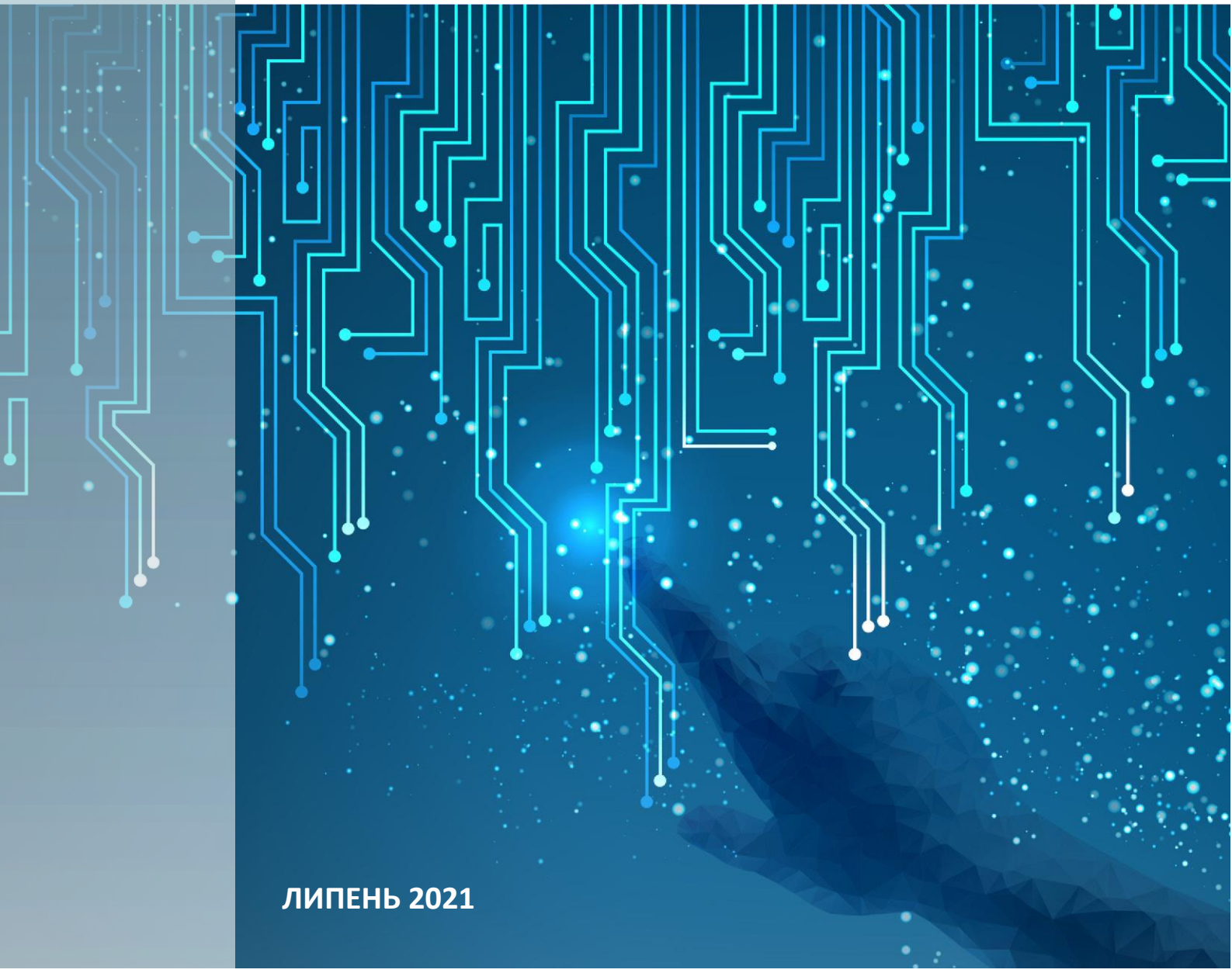
Неофіційний переклад

МОЖЛИВОСТІ ТА ВИКЛИКИ НОВИХ ТЕХНОЛОГІЙ ДЛЯ ПВК/ФТ



ЛИПЕНЬ 2021

Група з розробки фінансових заходів боротьби з відмиванням грошей (ФАТФ), є незалежним міжурядовим органом, який розробляє і проводить політику захисту глобальної фінансової системи від відмивання грошей, фінансування тероризму та фінансування розповсюдження зброї масового знищення. Рекомендації ФАТФ визнані в якості глобального стандарту у сфері протидії відмиванню коштів (ПВК) і фінансуванню тероризму (ФТ).

Якщо хочете дізнатися більше про ФАТФ, відвідайте www.fatf-gafi.org

Цей документ і/або будь-яка включена в нього карта не завдають шкоди статусу або суверенітету будь-якій території, делімітації міжнародних кордонів і назві будь-якої території, міста або району.

З посиланням на:

ФАТФ (2021), *Можливості та виклики нових технологій для ПВК/ФТ,* Париж, Франція, https://www.fatf-gafi.org/publications/fatfrecommendations/documents/opportunities-challenges-newtechnologies-aml-cft.html

Фото обкладинки: Gettyimages

Подяка

ФАТФ висловлює подяку зацікавленим сторонам державного та приватного секторів - включно з розробниками технологій, фінансовими установами та іншими експертами - за надання цінних даних, тематичних досліджень та відгуків щодо цього звіту.

Роботою цього звіту керував Секретаріат ФАТФ (Inês Oliveira), значний внесок зроблений Групою експертів із таких делегацій ФАТФ: Канада, Данія, Європейська Комісія, Єгипет, Німеччина, Ізраїль, Італія, Японія, Малайзія, Російська Федерація, Сінгапур, Великобританія, США, а також Європол та Секретаріат Євразійської групи (ЄАГ) з питань боротьби з відмиванням грошей та фінансуванням тероризму.

Зміст

Абревіатури і скорочення **3**

Короткий огляд змісту **4**

1. Вступ **6**

1.1. Орієнтація ФАТФ на відповідальні інновації та цифрові трансформації 8
1.2. Сфера застосування та методологія 9

2. Нові технології для ПВК/ФТ:на шляху до більш ефективного впровадження стандартів ФАТФ **12**

2.1. Впровадження ризик-орієнтованого підходу 14
2.2. Фінансове включення 16

3. Можливості нових технологій в ПВК/ФТ **22**

3.1. Штучний інтеклект (ШІ) 25
3.2. Обробка природних мов та гнучкі обчислювальні методи 26
3.3. Технологія розподіленого реєстру (блокчейн) 30
3.4. Програмне забезпечення для комплексної перевірки клієнтів 31
3.5. Інтерфейси прикладного програмування (ІПП) 37

4. Проблеми впровадження нових технологій для протидії відмиванню коштів та фінансуванню тероризму (ПВК/ФТ) **41**

4.1. Проблеми та виклики у сфері регулювання 41
4.2. Оперативні проблеми 46
4.3. Непередбачувані наслідки та можливість зловживань 48
4.4. Оцінка ефективності ПВК/ФТ технологічних рішенньь та способів усунення залишкових ризиків 51

5. Створення сприятливого середовища для використання нових технологій у ПВК/ФТ **52**

5.1. Технологічно активні наглядові органи 54
5.2. Заключні зауваження 60

Додатки **61**

Додаток A - Словник **62**

Додаток B - Пропоновані заходи щодо підтримки використання технологій у сфері ПВК/ФТ **67**

Додаток C - Тематичні дослідження SupTech **69**

Додаток D - Додаткові тематичні дослідження RegTech щодо використання нових технологій у ПВК/ФТ **75**

Список літератури **78**

Абревіатури

AI (ШІ)	Штучний інтелект
AML/CFT (ПВК/ФТ)	Протидія відмиванню коштів/фінансуванню тероризму
API (ІПП)	Інтрефейс прикладного програмування
CDD	Належна перевірка клієнтів
DL	Глибинне навчання
DLT (ТРР)	Технологія розподіленого реєстру
DNFBP (ВНУП)	Визначена нефінансова установа та професія
FATF (ФАТФ)	Група з розробки фінансових заходів боротьби з відмиванням грошей
MER	Звіт про взаємну оцінку
ML/FT (ВК/ФТ)	Відмивання коштів/Фінансовий тероризм
MVTS	Послуга з переказу грошей або цінностей
NLP (ОПМ)	Обробка природної мови
NRA (НОР)	Національна оцінка ризику
PEP	Публічний діяч
PSCF (КФПС)	Консультативні форуми приватного сектора
SSB (ОС)	Орган стандартизації
VASP	Постачальник послуг віртуальних активів

Короткий огляд змісту

1. Нові технології мають потенціал швидше, дешевше та ефективніше протидіяти відмиванню коштів (ПВК) та фінансуванню тероризму (ФТ). Вони можуть вдосконалити впровадження стандартів ФАТФ для сприяння глобальним зусиллям у сфері протидії відмиванню коштів та фінансуванню тероризму, забезпеченню фінансового включення та уникненню ненавмисних наслідків, таких як фінансове виключення.

2. Як глобальний засновник стандартів ПВК/ФТ, ФАТФ рішуче прагне бути в курсі інноваційних технологій та бізнес-моделей у фінансовому секторі, а також гарантувати, що загальносвітові стандарти залишаються актуальними та можуть забезпечити "розумне" регулювання фінансового сектору, яке як усуває ризики, так і сприяє відповідальній інновації. Відповідно, ФАТФ розглянув можливості та виклики нових технологій для протидії відмиванню коштів та фінансуванню тероризму для підвищення обізнаності про відповідний прогрес у галузі інновацій та конкретних цифрових рішень. ФАТФ також розглянула постійні виклики та перешкоди для їх реалізації та способи їх пом'якшення. Цей проект включав огляд та аналіз регуляторної технології (RegTech) та наглядової технології (SupTech), які можуть покращити ефективність стандартів ФАТФ.

3. Інноваційні навички, методи та процеси, а також новітні способи використання усталених технологічних процесів можуть допомогти регуляторам, наглядовим та регульованим структурам подолати багато з визначених проблем з відмиванням коштів та фінансуванням тероризму. Технології можуть полегшити збір, обробку та аналіз даних, а також допомогти суб'єктам визначити та управляти ризиками відмивання грошей та фінансування тероризму (ВК/ФТ) ефективніше та ближче до реального часу. Прискорені платежі та операції, більш точні системи ідентифікації, моніторинг, ведення діловодства та обмін інформацією між компетентними органами та підконтрольними установами також створюють переваги.

4. Посилене використання цифрових рішень для ПВК/ФТ на основі штучного інтелекту (ШІ) та його різних підмножин (машинне навчання, обробка природних мов) може потенційно допомогти краще визначити ризики, реагувати на підозрілу діяльність та контролювати її. На рівні державного сектору вдосконалений моніторинг у реальному часі та обмін інформацією з колегами дозволяють забезпечити більш інформований нагляд за регульованими структурами і тим самим допомагають поліпшити нагляд. На рівні приватного сектору технології можуть покращити оцінку ризиків, інтеграційну практику, зв'язки з компетентними органами, наявність умов для проведення перевірки, підзвітність та загальне належне управління, заощаджуючи витрати.

5. Звіт визначає проблеми, пов'язані з розробкою, прийняттям та застосуванням цих інноваційних рішень або практик. Багато з цих викликів зумовлені значними оперативними та регуляторними обмеженнями, такими як застарілі системи дотримання норм протидії відмиванню коштів та фінансуванню тероризму, а також традиційні нормативні рамки та механізми нагляду.

6. Складність та витрати, пов’язані із заміною або оновленням застарілих систем, ускладнюють використання потенціалу інноваційних підходів до ПВК/ФТ як для промисловості, так і для органів державного управління. У промисловості аналіз витрат та вигод для впровадження нових технологій і надалі залишається перешкодою для більш широкого впровадження інноваційних рішень у сфері протидії відмиванню коштів та фінансуванню тероризму, що, зокрема, є результатом реальної або передбачуваної відсутності нормативних стимулів для продовження інновацій. Труднощі з пояснюваністю та можливістю інтерпретації цифрових рішень є ще одним ключовим викликом як для галузі, так і для регулюючих органів, що частково пов'язано з обмеженою наявністю відповідної експертизи та недостатньою обізнаністю щодо потенціалу інноваційних технологій серед фахівців у сфері протидії відмиванню коштів та фінансуванню тероризму як у галузі, так і в уряді. Посилення комунікації та співпраці між державним та приватним сектором, проінформованими завдяки інформації та аналізу, які представлені у цьому звіті, разом з акцентом на відповідальному впровадженні нових технологій та ефективності, зокрема щодо норм захисту даних, будуть ключовими для подолання цих викликів та повної реалізації перспективного потенціалу відповідальних інновацій щодо посилення ефективності заходів протидії відмиванню коштів та фінансуванню тероризму.

