Mutualevaluations/Fatf-methodology.html>>, accessed 10 May 2023.

Демократичній Республіці Конго (ДРК). Вони відкрили корпоративний банківський рахунок в іноземній валюті в Afriland First Bank. Організація The Sentry, що займається розслідуваннями та розробкою політик, виявила "паризьку філію BMCE Bank International зі штаб-квартирою в Лондоні як банк-кореспондент, призначений для обробки транзакцій в доларах США та євро для рахунку Congo Aconde в Afriland First Bank".

Компанія реалізовувала будівельні проекти в ДРК. Один із проектів передбачав встановлення статуй, що є забороненою ООН діяльністю для Північної Кореї, спрямованою на отримання прибутку. Відповідно до Резолюції РБ ООН 2321 (2016), держави-члени не можуть прямо чи опосередковано купувати статуї у північнокорейських фізичних та юридичних осіб. Крім того, громадянам Північної Кореї заборонено постачати, продавати або передавати статуї.

У Доповіді групи експертів ООН щодо Північної Кореї за 2021 рік задокументовано, що Пак Хва Сонг і Хван Кіл Су надали північнокорейські паспорти під час процесу реєстрації компанії. Крім того, в їхніх паспортах було зазначено, що вони є співробітниками Міністерства закордонних справ, які виконують офіційні державні доручення. Крім того, їхні національності були записані як "КНДР" або "корейці". Нарешті, в установчих документах "Конго Аконде" була вказана адреса проживання.

У відповідь на запит групи експертів щодо фінансової діяльності Congo Aconde SARL:

одна фінансова установа описала свої процедури належної перевірки, які включають перехресні посилання на імена та номери паспортів у списках визначених суб'єктів ООН. Фінансова установа пояснила, що пани Пак Хва Сонг і Хван Кіл Су не є визначеними суб'єктами. Вони також надали групі експертів документальне підтвердження того, що обидва чоловіки підписали заяву про те, що їхні рахунки не будуть використані для забороненої діяльності, поміж іншого, ухилення від санкцій.

Заходи контролю, які, як очікувалося, мали бути застосовані як Afriland First Bank, так і BMCE Bank International, є наступними::

- Програма навчання співробітників для забезпечення належної обізнаності про CPF у фінансовій установі.
- Надійна система CDD та KYC для встановлення того, що Пак та Хван є громадянами Північної Кореї.
- Система CDD та KYC для визначення того, що Congo Aconde SARL контролюється громадянами Північної Кореї, а отже, становить підвищений ризик бути підставною компанією для юридичної особи, що перебуває під санкціями.
- Перевірка санкцій та негативної інформації у ЗМІ на наявність збігів із санкційними списками.
- При наданні кореспондентських банківських послуг - посилена належна перевірка операцій установ, що працюють у певних юрисдикціях.
- При наданні кореспондентських банківських послуг - аналіз та оцінка системи ПБК/ФТ/ФР банків-респондентів.

Джерела: The Sentry, "Негласні справи: як північнокорейські бізнесмени порушили санкції в Демократичній Республіці Конго", серпень 2020 р. <<https://thesentry.org/wp-content/uploads/2020/08/OvertAffairs-TheSentry-August2020.pdf>>, accessed 27 March 2023; UNSC, 'Resolution 2321 (2016)/ Adopted by the Security Council at its 7821st Meeting, on 30 November 2016', S/RES/2321, 30 November 2016; UNSC, 'UN Panel of Experts Report, S/2021/211', March 2021, p. 54, fn 129

Висновок

Цей посібник має на меті надати приватному сектору необхідну методологічну базу та інструменти для розробки і проведення інституційних ОР ФР. З цією метою в посібнику пропонуються підходи до проведення ОР ФР, визначення ризиків ФР та факторів ризику для оцінки вразливості установи до ФР, а також визначення заходів контролю та стратегій, спрямованих на пом'якшення ризиків.

Хоча цей посібник є корисною відправною точкою для проведення інституційних ОР, установи в кінцевому підсумку несуть відповідальність за аналіз та застосування цих настанов таким чином, щоб отримати обґрунтоване судження про свої інституційні ризики. За умови ретельного проведення, інституційна ОР, а також інформація, зібрана в ході цього процесу, має стати першим важливим кроком у кращому розумінні вразливості до ФР, проактивному усуненні прогалин у системі СРФ фінансових установ та пом'якшенні впливу діяльності з ФР на приватний сектор, а також на національну економіку та суспільство загалом.

Про автора

Ноемі Тамбе є асоційованим науковим співробітником Центру досліджень фінансових злочинів та безпеки при Королівському інституті об'єднаних служб (RUSI). Вона також є незалежним консультантом і дослідником з питань фінансових злочинів з більш ніж 20-річним професійним досвідом роботи в академічному, державному та приватному секторах, зокрема, у сфері приватного банкінгу. Вона є доцентом Люксембурзької школи бізнесу.