7. За умови відповідального та пропорційного застосування інноваційних технологій у сфері боротьби з відмиванням коштів та фінансуванням тероризму, можна виявити ризики та зосередити зусилля на дотриманні вимог існуючих та нових проблем, однак людський фактор та обробка інформації вручну залишаються дуже важливими. Наприклад, навіть у технологічно сприятливій системі регулювання слід покладатися на людський фактор та оцінювати будь-які залишкові ризики, які створюють нові технології, а також вводити відповідні заходи щодо пом'якшення їх наслідків. Поєднання ефективності та точності цифрових рішень зі знаннями та аналітичними навичками фахівців-експертів створює надійніші системи, що можуть ефективно відповідати вимогам протидії відмиванню коштів та фінансуванню тероризму і водночас повністю піддаватися перевірці та бути підзвітними.

8. Використання нових технологій та інновацій може допомогти державному та приватному секторам підвищити ефективність впровадження стандартів ФАТФ з урахуванням усіх ризиків. Розробка, впровадження та регулюючий нагляд за цими технологіями повинні відображати як загрози, так і потенційні можливості. Використання нових технологій та інновацій також має забезпечувати відповідність використання інноваційних інструментів міжнародним стандартам захисту даних, конфіденційності та кібербезпеки.

1. Вступ

9. Стандарти ФАТФ - це динамічний інструмент, який еволюціонує внаслідок зміни глобальних загроз, вразливостей та ризиків, пов'язаних з відмиванням грошей та фінансуванням тероризму (ВК/ФТ), а також внаслідок проблем, що виникають під час їх впровадження. Через тридцять років після їх початкового прийняття, належна перевірка клієнтів (CDD) та відповідні процедури значно підвищили прозорість операцій та ускладнили злочинцям, сторонам, що фінансують тероризм та сторонам, що фінансують розповсюдження зброї можливість зловживання фінансовими послугами. У той же час, попри той факт, що ідентифікація/перевірка та моніторинг клієнтів є ключовими елементами системи протидії відмиванню коштів та фінансуванню тероризму, вона продовжує створювати проблеми щодо впровадження та ефективності.

10. Зусилля CDD, що не спрямовані на ризик, можуть сприйматися як дорогі та неефективні, оскільки вони часто витрачаються і при цьому не сприяють створенню точних процесів оцінки ризику або безперешкодного доступу до фінансових послуг. Усвідомлюючи прискорення темпів інновацій, значний вплив цифрових трансформацій на фінансову систему та прагнення до більшої ефективності стандартів ФАТФ, ФАТФ започаткувала ініціативу з вивчення потенціалу нових технологій для пом'якшення загроз ВК/ФТ.

11. У даному звіті термін „нові технології для ПВК/ФТ"[1] означає:

    a. інноваційні навички, методи та процеси, які використовуються для досягнення цілей, що стосуються ефективного впровадження вимог ПВК/ФТ або

    b. інноваційні способи використання встановлених технологічних процесів з метою виконання зобов'язань з ПВК/ФТ.

12. Нові технології орієнтовані на покращення швидкості, якості чи ефективності та вартості деяких заходів ПВК/ФТ, а також на нормалізацію витрат на ширше впровадження системи ПВК/ФТ, порівняно з використанням традиційних методів та процесів. Найактуальнішими є технології багатопрофільного застосування, адже вони забезпечують нові цифрові способи збору, обробки та аналізу даних. Ці технології також дозволяють передавати дані та інформацію за допомогою різноманітних конкретних рішень. Цей потенціал можна використовувати різними способами, що дублюються, він спрямований на широкий спектр цілей ПВК/ФТ. Багато з названих можливостей та наслідків цих нових технологій досі в основному невідомі. Тим не менш, важливо розуміти їхні поточні можливості та потенційний вплив на ПВК/ФТ.

13. Наприклад, програмне забезпечення для цифрової ідентифікації особи уможливлює особисту ідентифікацію клієнтів та оновлення інформації. Воно також може покращити автентифікацію клієнтів для більш безпечного доступу до рахунку та посилити ідентифікацію та автентифікацію, коли прийняття на обслуговування та транзакції проводяться особисто, що

[1] У даному звіті терміни *«цифрові рішення», «цифрові інструменти», «інноваційні рішення або системи»* використовуються як взаємозамінні, і, якщо це доречно, для позначення нових технологій для ПВК/ФТ, як визначено в цьому параграфі.

сприяє фінансовому включенню та боротьбі з відмиванням грошей, шахрайством, фінансуванням тероризму та іншими видами незаконної фінансової діяльності.

14. Іншим прикладом є те, що обробка природної мови може сприяти більш точному, гнучкому та своєчасному аналізу інформації про клієнта, зменшити обсяг неточної або недостовірної інформації, а також забезпечити більш ефективну відповідність та пошук додаткових даних. Покращені та більш актуальні профілі клієнтів означають точнішу оцінку ризиків, покращення процесу прийняття рішень та зменшення випадків ненавмисного фінансового виключення.

15. Подібним чином, технологічні рішення, що базуються на технологіях штучного інтелекту (ШІ) та машинного навчання (МН) і застосовуються для великих обсягів даних, можуть посилити постійний контроль та зміцнити механізми звітності про підозрілі транзакції. Ці технологічні рішення можуть автоматично контролювати, обробляти та аналізувати підозрілі транзакції та іншу незаконну діяльність, розпізнаючи їх у ході звичайної діяльності в режимі реального часу, і водночас зменшуючи потребу у початковому беспосередньому перегляді даних людиною. Штучний інтелект та засоби машинного навчання також можуть більш точно та вичерпно оцінювати поточну належну перевірку клієнтів та їхніх ризиків, які можуть поповнюватися з урахуванням нових і виникаючих загроз у режимі реального часу. Однак технологічні рішення ШІ/МН значно різняться як за технологією, так і за використанням, і можуть представляти значні ризики, про які мова піде далі в цьому звіті.

16. Аналогічно, впровадження інноваційних рішень, таких як Інтерфейс прикладного програмування (ІПП) та Технологія розподіленого реєстру (ТРР), стандартизація даних та встановлених правил, які здатна зчитувати машина, можуть допомогти регульованим суб'єктам[2] ефективніше звітувати перед наглядачами та іншими компетентними органами. Технології також дозволяють отримувати попередження про останні зміни, звітувати про подальші дії та отримувати інші повідомлення від наглядових органів, правоохоронних органів або інших органів влади до регульованих суб'єктів та їх споживачів, а також для передачі інформації як серед регульованих структур, так і між ними та їхніми клієнтами. Застосування більш досконалої аналітики регулюючими структурами також дає змогу посилити експертизу та нагляд, в тому числі й шляхом потенційного надання більш точної та безпосередньої відповіді.

17. Впровадження нових технологій для нагляду за дотриманням правил ПВК/ФТ у деяких випадках перешкоджало питанню щодо можливості використання інноваційних технологій відповідно до Рекомендацій ФАТФ, а також відповідно до нормативно-правової бази ПВК/ФТ країн.

[2] Для цілей цього Звіту «регульовані суб'єкти» стосуються фінансових установ, постачальників послуг віртуальних активів (VASPs) та визначених нефінансових установ та професій (ВНУП), як визначено у Стандартах FATF.

1.1. Орієнтація ФАТФ на відповідальні інновації та цифрові трансформації

18. Як міжнародний орган, що встановлює стандарти (ОС), ФАТФ прагне йти в ногу з інноваційними технологіями та бізнес-моделями у фінансовому секторі та гарантувати, що глобальні стандарти ПВК/ФТ залишатимуться актуальними та ефективними в умовах прискорення цифрової трансформації. Це робиться для того, щоб вимоги ФАТФ забезпечили можливість "розумного" регулювання фінансового сектора, яке допомагає стимулювати відповідальні інновації з метою сприяння як інтеграційним цілям ПВК/ФТ, так і цілям фінансового включення.

19. ФАТФ офіційно підтримала відповідальну інновацію для ПВК / ФТ у публічній заяві, опублікованій в Буенос-Айресі 3 листопада 2017 р., в якій проголошувалося:

> "ФАТФ рішуче підтримує відповідальні фінансові інновації, що відповідають вимогам ПВК/ФТ, що містяться у Стандартах ФАТФ, і надалі вивчатиме можливості, які нові фінансові та регулятивні технології можуть продемонструвати у сфері поліпшення ефективного впровадження заходів ПВК/ФТ."

20. Публічна заява 2017 року базувалася на попередніх зусиллях ФАТФ спрямованих на підтримку відповідальних інновацій, і водночас розглядала потенційні ризики незаконного фінансування та проблеми регулювання та контролю ПВК/ФТ, які виникають в результаті застосування нових технологій. Ці зусилля включають видання численних практичних рекомендацій та кращих практик про передові методи, оновлення Рекомендацій щодо управління віртуальними активами (ФАТФ, 2019 [1]) та широку взаємодію з приватним сектором через державні та приватні семінари та Консультативні форуми приватного сектора ФАТФ (КФПС).[3]

21. Застосування відповідальних інновацій підтримується в інших міжнародних заявах, а саме в Резолюції Ради Безпеки ООН 2462 (2019) (ООН, 2019 [2]), яка закликає всі держави підвищити відстежуваність та прозорість фінансових операцій, в тому числі шляхом повного використання нових та таких, що розвиваються, фінансових та регуляторних технологій для посилення фінансового включення та сприяння ефективному впровадженню заходів ПВК/ФТ.

22. Незважаючи на широко визнані переваги, ефективне використання інноваційних технологій для ПВК/ФТ обмежене різноманітними факторами, що впливає на різних регульованих суб'єктів та наглядових органів.

23. Зробивши інновації одним із своїх головних пріоритетів, ФАТФ під головуванням Німеччини висунуло ініціативу цифрової трансформації, яка включає три проекти:

    - Дослідження, що лежить в основі цього звіту, де розглядаються можливості та проблеми нових технологій задля впровадження

[3] Багато позицій та відповідних документів FATF щодо FinTech та RegTech можна знайти на веб-сайті FATF FinTech & RegTech Initiative. Доступно за адресою: www.fatf-gafi.org/fintech-regtech/fatfonfintechregtech/.

більш ефективних та результативних заходів ПВК/ФТ приватним сектором та наглядовими органами;

- Вивчення можливостей та викликів для оперативних агентств, спрямованих на створення більш ефективних систем виявлення та розслідування ВК та ФТ та розуміння ризиків ВК/ФТ, а також
- Перевірка об'єднання та поповнення даних, спільної аналітики та захисту даних, яка має на меті допомогу приватному сектору вдосконалити використання ШІ та аналіз великих даних для ПВК/ФТ та підвищити ефективність дотримання нормативних вимог, забезпечуючи при цьому високий рівень захисту даних.

24. Президент ФАТФ виніс цей порядок денний на міжнародні форуми, наголосивши на його важливості для кращого впровадження стандартів ФАТФ та ефективності ПВК/ФТ. (ФАТФ, 2020[3])

25. Цей звіт має на меті:

- Збільшити обізнаність та визначити можливості для використання нових технологій та нових та існуючих технологічних рішень;
- Визначити умови, політику та практику, які допоможуть подальшому впровадженню нових технологій, що сприяють ефективності та результативності зусиль ПВК/ФТ у відповідності до підкріплених аналізом конкретних прикладів режимів правового регулювання;
- Дослідити наявність нормативних перешкод чи інших факторів, що перешкоджають успішному впровадженню нових технологій, та, де це доречно, запропонувати додаткові проекти ФАТФ для вивчення можливих засобів реагування у сфері політики; а також
- Забезпечити загальний ряд визначень, концептуальну базу та запропоновані дії для державних органів та зацікавлених сторін приватного сектору для сприяння відповідальному розвитку та використанню нових технологій для ПВК/ФТ.

1.2. Сфера застосування та методологія

26. У цьому звіті основна увага приділяється тому, як нові технології можуть допомогти юрисдикціям та регульованим суб'єктам ефективніше впроваджувати стандарти ПВК/ФТ. Зокрема, цифрові рішення, що дозволяють краще розуміти, оцінювати та зменшувати ризики, здійснювати як належну перевірку клієнтів та моніторинг, так і спілкування з наглядовими органами, можуть сприяти досягненню ефективності впровадження стандартів ПВК/ФТ.

27. Звіт стосується впровадження нових технологій, відомих як RegTech[4], таких як ШІ, машинне навчання, великі дані та передова когнітивна

[4] RegTech-це підмножина FinTech, яка зосереджена на технологіях, які можуть полегшити виконання нормативних вимог більш ефективно та результативно, ніж існуючі можливості, як зазначено у Заяві зворотного зв'язку FS16/4, Орган з

аналітика/алгоритми, орієнтовані на вимоги ідентифікації та верифікації клієнтів, а також на більш широкі зобов'язання щодо дотримання ПВК/ФТ. Проект також розглядає SupTech[5] або технології, що використовуються наглядовими органами, наприклад, інструменти оцінки ризику, засоби візуалізації даних або інші. (Coelho et al., 2019[4])

28. У дослідженні, представленому в цьому звіті, розглядаються питання того, де технології були впроваджені успішно, які передумови дали змогу ефективно їх використовувати, які переваги були досягнуті та якими є, якщо вони наявні, нові вимоги, зумовлені успішним використанням інноваційних рішень.

29. У звіті також розглядаються випадки, коли перспективні технології не були успішно впроваджені, та визначаються проблеми або перешкоди для їх ефективного використання. Він також досліджує, наскільки необхідні скоординовані глобальні дії, щоб дозволити ширше використовувати інноваційні технологічні рішення для підтримки цілей ПВК/ФТ. Сюди входить аналіз структурних проблем, наприклад, питання якості даних, зміна застарілих систем, обмеження витрат та відсутність нормативних стимулів.

30. У випадках, коли ці технології відкривають реальну вигоду та допомагають ефективно реагувати на загрози, ФАТФ аналізує випадки їх використання тими, хто вперше впроваджував нові технології, щоб дати можливість іншим регульованим суб'єктам та органам влади застосовувати їх найбільш ефективно.

31. Приклади інших технологій, придатних для кращого впровадження стандартів ФАТФ, не запропонованих для аналізу у цьому звіті, включають:

    - Інструменти управління даними та механізми поширення даних
    - Аналітичні інструменти, включаючи використання машинного навчання та аналізу великих даних ПФР

32. Цей звіт спирається на загальні теоретичні дослідження та відповіді на онлайн запитальник щодо цифрової трансформації[6], яку Секретаріат ФАТФ розповсюдив серед державних органів та експертів державного та приватного секторів. Секретаріат також провів консультації з ключовими зацікавленими сторонами для отримання додаткової інформації та думок експертів, в тому числі й під час Наради Високого Рівня за Круглим Столом щодо можливостей та викликів нових технологій для ПВК/ФТ, який було організовано ФАТФ онлайн 10 березня 2021 року.

фінансової поведінки, *Заклик до участі у підтримці розвитку та впровадження RegTech (2016).*
Доступно за адресою: www.fca.org.uk/publication/feedback/fs-16-04.pdf

[5] Наглядова технологія (suptech) - це використання інноваційних технологій наглядовими органами для підтримки нагляду. Див., (Broeders D. and Prenio J., 2018 [36])

[6] Запитальник був спрямований на отримання інформації щодо можливостей та проблем використання нових технологій у рамках даного проекту. В ньому зібрано 188 відповідей, до числа яких входять конкретні приклади справ та цифрових рішень.

33. Запитальник ФАТФ з цифрової трансформації мав не меті з'ясувати погляди зацікавлених сторін стосовно основних користувачів (тих, хто лише переходить на використання) нових технологій, цілі та цінність даних технологічних рішень відповідно до правового регулювання ПВК/ФТ та інших нормативно-правових рамок юрисдикції. Він також сконцентрував їхній вплив на взаємовідносинах користувачів з наглядовими органами та перешкодах на шляху їх впровадження, а також на взаємозв'язку нових технологій зі стандартами ФАТФ та іншими нормативними рамками. Він також заохотив респондентів подати тематичні дослідження, що ілюструють найкращі практики та/або конкретні проблеми. 54% респондентів визнали себе представниками приватного сектору, переважно великих банків та розробників технологій. На рівні державного сектору більшість відповідей подавали наглядові органи.

2. Нові технології для ПВК/ФТ: на шляху до більш ефективного впровадження стандартів ФАТФ

34. Однією з основних проблем, що заважають ефективному впровадженню заходів ПВК/ФТ, є слабке уявлення про загрози та ризики, пов'язані з ВК/ФТ. Прийняття рішень на основі неналежних оцінок ризиків іноді є помилковим та неактуальним, оскільки всеціло залежить швидше від людського фактора та формального підходу до ризику, а не від застосування справжнього ризик-орієнтованого підходу.

35. Нездатність належним чином ідентифікувати, оцінити та пом'якшити ризик відмивання коштів та фінансування тероризму, в тому числі й основні елементи ідентифікації ризиків (ідентифікація/перевірка клієнтів та моніторинг операцій), створюють перешкоди для ефективності роботи ПВК/ФТ. Саме тут нові технології можуть представляти найбільшу цінність.

36. Більшість зусиль з оцінки та управління поточними ризиками базуються на поєднанні автоматизованого, однак статичного аналізу заздалегідь визначеного ряду факторів ризику, та людських рішень. Старі системи[7] оновлюються новими алгоритмами та введеною вручну інформацією, тим самим створюючи матриці для інтерпретації ризиків та вживання заходів, але вони дуже рідко надають можливість для огляду транзакцій або інституційних ризиків у реальному часі.

37. Більше того, традиційні інструменти оцінки ризиків, засновані на електронних таблицях (таких як Excel) або статичних платформах звітності, не дозволяють аналізувати дані в великих масштабах, обмежуючи можливість кореляції та аналізу генерувати більш детальну картину ризиків. Крім того, якість даних, отриманих застарілими системами, варіюється і можливо не забезпечуватиме точності та деталізації, які необхідні для відповідності стандартам ПВК/ФТ.

38. У приватному секторі неякісна оцінка ризику може призвести до застосування формальної захисної системи ПВК/ФТ, що є неефективною та обтяжливою, і, що більш важливо, не відображає реальних загроз ВК/ФТ для установ. Неякісна оцінка ризиків негативно впливає на реальний підхід до прийняття рішень та захист цілісності фінансової системи на основі ризиків. Це потенційно сприяє виникненню двох окремих проблем - недостатньої уваги до проблеми пом'якшення нових ризиків чи ризиків, які знаходяться в стадії формування (дозволяють відбуватися ВК та ФТ) та надмірному застосуванню заходів щодо зменшення ризиків в ситуаціях з невисоким рівнем ризиків, де можуть бути доречними спрощені заходи (тим самим створюючи клієнтам непотрібні витрати та ускладнення в роботі, включаючи фінансове відчуження).

39. Використання нових технологій для ідентифікації, оцінки та управління ризиками ВК та ФТ дозволяє аналізувати ризики більш динамічно, забезпечувати аналіз мережі та функціонувати на рівні споживачів, інституцій, юрисдикції та транскордонного рівня (див. Вставку 1). Однак для

[7] Для цілей цієї статті під «*старими системами*» мають на увазі системи та практики, які покладаються на *низькотехнологічні (подання вручну та бази даних)* процеси для збору та аналізу даних.

оптимального використання цих інструментів необхідні законодавчі та політичні умови, які передбачають оптимальне об'єднання (даних) та обмін даними, або ж спільну аналітику, а також належний доступ наглядових та правоохоронних органів.

Вставка 1. Інструмент динамічної оцінки ризиків для фінасових установ (FIs)

Багатонаціональна FI будує Інструмент динамічної оцінки, щоб:

- Глибше і в більшому обсязі використовувати, які динамічно оновлюються і відображають результати останніх досліджень.
- Визначати ризики скоєння фінансового злочину значно швидше та більш результативно.
- Проводити точнішу та складнішу оцінку ризиків клієнта.

Цей інструмент використовує можливості хмарного аналізу для централізації та масштабованої обробки даних. Він також включає нові методи, у тому числі машинне навчання, для виявлення ризиків скоєння фінансових злочинів методом:

- Об'єднання існуючих знань щодо типології фінансових злочинів та підозрілих операцій.
- Перевірки транзакційних та соціальних зв'язків суб'єкта господарювання з іншими суб'єктами, які є підозрілими або мають підтверджену негативну характеристику.
- Кількісної оцінки (збору інформації щодо) девіантної поведінки суб’єкта стосовно груп підприємств-аналогів з подібними характеристиками.
- Кількісної оцінки (збору інформації щодо) девіантної поведінки суб’єкта стосовно власної історії попередніх дій.

40. Труднощі у виявленні, розумінні та управлінні ризиками негативно впливають як на державний, так і на приватний сектор. Аналіз Звітів про взаємну оцінку (MERs) четвертого раунду ФАТФ показав, що багато наглядових органів досі не можуть провести належну оцінку ризиків підконтрольних суб'єктів чи то по кожному сектору, чи на інституційному рівні. Проаналізовані MERs дають змогу припустити, що багато наглядових органів не мають можливості збирати та обробляти дані через брак ресурсів та інструментів. Оцінки ризиків деяких наглядових органів не оновлюються належним чином та не мають критичної бази, необхідної для того, щоб прийняти ризик-орієнтований підхід, та забезпечити належний зворотний зв’язок з підконтрольними суб’єктами.

41. В той час як кількість цифрових ідентифікаційних даних та рішень з перевірки транзакцій та звітності ПВК/ФТ зростає, а фірми RegTech швидко поширилися (див. Додаток D), респонденти підтверджують, що все ще існує значний розрив у можливостях наглядових органів та органів регулювання, а також у тому, як вони впроваджують ці технології.

Вставка 2. Інструмент динамічної оцінки ризику для наглядових органів: цифрове рішення для оцінки ризику

Готовий комерційний інструмент (COTS) для наглядових органів за FI або ВНУП автоматизує процес оцінки ризиків ПВК/ФТ, який зазвичай виконується щорічно, для надання інформації про діяльність наглядових органів за певний цикл.

Інструмент COTS забезпечує підтримку ризико-орієнтованого підходу, за допомогою трьох модулів:

- модуль збору даних для забезпечення якості даних та управління опитуваннями,
- модуль оцінки з моделлю ризику, яка імпортує дані, отримані в процесі опитування, оцінює внутрішній ризик та поєднує отримані дані з оцінкою якості контролю для формування рейтингів залишкового ризику на інституційному рівні, та
- модуль аналізу даних для забезпечення відповідного аналізу керівниками секторів, підгалузей, окремих структур та окремих факторів ризику.

Інструмент COTS використовує органічно розроблену модель ризику, що включає концепцію *зменшення розмірності* в алгоритмі оцінки ризику як одну з концепцій машинного навчання. Алгоритм підрахунку оптимізує модель ризику для кожного суб'єкта шляхом зменшення змінних моделі (факторів ризику) до тих, про які повідомляється найактивніше, усуваючи „ефект зглажування/розмивання". Значною перевагою є те, що цей інструмент виявляє ризиковано вузькі бізнес-моделі та невеликих, але ризикованих суб'єктів.

Це рішення виявляє ризики з більшою релевантністю та точністю, а також отримує результати залишкового ризику швидше та з меншими експлуатаційними витратами, ніж неавтоматизовані альтернативні дії.

2.1. Впровадження ризикоорієнтованого підходу

42. *«Ризик-орієнтований підхід – це наріжний камінь ефективної системи ПВ /ФТ, він є важливим для належного управління ризиками»*. (ФАТФ, 2014[5]) Тим не менше, незважаючи на керівні вказівки ФАТФ (ФАТФ, n.d.[6]), які ставлять перед собою цю мету, Стратегічний аналіз 4-го туру взаємних оцінок ФАТФ дійшов висновку, що багато юрисдикцій продовжують застосовувати системи, які базуються на правилах. Подібним чином приватний сектор стикається зі складнощами, коли намагається впроваджувати ризик-орієнтований підхід, і в результаті віддає перевагу дорогому та захисному підходу до ПВК/ФТ.

43. Наявність фундаментальної бази знань та розуміння ризиків, які дають можливість зменшувати та пропорційно розглядати ризики, має вирішальне значення для ефективного впровадження стандартів ФАТФ.

44. Традиційний підхід, заснований на правилах, призвів до дотримання законодавчих вимог з метою захисту, а не до застосування різних пом'якшувальних заходів до різних рівнів ризику. Реакція влади на надлишкове звітування ніж на неповне звітування ще більше сприяла застосуванню захисних заходів.

45. Захисна структура ПВК/ФТ є результатом невизначеності оперативних чи нормативних задач та/або недовіра до застосовуваних стратегій та механізмів. Як державний, так і приватний сектори можуть не довіряти власним оцінкам ризиків через недостатнє розуміння дійсності, відсутність інформації та даних, а також відсутність ресурсів та інструментів для проведення надійних, сучасних та всебічних оцінок ризиків.

46. Більший потенціал для збору та обробки даних, а також можливість ділитися ними з зацікавленими сторонами можуть надати значні переваги в цій галузі, оскільки це сприятиме більш динамічному ризик-орієнтованому підходу.

47. Застосування машинного навчання та інших, заснованих на ШІ, інструментів, які дозволяють здійснювати швидкий та точний аналіз даних у режимі реального часу, може забезпечити вирішення проблем, визначених вище. Такі інструменти можуть частково або повністю автоматизувати процес аналізу ризиків, надаючи йому можливість враховувати більший обсяг даних та виявляти виникаючі ризики, які не відповідають раніше зрозумілому набору параметрів. Такі інструменти також можуть забезпечити альтернативні способи виявлення ризиків, фактично виступаючи як напівнезалежна перевірка висновків традиційного аналізу ризиків.

48. Навіть у випадку, коли висновки, зроблені за допомогою таких інструментів, співпадають з висновками, що є результатом традиційного аналізу ризиків, підтвердження цього може вселити в учасників впевненість у повноті та точності їхніх оцінок. Таким чином, машинне навчання може підвищити ступінь їхньої довіри щодо застосування ризик-орієнтованих заходів, і дозволити їм спокійніше і легше виправдати застосування таких заходів перед своїми наглядовими органами. Наглядовим органам простіше перевіряти автоматизовані інструменти оцінки ризику, які забезпечують більшу об'єктивність.

49. Впровадження нових технологій для усунення цих недоліків вимагає технічної роботи. Однак основними перешкодами є деякі існуючі практики нагляду і контролю та труднощі, з якими стикаються деякі наглядові органи при впровадженні інновацій, як повідомляють респонденти. Тим не менше, приклад з практики у Вставці 3 демонструє, що відбувається бажана зміна у загальній культурі, і деякі керівники вже співпрацюють із сектором, щоб заохотити впровадження нових технологій.

Вставка 3. FinCEN and Федеральні банківські агентства

У грудні 2018 року Федеральні банківські агентства (ФБА) та FinCEN опублікували "Спільну інноваційну заяву", яка заохочує галузь розглядати, оцінювати та, де це доречно, відповідально впроваджувати інноваційні підходи в зобов'язання ПВК/ФТ, дотримуючись Закону про банківську таємницю (BSA)/Зобов'язань щодо дотримання ПВК. Заява фокусується на рішеннях про дотримання ПВК (моніторинг транзакцій), але також включає інноваційні рішення для більш широкого дотримання вимог BSA/ПВК, включаючи інноваційні рішення щодо цифрових ідентифікаційних даних. Він визнає, що відповідальні інновації приватного сектору, включаючи нові способи використання існуючих інструментів або впровадження нових технологій, можуть допомогти банкам виявляти та повідомляти про відмивання грошей, фінансування тероризму та іншу незаконну фінансову діяльність шляхом підвищення ефективності та ефективності дотримання банками BSA/ПВК програми.

Заява має на меті надати гарантію того, що пілотні програми ПВК, призначені для перевірки та підтвердження ефективності відповідальних інноваційних підходів, самі по собі не обов'язково приведуть до:

1) критики з боку наглядових органів, якщо пілотні програми, зрештою, виявляться невдалими;
2) здійснення нагляду, якщо пілотна програма виявляє прогалини в існуючій програмі дотримання ПВК; або
3) додаткових вимог регуляторних органів у разі впровадження інноваційних підходів.

У Заяві також чітко вказується, що FinCEN буде використовувати свої надзвичайні повноваження для підтримки відповідальних інноваційних пілотних програм ПВК/ФТ, які в іншому випадку навряд чи були б можливими через конкретну законодавчу заборону або перешкоду.

Заява також заохочує приватний сектор взаємодіяти з агентствами стосовно їхніх інноваційних пілотних програм для інноваційних підходів BSA/ПВК, наголошуючи на тому, що своєчасне залучення до процесу може сприяти кращому уявленню агентств про ці підходи та дозволить здійснити вимоги наглядових органів коли це потрібно і так, як потрібно.

2.2. Фінансове включення

50. Сприяння фінансовому включенню є важливою частиною ефективного впровадження стандартів ФАТФ та може зменшити загальний ризик ВК/ФТ. Однак пом'якшення фінансового виключенн продовжує створювати проблему.

51. По всьому світу один мільярд людей відчувають великі труднощі, надаючи належні ідентифікаційні документи для відкриття банківських рахунків або забезпечення збереження доступу до фінансових послуг. (Vyjayanti T Desai et al., 2018[7]) Навіть коли ідентифікація є можливою, процедури CDD разом із суворим і формальним впровадженням практик управління ризиками часто призводять до фінансового виключення найбільш слабких сегментів суспільств.

52. Більшість респондентів погодились з тим, що захист прав людей на доступ до фінансових послуг та забезпечення фінансового включення є ключовими елементами адекватного впровадження ПВК/ФТ, і для того, щоб впровадження було ефективним, пом'якшення та уникнення таких непередбачених наслідків повинно бути пріоритетним завданням.

53. ФАТФ підтвердив свою спрямованість на відповідне прийняття своїх Стандартів з урахуванням ризиків, з метою захисту найбільш вразливих груп, та підтримки досягнення гарантій ПВК/ФТ. Публікація Керівних вказівок (інструкцій) ФАТФ щодо заходів ПВК/ФТ та фінансового включення, з додатком стосовно належної перевірки клієнтів, спрямована на підвищення рівня обізнаності щодо цього питання, а також "*заохочення країн використовувати гнучкість Рекомендацій ФАТФ для надання ефективних фінансових послуг особам, які не мають доступу до фінансового сервісу.* (Vyjayanti T DesШІ et al., 2018[7])

54. Останні Керівні вказівки (інструкції) ФАТФ щодо цифрових ідентифікаційних даних (ФАТФ, 2020[8]) також включають детальну інформацію про використання ризик-орієнтованого підходу до рішень стосовно цифрових ідентифікаційних даних для підтримки фінансового включення.

55. У прийнятих на найвищому рівні Принципах G20 (групи двадцяти) стосовно цифрового фінансового включення (G20, 2016[9]) наголошувалося на фінансовому включенні і підтверджувалася необхідність рівномірного підходу з урахуванням факторів ризику до ідентифікаційних вимог, з допомогою цифрових інструментів та фінансової грамотності.

56. Робота ФАТФ посилюється роботою Організації Об'єднаних Націй, яка сприяє та підтримує відповідальне використання біометричних даних для боротьби з тероризмом, з метою запобігання непередбачуваних наслідків та дотримання міжнародного права (UN, 2018[10]).

57. Ключовим елементом забезпечення фінансового включення є впровадження фінансовими установами ефективних ризик-орієнтованих підходів до ПВК/ФТ, включаючи вимоги CDD. (EBA, 2021[11]) CDD лежить в основі оцінки ризику, пов'язаного з окремими клієнтами, замість жорсткого формального підходу і невибіркової політики для широких категорій клієнтів. Інноваційні рішення, засновані на технологіях - як цифрові ідентифікатори (цифрові посвідчення), так і інструменти моніторингу транзакцій на відповідність ПВК - можуть сприяти більш точній та сучасній оцінці ризиків ціною оптимальних затрат та забезпечувати більшу довіру до висновків цієї оцінки ризику, дозволяючи ширше проводити спрощену належну перевірку у відповідних випадках. Це могло б стати важливим фактором, що сприяє фінансовій інтеграції, яка до цього часу стримувалась через неготовність використовувати в повному обсязі гнучкість, передбачену як ризик-

орієнтованим підходом, так і діловими рішеннями на основі прибутку фінансових установ.

58. Інноваційні технологічні рішення можуть сприяти фінансовій інтеграції, якщо вони впроваджуються за допомогою відповідального (Chase, 2020[12]) та ризик-орієнтованого підходу. Вони можуть зводити до мінімуму наявність слабких місць у невідповідностях, пов'язаних із людськими засобами контролю, покращити взаємодію з клієнтами, заощадити витрати та полегшити моніторинг транзакцій, як вказано у Вставці 4.[8] Традиційні вимоги до посвідчення особи (Kazzaz, 2020[13]) можуть бути найбільш очевидним інструментом ідентифікації клієнтів, але не повинні бути єдиним інструментом, який використовуєтьсяз цією метою.[9] Наприклад, засоби обробки природної мови, використання біометрії та інші подібні інструменти[10] можуть бути більш корисними для процесу CDD, ніж примус до особистого виготовлення фізичних документів щодо посвідчення особи, безвідносно до ролі та оглядів аналітиків та експертів, які залишаються ключовими фігурами для запобігання упередженості та інших непередбачуваних наслідків надмірної залежності від технологій.

[8] Докладніше про переваги електронного посвідчення див. (ФАТФ, 2020[8]).

[9] Будь ласка, зверніться до попередніх публікацій FATF щодо електронного ID https://www.fatf-gafi.org/publications/financialinclusionandnpoissues/documents/digital-identity-guidance.html та COVID-19 https://www.fatf-gafi.org/publications/fatfgeneral/documents/covid-19-ml-tf.html для відповідних рекомендацій щодо використання електронних фінансових послуг.

[10] Широко відомий як «електронний ID», що відноситься до сукупності інформації про особу, організацію чи електронний пристрій, який існує в Інтернеті.

Вставка 4. Переваги електронне ID для фінансового включення для регульованих юридичних та фізичних осіб

Для регульованих суб'єктів:

1. Зниження витрат: Електронний ID може підтримувати більш дешеві та складні процеси для прийняття клієнтів на обслуговування. Зокрема, у поєднанні з розширеними можливостями доступу до фінансових послуг через мобільні пристрої та смартфони, технології можуть кардинально змінити спосіб доступу клєінтів до фінансових послуг. Дешевші та більш автоматизовані процеси CDD, що дозволяють розширити набори та джерела даних, можуть дозволити клієнтам, які не мають традиційнї кредитної історії, отримати доступ до фінансових послуг або автоматизованих брокерських послуг - і зробити такі послуги більш доступними.
2. Портативність та експлуатаційна сумісність: Системи можуть використовуватися в рамках декількох установ або фінансових операцій, скорочуючи обтяжливу перевірку лише до одного кроку зарахування клієнта на обслуговування (що дає окремі переваги, якщо початкова перевірка проводиться за ініціативи уряду).
3. Зменшення людських помилок: Хоча людське втручання все ще може бути необхідним і бажаним, автоматизація збору та узгодження даних дозволяє врахувати набагато більше базових даних за коротший проміжок часу, ніж це було б можливо виконати вручну.

Для фізичних осіб:

4. Покращення рівня задоволення клієнтів від якості обслуговування: Цифрове ID значно спрощує складний процес особистого оформлення ID, наприклад, усуває необхідність мати при собі та подавати велику кількість фізичних документів.
5. Багаторазове використання: Системи, що дозволяють багаторазово використовувати перевірений ID, спрощують щоденні операції та сприяють більш ефективній взаємодії з постачальниками послуг та органами влади.

59. Технології також можуть забезпечити фінансове включення завдяки вдосконаленим цифровим інструментам для моніторингу транзакцій. Як викладено в керівних вказівках стосовно фінансового включення, постійний посилений моніторинг можна використовувати для управління ризиками ВК/ФТ, пов'язаними з надійністю даних ідентифікації та перевірки клієнтів, так що управління ризиками ВК/ФТ не так сильно залежить від CDD на час прийняття клієнтів на обслуговування. Наприклад, у випадках, коли клієнти можуть надати лише менш надійні форми підтвердження особи - а отже, елементи ідентифікації та перевірки є недостатньо надійними, - технологічні рішення, такі як аналіз поведінки клієнта, можуть сприяти підвищеному та посиленому моніторингу транзакцій та ділових відносин, тим самим

заохочуючи клієнтів до співпраці. Ці технології також можуть забезпечити надійний і невпинний процес моніторингу та краще розуміння ризиків.

60. Розробка технологічних рішень у цьому контексті може сприяти операціям із "білим маркуванням" (наприклад, зарплата, оплата комунальних послуг та витрат на проживання, виплати державної допомоги тощо), а також може використовуватися для розширення обмежених рахунків, за умови, якщо і у випадках, коли оцінка ризиків клієнтів дозволяє це робити. Це дало б можливість більшій кількості клієнтів отримати доступ до основних банківських послуг, одночасно пом'якшуючи ризики, з якими стикаються фінансові установи. Тим не менш, важливо забезпечити, щоб CDD при відкритті рахунку надавав достатньо інформації для ефективного моніторингу клієнтів, що має наслідки з точки зору кількості інформації, яку потрібно зібрати. Моніторинг не буде ефективним методом контролю, якщо установа має занадто мало інформації про своїх клієнтів та про очікуване використання ними відповідних фінансових продуктів.

61. Крім того, вдосконалення моніторингу транзакцій може полегшити фінансове виключення, якщо вони надають банкам більшої впевненості в тому, що інші види фінансових установ, такі як надавачі MVTS, використовують надійні програми дотримання вимог. Краща оцінка ризиків, процедури CDD та адекватні інструменти моніторингу можуть стати важливою частиною більш інклюзивних та безпечних фінансових систем, які не дискримінують на основі засобів, соціального чи регіонального контексту.

62. Цифрові рішення для фінансового включення, наприклад біометрія, не позбавлені власних проблем. Також існують ризики, що такі процеси можуть посилити фінансове виключення в тих секторах населення, які не мають доступу до електронних пристроїв, обізнаності та довіри до можливостей, які вони створюють, особливо там, де надавачі фінансових послуг розробляють лише цифрові бізнес-моделі. Деякі з нинішніх стратегій, що застосовуються для сприяння фінансовому включенню, можуть також призвести до затримки процесу виключення. Обмежені рахунки[11] можуть звужувати тип діяльності або функції, яких очікують від банківського рахунку, і призвести до незадовільної якості обслуговування клієнтів та подальшого виходу з офіційної банківської системи. Також було визначено, що віддалена реєстрація, рівні рахунків та відстрочені посвідчення особи іноді призводять до створення додаткових труднощів у повному доступі до фінансових послуг. (Kazzaz, 2020[13]) У цьому контексті інновації можуть також допомогти пом’якшити непередбачувані наслідки нових технологій, пропонуючи альтернативи моніторингу банківських зв'язків фінансових установ. Профілі поведінкових ризиків, мережевий аналіз та використання психометричних даних можуть, наприклад, інформувати про андеррайтинг та доступ до кредитів, стаючи потужним доповненням до переваг, що створюються системами цифрових ідентифікаторів.

63. Важливо, щоб використання таких підходів також створило шлях до повного обслуговування та необмеженого доступу до фінансових послуг, де це можливо. Вищезазначені рішення мають певний потенціал для сприяння

[11] Обмежені або базові рахунки – це мінімальні рахунки, призначені для надання доступу до фінансових послуг. Ці облікові записи часто мають обмеження на вартість транзакцій, можливість доступу до кредитних та онлайн-банківських інструментів або платіжних систем.

цьому переходу (наприклад, посилений технологією постійний моніторинг протягом тривалого періоду та аналіз поведінки клієнта можуть дати більш надійну основу для профілювання ризиків клієнтів та підвищити ефективність посиленої належної перевірки, пов'язаної з недостатньою надійністю ідентифікації та перевірки клієнта, що потенційно дозволяє розширити функції вищезазначених рахунків).

64. Зрештою, будь-яке прийняття нових технологій для цілей ПВК/ФТ повинно слідувати підходу, орієнтованому на вирішення проблем, водночас не створюючи додаткового навантаження чи непередбачуваних наслідків.

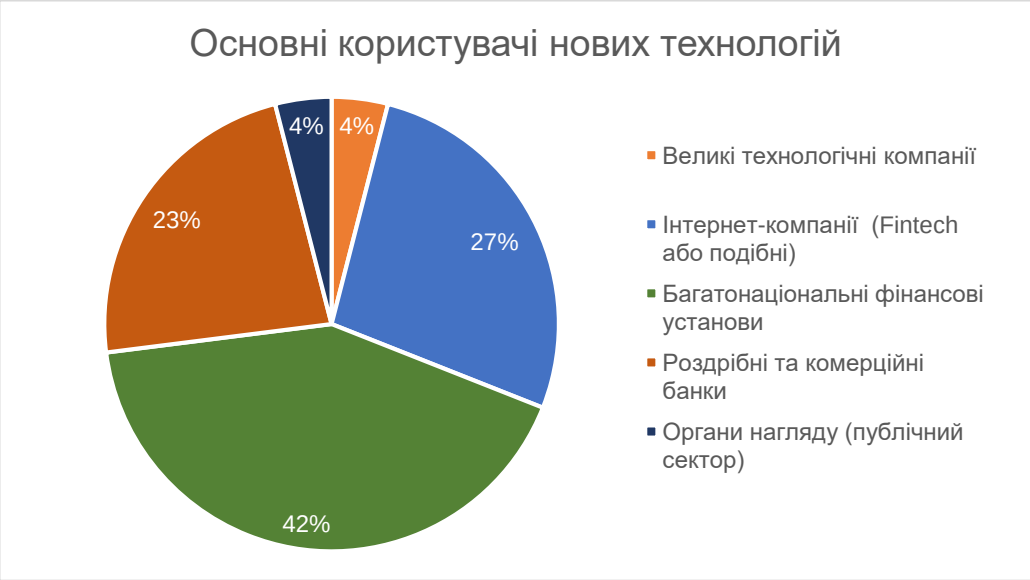
3. Можливості нових технологій у ПВК/ФТ

65. Запитальник з цифрової трансформації ФАТФ передбачав збір інформації про те, як розробляються та впроваджуються нові технології для ПВК/ФТ, зокрема:

- *Хто* використовує нові технології?
- Для яких функцій ПВК/ФТ вони використовуються?
- Які основні технології використовуються для виконання цих функцій?

66. Щодо питання, хто використовує нові технології, FI, розробники технологій та регульовані компанії FinTech субнаціональні компанії очолили групу користувачів нових технологій, як показано на рисунку 1.

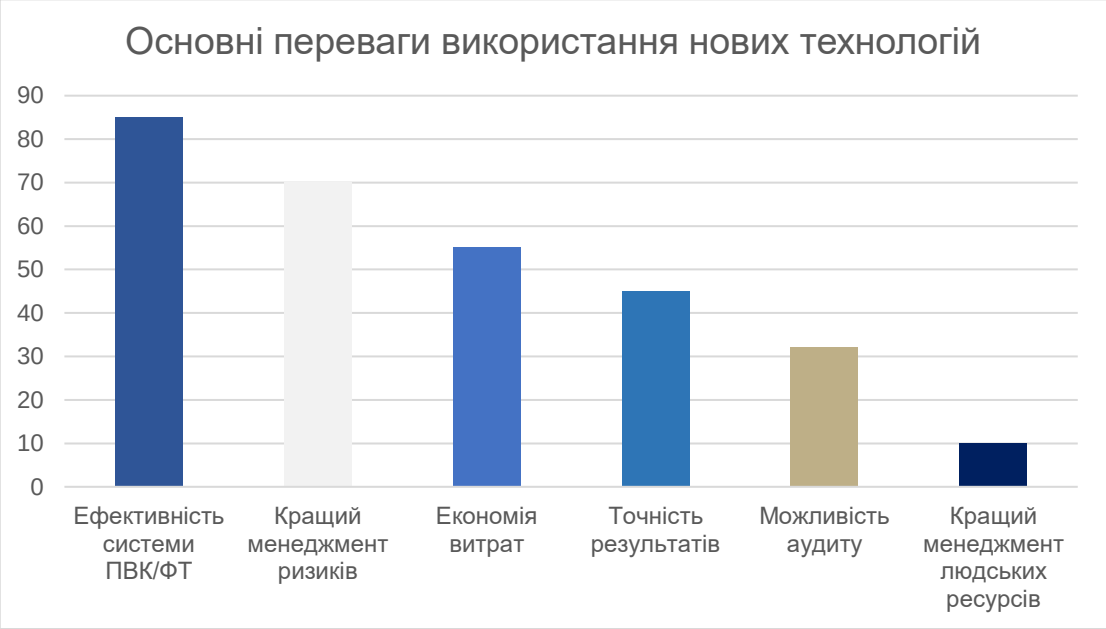
Рисунок 1. Основні користувачі нових технологій



67. Респонденти вважають, що впровадження та попит на нові технології залишаються нерівномірними і що значні прогалини продовжують існувати не тільки між великими фінансовими установами та меншими суб'єктами, але і на регіональному та національному рівнях, а менші економіки не встигають за цифровими інноваціями.

68. Щодо питання, *для яких* функцій ПВК/ФТ вони використовуються, нові технології обіцяють перспективу підвищення ефективності діяльності ПВК/ФТ, надаючи зацікавленим сторонам більш швидкі та ефективні в економічному відношенні інструменти. 85% респондентів погоджуються, що ефективність ПВК/ФТ загалом є найважливішою перевагою використання нових технологій, тоді як краще управління ризиками займає наступне місце за актуальністю, як це показано на рисунку 2. Респонденти заявили про швидкість, гнучкість, функціональні можливості та краще управління, які є прямим результатом застосування нових технологій і сприяють підвищенню ефективності ПВК / ФТ.

Рисунок 2. Основні переваги використання нових технологій



69. Респонденти наголосили на більш широкому використанні наглядовими органами нових технологій, які могли б сприяти підвищенню ефективності ПВК/ФТ через розширення можливостей нагляду. Переваги нових технологій для наглядових органів, згаданих експертами, включають здатність:

- Контролювати більшу кількість суб'єктів господарювання[12];
- Краще виявляти та розуміти ризики, пов'язані з різними секторами окремих суб'єктів господарювання;
- Здійснювати контроль дотримання стандартів ПВК/ФТ у реальному режимі та вживати заходів у випадках невідповідності;
- Встановлювати ефективні зв'язки з підконтрольними організаціями та здійснювати додаткові інформаційні запити;
- Зберігати, обробляти та звітувати про більший набір наглядових даних;
- Обмінюватися інформацією з іншими компетентними органами.

70. Переваги для приватного сектора включають можливість:

- Кращого виявлення, розуміння та управління ризиками ВК/ФК;
- Можливість обробки та аналізу більших наборів даних швидше, невідкладніше і точніше;
- Більш ефективних інтеграційних практик (цифрових);

[12] Збільшення кількості контрольованих суб'єктів як наслідок діджиталізації визначають як один із вирішальних факторів попиту на використання Suptech. Інші включають потребу в більш точних даних, підвищену складність нормативних актів, вдосконалення можливостей управління ризиками, а також більш змістовну політику, а також сприяють наглядовому контролю. (FSB, 2020[14])

- Забезпечення більшої наявності умов для проведення перевірки, підзвітності та загального належного управління;
- Зниження витрат та максимізація людських ресурсів для більш складних областей ПВК/ФТ;
- Поліпшення якості подання звітів про підозрілу діяльність.

71. На більш детальному рівні респонденти підкреслили здатність нових технологій забезпечувати результати загалом та результати обробки даних, які не тільки виходять за межі людських можливостей у сфері обробки великих обсягів інформації в рекордні терміни, але також є більш надійними та простішими для передачі їх іншим суб'єктам, як результат стандартизації даних та узгодження програмного забезпечення.[13]

72. 52% респондентів визнали RegTech сферою ПВК/ФТ, де можна отримати максимальну кількість переваг від нових технологій.[14] Зокрема, респонденти підтвердили, що обробка та аналіз великих наборів даних, необхідних для оцінки та аналізу ризиків, CDD, а також моніторинг транзакцій є сферами, які забезпечують найбільш практичне використання переваг нових технологій.

73. Респонденти наголосили на тому, що нові технології можуть покращити можливості ПВК/ФТ та вивільнити людські ресурси для більш важливої роботи, такої як аналіз складних випадків ВК/ФК. Організація обробки даних, в тому числі можливість збирати, аналізувати та використовувати інформацію корисним, але ефективним з точки зору затрат способом, була наскрізним елементом відповідей.

74. Крім того, нові технології були охарактеризовані як такі, що дозволяють отримати більш точну інформацію, яка зберігається у внутрішніх системах, хоча деякі респонденти наголошували на важливості постійного контролю та на тому, що машинне навчання передбачає навчання на основі дій та рішень людини, а також на основі існуючих інституційних практик.

75. Також ключовою перевагою було виділено елемент своєчасності та можливості постійного аналізу та оновлення даних без потреби втручання людини; зокрема, щодо застарілих систем та можливості оновлення записів клієнтів. Це особливо актуально для інструментів обробки природними мовами, які дозволяють узгоджувати записи клієнтів, незважаючи на різницю в написанні чи помилку при введенні вихідних даних.

76. По третьому питанню - які основні технології використовуються для виконання цих функцій - в запитальнику було поставлено питання, які технології мають найбільший потенціал для сприяння ефективності ПВК/ФТ. Відповіді визначили ШІ (включаючи інструменти машинного навчання та обробки природних мов), Інтерфейси Прикладного Програмування та інструменти, що використовуються для цілей CDD, як найбільш спроможні.

[13] Детальніше про роль обміну інформацією див. (ФАТФ, 2020[37])

[14] Опитування EBA 2019 щодо Regtech показало, що значна частка банків, включених до вибірки (42%), впровадили принаймні одне рішення RegTech. Доступно за адресою: https://www.eba.europa.eu/financial-innovation-and-fintech/fintech-knowledge-hub/regtech-industry-survey

77. Технологія розподіленого реєстру (або технологія блокчейну) згадувалася на ранніх стадіях цієї роботи як потенційно важлива, але респонденти виявили нижчий рівень її прийняття. Тим не менше, кілька прикладів конкретних проектів, заснованих на TPP – які, в основному, все ще перебувають на стадії розробки - наведено нижче.

3.1. Штучний інтелект (ШІ)

78. ШІ - це наука про імітацію здібностей людського мислення для виконання завдань, вирішення яких, як правило, потребує людського інтелекту, наприклад, розпізнавання закономірностей, складання рекомендацій щодо прогнозів або прийняття рішень. ШІ використовує передові обчислювальні методи для одержання інформації про різні типи, джерела та якість (структуровану та неструктуровану) інформаційного забезпечення для "автономного" вирішення проблем та виконання завдань. Існує кілька типів ШІ, які працюють з (і досягають) різними рівнями автономії, але загалом, ШІ системи поєднують у собі інтенціональність, рівень інтелекту системи та переналагоджуваність.

79. *Машинне навчання* - це тип (підмножина) ШІ, який «навчає» комп'ютерні системи для вивчення даних, виявлення закономірностей та прийняття рішень із мінімальним втручанням людини. Машинне навчання передбачає розробку послідовності дій для автоматичного вирішення проблеми за допомогою досвіду та існуючих алгоритмів розпізнавання образів з обмеженим втручанням або без участі людини - тобто це метод аналізу даних, який автоматизує побудову аналітичної моделі. Респонденти називають машинне навчання та обробку природних мов як можливості інтелектуальних програмних продуктів, що забезпечують великі переваги для ПВК/ФТ для регульованих суб'єктів та наглядових органів (див. Вставку 5). За деякими даними машинне навчання створює найбільш сприятливі умови завдяки своїй здатності вчитися на вже існуючих системах, а саме зменшує потребу введення даних про моніторинг вручну, зменшує хибні спрацьовування та виявляє складні випадки, а також полегшує управління ризиками.

Вставка 5. Використання наглядовими органами машинного навчання

Бразилія

Процеси нагляду

У 2019 році Центральний банк Бразилії (ЦББ) розробив матрицю пріоритетів з набору об'єктивних показників для того, щоб визначити, яким суб'єктам нагляду слід надавати пріоритет у річному плануванні нагляду (РПН). Ця матриця пріоритетів була вперше використана у 2020 році як вхідна інформація для планування нагляду на 2021 рік (як прототип).

ЦББ використовує машинне навчання для вдосконалення матриці пріоритетів для підтримки свого РНП в рамках ризикоорієнтованого підходу. Метод навчання без контролю ззовні використовується для розрахунку оцінки ризику регульованих суб'єктів.

80. Програми машинного навчання корисні для виявлення аномалій та показників, що випадають із загального ряду, виявлення та усунення повторюваної інформації для покращення якості даних та аналізу. Наприклад, технологія глибинного вивчення (DL) - це вдосконалений тип машинного навчання, в якому штучні нейронні мережі (алгоритми, на які надихнув людський мозок) з численними і глибокими шарами, навчаються на великих обсягах даних значною мірою автономно. Алгоритми DL виконують завдання багато разів, кожного разу трохи його підправляючи для поліпшення результату, тим самим дозволяючи машинам вирішувати складні проблеми без втручання людини.

3.2. Обробка природної мови та м'які обчислювальні техніки

81. Обробка природної мови (ОПМ)[15] - це розділ ШІ, що дозволяє комп'ютерам розуміти, інтерпретувати та підробляти людську мову. Нечітка логіка - це технічний логічний прийом, який бере неточні або приблизні дані та обробляє їх, використовуючи кілька значень, таким чином, що дає придатний для використання (але неточний) результат. Такі логіки не є бінарними, оскільки використовують широкий діапазон значень, а не лише 0 або 1. Системи нечіткої логіки можуть давати корисний результат у відповідь на неповні, неоднозначні, спотворені або неточні (нечіткі) дані, симулюючи прийняття людських рішень більш точно, ніж класична логіка, і отримання більш корисної інформації з даних, які є надто неточними, щоб дозволити отримувати певні результати за допомогою класичної логіки. Нечітка логіка може бути реалізована в апаратному устаткуванні, програмному забезпеченні або в їх поєднанні.

[15] «Обробка природної мови (ОПМ) – це підвид штучного інтелекту, який допомагає комп'ютеру розуміти, інтерпретувати та підробляти/відтворювати людську мову. ОПМ допомагає комп'ютеру обмінюватися інформацією з людьми їхньою ж мовою, даючи змогу комп'ютеру зчитувати текст, слухати усну мову, інтерпретувати її, зчитувати емоційний тон , та визначати, які з цих частин є важливими.» (SAS, n.d.)

Вставка 6. Нечіткі логічні програми

Італія

Підрозділ фінансової розвідки Італії (ПІРФ) у співпраці з Генеральним управлінням фінансового нагляду та регулювання Банку Італії створили застосунок із застосування нечіткої логіки для створення показників ПВК для небанківських фінансових посередників. Запропонована нечітка система - на даний момент на експериментальному етапі - дозволяє опрацьовувати кількісні дані (тобто транскордонні платежі з/до країн з підвищеним ризиком) для підтримки періодичної оцінки ризиків ПВК/ФТ таких посередників.

Джерелом даних, що використовуються для обчислення показників, є сукупна база даних звітів про боротьбу з відмиванням грошей (S.AR.A. з італійської абревіатури) та звіти наглядових органів. Для побудови показників небанківські фінансові посередники розподіляються за різними класами відповідно до їх типології (наприклад, суб'єкти регулювання інвестицій, компанії з управління активами, установи, що здійснюють платежі та електронні гроші, кредитні організації) та основної діяльності (наприклад, відкриті фонди, закриті фонди, грошові перекази, електронні гроші та інші платіжні послуги тощо).

82. Інструменти обробки природних мов та нечітких відповідностей також створюють можливість для більш ефективного зменшення помилкових спрацьовувань та негативних наслідків (наприклад, у процесі перевірки санкцій), але головним чином вони долають проблеми якості даних, оскільки програми покращують зв'язування різних елементів інформації, наприклад, пов'язують сторінки видачі результатів пошукової системи зі списками PEPs, виявляють спроби шахрайства, моніторять санкційні списки тощо, як показано у Вставці 7.

Вставка 7. Обробка природної мови на практиці

Бразилія

Центральний банк Бразилії (ЦББ) затвердив проект SupTech з обробки природних мов (ОПМ) у квітні 2020 року, з метою включення застосунків ШІ для обробки документів на основі ОПМ техніки з метою нагляду.

Цим проектом ЦББ має намір і надалі зменшувати ризик, пов'язаний з невиконанням своїх наглядових повноважень, встановлених у його законодавчій та нормативній базі, та збільшити продуктивність нагляду.

Інструменти, що розробляються, включають аналіз:

- Соціальних мереж: збір текстів як допоміжного джерела інформації для наглядової діяльності;
- Внутрішніх звітів та документів: класифікація та короткий зміст відповідей регульованих суб'єктів в контексті дистанційного контролю ПВК/ФТ, що зберігається у вебсистемі (SisAPS - докладніше в Додатку С) з метою збільшення продуктивності обробки представленої якісної інформації, з забезпеченням покращення наглядових запитів;
- Зовнішніх звітів та документів (пояснювальні записки, звіти про аудит, відповідні факти та протоколи колегій): досліджень, узагальнень та класифікації відповідної інформації до Нагляду, наприклад, якісної інформації у пояснювальних примітках зі звітів про аудит;
- Глобальний інтернет-пошук (веб-вилучення даних): сканування публічних даних для аналізу, створення показників та/або формування баз даних з метою вилучення інформації, пов'язаної з регульованими суб'єктами, залученими до ВК/ФТ. На другому етапі машинне навчання буде використано для читання новин та вилучення з них свідчень про юридичних осіб, які беруть участь у відмиванні грошей на основі торгівлі (TBML);
- Автоматизації звітів - перевірки та прогрес: автоматизоване формування описових текстів робочих документів та звітів для використання в перевірках.

83. В широкому розумінні, застосування ШІ до процесів ПВК/ФТ може посилити здатність суб'єктів реагувати на ризики та ефективніше реалізовувати вимоги. Ці інструменти не є заміною, а скоріше доповненням систем, спрямованих на поліпшення результатів та спрощення дотримання вимог.

84. Моніторинг транзакцій з використанням ШІ та інструментів машинного навчання можуть давати регулюьованим суб'єктам можливість виконувати звичні функції з більшою швидкістю, точністю та ефективністю (за умови, що машина належним чином та точно налаштована) (див. Вставку 8). Ці моделі

корисні для фільтрації справ, які потребують додаткового розслідування. Використання нових технологій для цілей моніторингу, здебільшого, слід і надалі інтегрувати з більш широкими системами контролю, які включають елемент людського аналізу для конкретних оповіщень або сфер підвищеного ризику. Ці системи також мають покращити ступінь з'ясовності та наявності умов для проведення перевірки, щоб повністю відповідати більшості наглядових вимог.

Вставка 8. Де машинне навчання може забезпечити корисні результати?[1]

- *Ідентифікація та перевірка клієнтів:* У контексті дистанційного взяття на обслуговуваннчя клієнта та автентифікації, ШІ, включаючи біометрію, так і методи машинного навчання та детектори життєздатності можуть використовуватися для проведення: аналізу мікроміміки, перевірок на підробку, виявлення підроблених зображень та аналізу особливостей обличчя людини.
- *Моніторинг ділових відносин та аналіз поведінки та транзакцій:*
  - *Неконтрольовані алгоритми машинного навчання:* На основі поведінки клієнтів відносити їх до цілісних груп, що надалі створюватиме елементи контролю, які можна встановлювати більш ефективно, на основі підходу, заснованого на оцінці ризику (наприклад, налаштування порогу транзакцій), що дозволяє здійснювати індивідуальний та ефективний моніторинг ділових відносин.
  - *Керовані алгоритми машинного навчання:* дозволяють проводити більш швидкий аналізу даних у режимі реального часу відповідно до відповідних вимог ПВК/ФТ.
  - *Підрахунок попереджень:* Підрахунок попереджень допомагає зосередитись на моделях діяльності та направляти відповідні повідомлення або сповіщати про потребу посиленої належної перевірки.
- *Визначення та впровадження нормативних оновлень:* Методи машинного навчання з обробкою природних мов (ОПМ), когнітивними обчислювальними можливостями та автоматизованою робототехнікою можуть постійно сканувати та інтерпретувати великі обсяги неструктурованих нормативних джерел даних для автоматичного виявлення, аналізу та створення шорт-листів, які потім застосовуються до установи; або впроваджувати (до певної міри) нові чи вже переглянуті нормативні вимоги (шляхом кодифікації та створення робочих процесів реалізації), щоб регульовані суб'єкти могли дотримуватися відповідних програмних засобів контролю.
- *Автоматизована звітність даних (ADR):* використання стандартизованих шаблонів звітності з використанням автоматизованих цифрових додатків (інструментів

використання даних), що робить деталізовані висхідні дані про регульованих суб'єктів в цілому доступними для наглядових органів.

1. Неповний перелік

3.3. Технологія розподіленого реєстру (блокчейн)

85. TPP може покращити відстежуваність трансакцій на міжнародному рівні, і навіть у глобальному масштабі, потенційно полегшивши перевірку особи. Відповідальне та регламентоване використання TPP для цілей управління даними та процесами також може пришвидшити процес CDD, оскільки споживачі можуть автентифікуватися і їх доступ може бути автоматично схвалений або заборонений за допомогою смарт-контрактів, що перевіряють дані (див. Вставку 9).

86. Крім того, при належному режимі гарантій та відповідній нормативній базі, транзакціями потенційно можна керувати як через єдиний реєстр, яким користуються декілька установ з різними юрисдикціями, так і через взаємно сумісні реєстри. Це значно збільшило б можливості моніторингу порівняно з існуючими рамками. Це також означає, що в міру того, як TPP стає більш зрозумілим та доступним, договірні відносини, наприклад, можуть бути вбудовані в цінні папери, оскільки вони випускаються за допомогою смарт-контрактів, що означає, що кожного разу, коли ініціюється операція з цінними паперами, інші акціонери автоматично отримуватимуть повідомлення та можуть стати - залежно оформлення контракту- контрагентами даної операції.

87. Технології TPP можуть також забезпечувати переваги для управління вимогами CDD, що сприятиме зацікавленню користувачів цим процесом, більшій економічній ефективності для приватного сектора та створенню більш точної та якісної бази даних. Наприклад, у Китаї TPP використовується фінансовими установами для обміну списками контролю чи попереджувальними червоними прапорцями на основі ступеня конфіденційності, дозволеного цією системою.

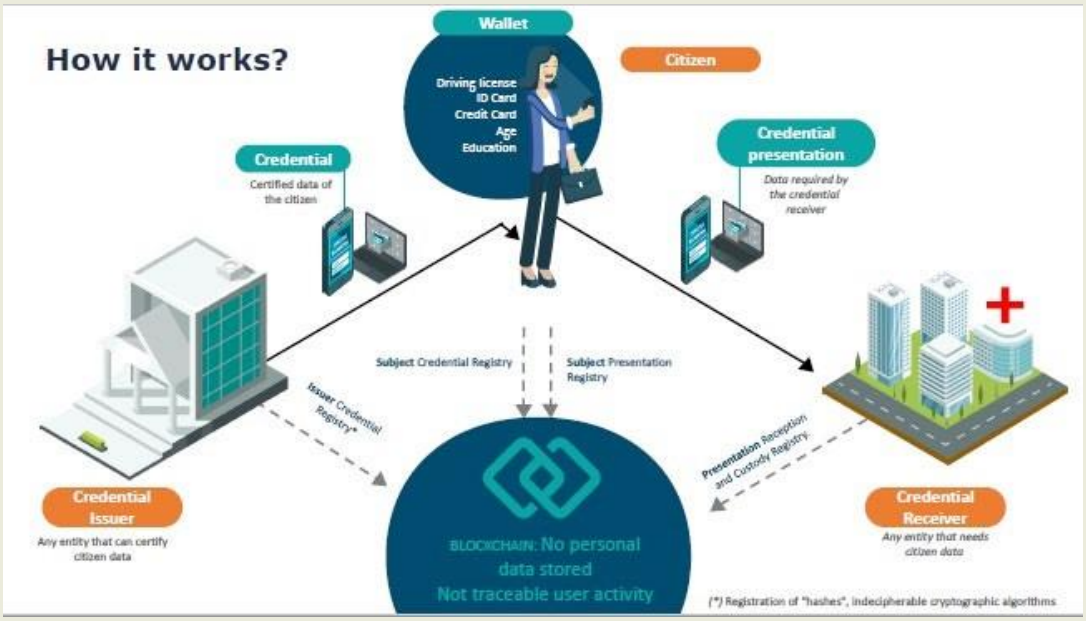
88. Незважаючи на переваги, TPP, здається, продовжує створювати проблеми і підвищувати стурбованість з точки зору ПВК/ФТ, як видно з регулювання та/контролю віртуальних активів.[16] На відміну від транзакцій, які проводяться через звичайних посередників, таких як банки, транзакції з віртуальними активами (VA), засновані на TPP, мають децентралізований характер і дозволяють здійснювати опосередковані транзакції між двома фізичними особами без будь-якого контролю. Вони також створюють проблеми юридичного характеру, якщо немає єдиного органу чи чіткого місця розташування закладу, відповідального за діяльність. Це може створити потенційні проблеми для традиційних стандартів ФАТФ, які зосереджені на регулюванні/контролі посередників. Тому використання цієї технології повинно контролюватися та додатково в деталях розглядатися членами ФАТФ. Влада також може мати бажання розглянути негоативні

[16] Розгляньте (FATF, 2021[38]) Розділ V

екологічні наслідки використання TPP у порівнянні з традиційними інструментами.

Вставка 9. CDD та TPP

Проявивши сумісну ініціативу разом з дев'ятьма великими приватними компаніями з різних галузей та отримавши підтримку від місцевих наглядових органів, даний суб'єкт демонструє модель управління особистими даними з точки зору керованості користувачем (суверенна ідентичність). Вона слідує європейським та іспанським стандартам, щоб гарантувати сумісність з майбутніми альтернативами. Оскільки ця система використовує TPP, вона надає змогу користувачеві контролювати операції з «гаманця», що спрощує обмін та процедури ID та CDD з суб'єктами-партнерами. Даний проект знаходиться в пілотній фазі розробки, запуск у виробництво очікується у 2021 році.



3.4. Програмне забезпечення для належної перевірки клієнтів

89. Ідентифікація/верифікація та моніторинг клієнтів є ключовим елементом системи ПВК/ФТ, але, в деяких випадках, продовжує створювати проблеми щодо впровадження та ефективності. Застосовані на неризиковій основі, ці зусилля вважаються витратними та здебільшого неефективними, оскільки вони забирають ресурси та час, часто не призводячи до точних процесів оцінки ризику чи успішних ділових відносин.

90. За даними опитуваних учасників приватного сектору, заходи CDD та моніторинг являють собою надзвичайно трудомісткий процес, до того ж створюючи високі рівні невизначеності щодо якості даних, труднощі з оновленням та узгодженням інформації у відповідності до вимог. Процедури CDD також є одними з основних джерел невдоволення клієнтів. Процес збору та перевірки інформації часто буває складним та напруженим, сповненим відповідних запитів на документи та додаткових особистих періодичних надань доказів. Крім того, експерти вказують, що аналіз ризиків, згенерований CDD, надто засновується на правилах замість того, щоб виходити з поведінки або контексту, що призводить до фінансової ізоляції непривілейованих осіб чи груп, які роблять все можливе, щоб виконати вимоги.

91. Застосування нових технологій до CDD та моніторингу може сприяти вирішенню цих проблем за допомогою більш налагоджених процесів *взяття на обслуговування* клієнтів, адаптованих до ризику, контексту та окремих людей, не порушуючи цілісність суб'єкта, який надає послугу, або забезпечує фінансову систему. Вони можуть покращити взаємодію з клієнтами, а також сприяти забезпеченню більш ефективних гарантій ПВК/ФТ. Наприклад, дані свідчать, що змішані підходи, коли офіційні посвідчення надаються в парі з біометричною ідентифікацією, можуть забезпечувати більш надійні процеси ідентифікації та верифікації.

92. ID представляє собою один з найкращих практичних прикладів у цій галузі, оскільки він був широко прийнятий і підтримується в багатьох юрисдикціях (а ФАТФ видав вказівки щодо його використання). Докази свідчать, що криза підчас епідемії COVID-19 ще більше сприяла попиту на віддалене надання фінансових послуг. Насправді електронна ідентифікація та верифікація є одними з «найбільш зрілих та елементів технології в ПВК, які можна використовувати миттєво». (Richard Grint et al, 2017 [14]) Вони також є одним із найбільш впізнаваних і часто згадуваних респондентами опитування як хороша практика в ПВК / ФТ (див. Вставку 10).

93. Електронний ID може покращити, наприклад, доступ клієнтів до фінансових послуг через мобільні пристрої та смартфони, одночасно гарантуючи безпеку та точність інформації про клієнта за допомогою біометричної інформації як доповнення до персональної інформації про особу. Деякі фінансові установи можуть, спираючись на основну інформацію про ID особи, збільшити різноманітність джерел даних, збираючи додаткові дані від клієнтів, з їх дозволу, що в кінцевому підсумку зміцнює знання та здатність керувати діловими відносинами.

Вставка 10. Рішення щодо цифрової ідентифікації

Положення eIDAS

Положення eIDAS є першим глобальним транскордонним механізмом для довіреної електронної ідентифікації та довірчих послуг. Правила дозволяють використовувати ідентифікатори електронної пошти, видані в одній державі-члені ЄС, для доступу до мережевих державних послуг в іншій державі-члені. Довірчі послуги - це електронні послуги, які ставлять за мету зробити електронні бізнес-операції більш безпечними, зручними та ефективними. Довірчі послуги згідно eIDAS включають електронні підписи, електронні печатки, додаткову часову інформацію, послуги електронної доставки та автентифікацію веб-сайту. eIDAS встановлює узгоджені правила та певний процес для розвитку європейського внутрішнього ринку довірчих послуг, які визнаватимуться в різних країнах, і матимуть такий самий правовий статус, як їхні традиційні еквівалентні паперові процеси.

Індія - eKYC

Індія запровадила систему електронної перевірки ідентифікаційних даних клієнта - eKYC (електронний принцип індивідуальної роботи з клієнтами). Ця система реалізована через Aadhaar, 12-значний ідентифікаційний номер, виданий Управлінням з індивідуальної ідентифікації Індії (UIDAI). Під час реєстрації в Aadhaar, такі деталі, як ім'я, адреса, стать, дата народження, номер мобільного телефону та електронна адреса фіксуються і заносяться в базу даних UIDAI.

FI можуть використовувати інтерфейс прикладного програмування eKYC (API) для отримання доступу до деталей Aadhaar для перевірки, а UIDAI гарантує, що FI відповідають встановленим стандартам захищеності, безпеки та конфіденційності під час збору даних. Аутентифікація клієнта здійснюється за допомогою одноразового пароля, надісланого на записаний номер мобільного телефону, або за допомогою біометрії. Ці положення щодо eKYC були включені до Правил запобігання відмиванню грошей, 2005 (PMLR), в 2019 році. „Засіб автентифікації eKYC" було визначено відповідно до правила 2 (1) (ca).

CKYC

Індія ввела в дію Центральний реєстр KYC (CKYC), централізоване сховище записів клієнтів у фінансовому секторі KYC з єдиними нормами KYC, щоб забезпечити зручність взаємного використання.

CKYC керується CERSAI (Центральний реєстр реконструкції активів сек'юритизації та захисту інтересів Індії) і уникає ситуацій, коли у

клієнтів виникає необхідність виконувати формальності KYC з кількома фінансовими органами до встановлення ділових відносин.

CKYC був включений у PMLR у 2019 році та визначений відповідно до правила 2 (1) (ac).

Сінгапур – MyInfo

Сінгапур запустив першу Національну службу електронних посвідчень у 2017 році, відому як MyInfo, яка надає перевірені урядом дані, отримані з різних державних установ. Згода на використання MyInfo дає змогу жителям та корпораціям обмінюватися перевіреними даними з підприємствами, тим самим мінімізуючи необхідність бізнесу отримувати додаткові фізичні чи електронні документи для обробки.

Використання MyInfo для проведення належної перевірки клієнтів підвищило ефективність, безпеку та досвід клієнтів стосовно процесу оформлення клієнта. Це також дало змогу фінансовим установам продовжувати приєднання нових клієнтів під час пандемії COVID-19, коли існує більший попит на дистанційне надання фінансових послуг.

94. Крім того, інструменти *при взятті на обслуговування клієнта*, що дозволяють швидко здійснити CDD та аналіз клієнтських систем (такі як геолокація, перевірка кредиту, програмне забезпечення для боротьби з шахрайством та інші), також збагатять CDD та процес моніторингу та призведуть до більш точного розуміння природи ділових відносин, а також його значення для установ.

95. Розширене використання технологій для перевірки та підбору клієнтів має великий потенціал для вдосконалення процесів дотримання вимог, оскільки залежність від застарілих та регіонально нерелевантних списків санкцій, PEP та інших списків, визнано сферою, яка потребує вдосконалення (див. Вставку 11). Такі інструменти дозволяють диференціювати подібні імена та інші елементи ідентифікації, долати мовні відмінності, визначати перехресні посилання з несприятливою інформацією в засобах масової інформації та різними базами даних. Обробка природної мови та вдосконалені інструменти нечітких відповідностей можуть надати значні переваги цій функції. Узгодження даних також допомогла б усунути помилкові спрацьовування та спроби шахрайства, оскільки суб'єкти починають використовувати об'єднану інформацію та різноманітні системи перевірки.

96. Насамкінець, вважається, що цифрові рішення, спрямовані на реагування на виклики належної перевірки клієнтів, найбільше сприяють ефективності ПВК/ФТ, коли обмін інформацією та об'єднання даних дозволяється та застосовується на практиці, що є ще одним прикладом важливості подолання бар'єрів обміну даними. Спільна CDD була визначена респондентами як важливий елемент більш ефективної системи, а отже, тієї, на розробці якої

політики та наглядові органи повинні зосередитись, знаходячи при цьому адекватні рішення, щоб примирити їх з необхідністю того, що регульованим суб'єктам потрібно брати на себе свої обов'язки відповідно до ризик-орієнтованого підходу.

Вставка 11. Машинне навчання для цілей CDD

Бразилія

Системоутворюючі фінансові установи Бразилії (SIFI) використовують машинне навчання у власних системах моніторингу та процесах CDD/співробітників/ партнерів з метою виявлення нових ризиків відмивання грошей та фінансування тероризму та збільшення швидкості аналізу та ролі сповіщень з попередженями.

З цією метою у них створені спеціалізовані групи, наявні спеціалісти з теорії та методів аналізу даних і процесів, а також технологічне середовище, які здатні підтримувати великі обсяги даних (напр.: SAS, Teradata, R-Studio, Foundry, Hadoop, Python тощо).

Щодо процесів моніторингу та сповіщень з попередженнями

Використовуючи інструменти аналітики та інтеграцію різних баз даних, SIFI створили нові сценарії, що призвело до зменшення помилкових позитивних сповіщень та підвищення ефективності аналізу сповіщень у цілому. Слід зазначити, що багато SIFI створюють різні тематичні сценарії, результати яких вже виявилися ефективними, особливо ті, що зосереджені на ситуаціях, що виникають внаслідок пандемії COVID-19, наприклад, придбання лікарняного обладнання за державні ресурси та оплата екстреної допомоги.

На основі алгоритму машинного навчання типу посилення градієнта, деякі SIFI створили кластери ризиків, які дозволяють приймати рішення методом групового, а не індивідуального аналізу, щоб оцінити ймовірність того, що попередження буде передано до Підрозділу фінансової розвідки (ПФР).

Деякі SIFI також використовують контрольовану техніку кластеризації, щоб визначити правила для вловлювання "різко випадаючих показників" в операціях з готівкою, тоді як інші використовують одномірний та двомірний дослідницький аналіз, аналіз ознак та технології для конструювання ознак, щоб ідентифікувати клієнтів, які здійснюють транзакції поза їх профілем.

SIFI розробив інструмент, який використовує аналітичні технології для аналізу зв'язків між учасниками оповіщення,

картографування взаємозв'язків, ризиків та географічної інформації для підтримки його аналізу.

Щодо процесів CDD

SIFI використовують методи машинного навчання для підтримки оцінки ризиків своїх клієнтів, беручи до уваги різні змінні, пов'язані з реєстрацією клієнтів та фінансовими операціями.

Наприклад, SIFI поєднує техніки машинного навчання (посилення градієнта, алгоритм випадкового лісу, класифікатор голосування, серед інших) з логістичною регресією для вибору клієнтів для посиленої належної перевірки. Інша SIFI розробляє інструменти для ідентифікації компаній-оболонок та впровадження інтегрованого моніторингу клієнтів на основі реєстрації та фінансової інформації.

Результати

SIFI вже отримали переваги в результатах своїх процесів ПВК/ФТ, таких як:

- вища якість інформації, отриманої під час спостереження за поведінкою своїх клієнтів, що дає змогу генерувати попередження з точки зору клієнта;
- більша активність генерування попереджень шляхом виявлення тих, що становлять більший ризик для підконтрольних суб'єктів;
- зменшення помилкових позитивних сповіщень шляхом побудови більш чітко визначених правил шляхом вивчення зразків поведінки та моделей;
- більша ефективність та дієвість аналізу попереджень;
- покращення якості звітності до ПФР, надання більш детальної інформації про підозрілі операції;
- збільшення кількості звітів про підозрілі транзакції (STRs) до ПФР як наслідок створених нових сценаріїв та правил;
- виявлення нових ризиків ВК/ФТ завдяки посиленню співвідношення даних, що дозволяє приймати кращі рішення;
- можливість моніторингу замовника в цілому на основі реєстрації та фінансової інформації, доступної в установах конгломерату та зовнішніх постачальників.

3.5. Інтерфейси прикладного програмування (ІПП)

97. ІПП - це тип програмного забезпечення, яке дозволяє різним програмам підключатися та спілкуватися. ІПП також часто використовуються для надання платіжних послуг, наприклад, для прийому пожертв через вебсайти. Респонденти на запитання про цифрову трансформацію ШІ згадали ІПП серед найбільш вживаних та найрелевантніших рішень для виявлення проблем відмивання грошей та фінансування тероризму.

98. Їх користь для ПВК/ФТ полягає у здатності, наприклад, пов'язувати програмне забезпечення для ідентифікації клієнтів із інструментами моніторингу, або інструменти ідентифікації ризиків та загроз із профілями ризиків клієнтів, щоб генерувати попередження або змінювати класифікації ризиків як відповідні. ІПП дозволяють здійснити цю інтеграцію набагато швидше та з набагато більшими наборами даних. Це особливо актуально, оскільки однією з найскладніших проблем для багатьох фінансових установ є інтеграція багатьох різних та часто несумісних систем, включаючи успадковані технології та спеціалізовані інструменти, створені різними розробниками.

Вставка 12. Переваги ІПП

- Посилення взаємодії між традиційними банківськими даними та відхід від закритих систем із фрагментованими структурами.
- Збільшення автоматизації, що може відобразитися в оптимізації ресурсів і висхідній точності системи.
- Забезпечення комплексного та уніфікованого потоку даних, який допомагає сконструювати більш повний профіль ризиків для нових клієнтів, наприклад під час процесу взяття клієнтів на обслуговування.

99. ІПП також представляють значну цінність для державного сектора, оскільки дає змогу отримувати доступ до реєстрів підприємств та інших осіб, а також забезпечує "швидкість адаптації, яка буде змінюватися для тимчасового моніторингу у відповідь на несподівані потрясіння в економіці або ж частіше у відповідь на зміни у бізнес-моделях фінансової системи".[17]

[17] (FSB, 2020[15])

Вставка 13. ІПП на практиці

Платформа Hannibal

ПФР Тунісу, CTAF, запустила у січні 2021 р. Regtech під назвою «Платформа Hannibal», який постійно контролює фізичне перевезення валюти в країні. Платформа Hannibal - це плід співпраці та координації між правоохоронними органами (Міністерством внутрішніх справ та митниці), банками, поштою, обмінними пунктами, під наглядом та керівництвом ПФР Тунісу.

Платформа Hannibal націлена на розуміння, виявлення та оцінку національних ризиків відмивання грошей та фінансування тероризму, пов'язаних із фізичним транскордонним перевезенням валюти.

Ця платформа була розроблена з використанням технології блокчейну, яка вважається однією з найважливіших сучасних технологій у галузі зберігання даних. Вона гарантує прозорість інформації та підвищує її безпеку від будь-яких спроб злому. Платформа також покладається на ІПП, які з'єднують бази даних зацікавлених сторін (Міністерство внутрішніх справ, митниця, банки, пошта, обмінні пункти та ПФР Тунісу).

Використання API дає змогу відповідним органам влади отримувати дані про обсяги імпорту іноземних валют та всіх банківських операцій, пов'язаних з іноземними валютами, та дані про вилучення іноземних валют правоохоронними органами, у режимі реального часу.

Використовуючи цю технологію, відповідні органи отримують змогу відстежувати кінцеве призначення валют, що експортуються чи імпортуються та декларуються на митниці. Зазначена технологія також уможливлює здійснення кількох точок перетину операцій, з метою отримання негайних попереджень залежно від програмованих параметрів, і навіть трансформувати інформацію в розвідувальні дані.

Платформа дає можливість владі Тунісу вживати відповідних заходів для зменшення національних ризиків відмивання грошей та фінансування тероризму, пов'язаних із фізичним транскордонним перевезенням валюти.

Агрегатори рахунків

IndiaStack - це набір ІПП, що дозволяє урядам, компаніям, стартапам та розробникам використовувати унікальну цифрову інфраструктуру для вирішення в Індії проблем у сфері надання безпаперових та безготівкових послуг.

India Stack пропонує чотири різні технологічні рівні, включаючи універсальну біометричну цифрову ідентифікацію особи, єдиний інтерфейс для всіх банківських рахунків країни, безпечний спосіб обміну даними та можливість для цифрових ідентифікаційних

документів рухатись вільно, усуваючи необхідність збору та зберігання паперових документів.

Ця інфраструктура складається з Aadhaar, eKYC, eSign, DigiLocker та UPI, інструментів, що сприяють впорядкованому зростанню відкритого банкінгу в країні.

Соціальна служба США на основі згоди Адміністрації соціального забезпечення США Перевірка номера безпеки (CBSV)

Служба CBSV використовує вузол ІПП, до якого кваліфіковані фінансові установи або їх уповноважені постачальники послуг (дозволені організації) можуть отримати доступ, щоб перевірити, за згодою фізичної особи та у встановлених законом цілях, чи вказане ім'я особи, SSN та дата народження, подані уповноваженою організацією, відповідають цій інформації в записах SSA. CBSV повертає підтвердження відповідності у вигляді "так" або "ні". Якщо записи SSA показують, що власник SSN помер, CBSV також повертає підтвердження смерті. CBSV не перевіряють чи є документи, що засвідчують особу, справжніми.

В даний час CBSV, як правило, використовується компаніями, які надають банківські та іпотечні послуги, здійснюють кредитні перевірки, забезпечують попередні перевірки даних, задовольняють вимоги щодо ліцензування тощо. CBSV потребує одноразової початкової плати за реєстрацію в розмірі 5000 доларів США та плати за кожну транзакцію верифікації SSN.

100. Окрім спрощення внутрішніх процедур, ІПП спрощують обмін інформацією між суб'єктами.

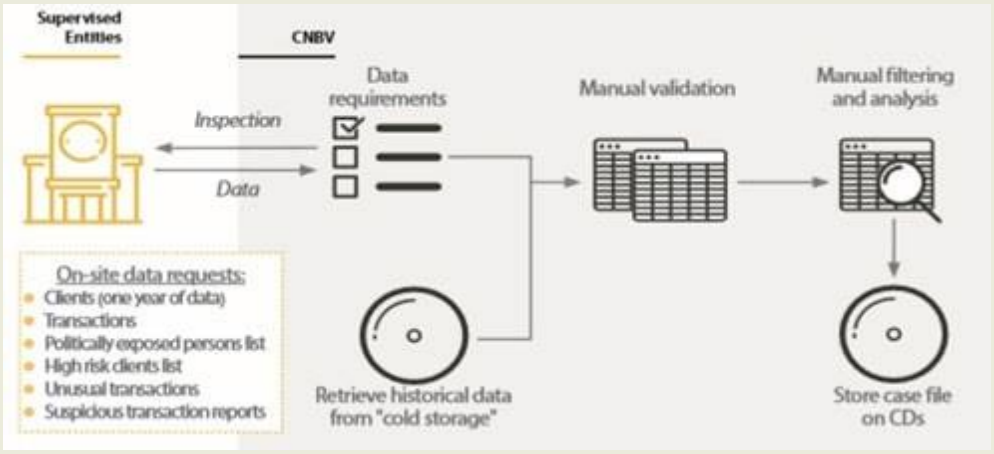
101. Використання наглядовими органами ІПП в поєднанні з аналізом, керованим ШІ, може підвищити ефективність санкціонованих практик звітності та якість ризик-орієнтованого нагляду. Як показано у Вставці 14 нижче, такий тип інструменту дозволяє наглядовим органам обробляти накопичені статистичні дані паралельно з даними виїзних перевірок та ситуативними факторами, а також створювати автоматизовані звіти для розгляду та визначення дій.

102. Цей автоматизований аналіз надає можливість забезпечити регулбованих суб'єктів більш нагальними та детальними зворотними відгуками про процес нагляду та очікувані результати.

Вставка 14. Мексика

Неефективність архітектури даних щодо ВК у поєднанні з багатьма фінансовими установами, які класифікуються як ризики із середнім та середнім ризиком, призводить до *невдач в отриманні детальної інформації* з даних, що інформують про виїзні перевірки або в інший спосіб, а також до *затримки та непродуктивного аудиту*.

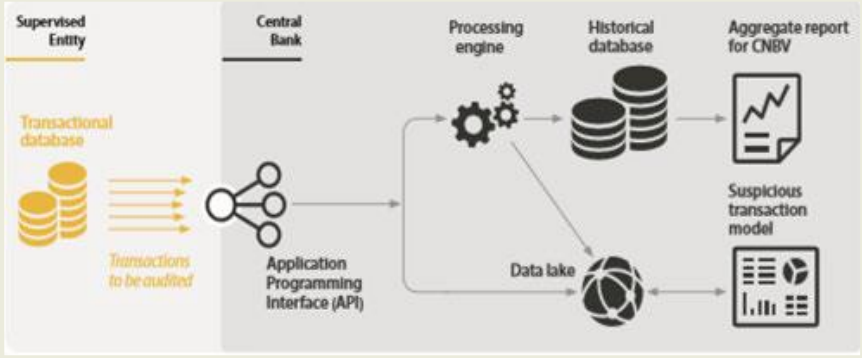
Відправна точка:



Інноваційне рішення SupTech:

Архітектура даних ПВК на основі API та *інструмент аналітики на основі штучного інтелекту*, який включає: Централізовану платформу для створення стандартизованих, автоматизованих запитів до підконтрольних об'єктів із необробленими даними, отриманими за допомогою методу push або pull, що зберігаються в базі даних. API призначений для створення безпечної, прямої лінії передачі даних від машини до машини, яка передає дані в механізм обробки, миттєво запускаючи перевірку якості, змісту та структури звітів та направляючи оброблені дані в озеро даних, створюючи консолідовану, єдину та доступну архітектуру керованих даних.

Аналітика на основі штучного інтелекту, яка виявляє підозрілі транзакції за допомогою прогнозного аналізу та методів відмивання коштів (кластеризація, нейромережі, логістична регресія, випадкові ліси) та рекомендує сповіщення щодо відмивання коштів, використовуючи технології ВК на основі фінансових ризиків. Панелі приладів та відстеження списків спостереження надають уявлення про ландшафт ризиків ПВК. На другому етапі мита включатиме аналітичний інструмент на основі штучного інтелекту, який виявляє підозрілі транзакції за допомогою прогнозного аналізу та методів відмивання коштів (кластеризація, нейромережі, логістична регресія, випадкові ліси) та рекомендує сповіщення щодо відмивання коштів, використовуючи ВК, що базується на відповідних ризиках FIs.



4. Проблеми впровадження нових технологій для протидії відмиванню коштів та фінансуванню тероризму (ПВК/ФТ)

103. Прийняття та впровадження нових технологій в рамках ПВК/ФТ відбувається не без проблем. До основних проблем відносяться проблеми у сфері регулювання та оперативні складнощі.[18]

Рисунок 3. Виклики у розробці та/або впровадження нових технологій

4.1. Проблеми регулювання

104. Дані, зібрані для цього звіту, свідчать про необхідність чіткої підтримки з боку ФАТФ та національних компетентних органів щодо інновацій у сфері ПВК/ФТ. Кілька експертів висловили бажання мати «технологічно активні наглядові органи» - наглядові органи, які бажають взаємодіяти з розробниками технологій, а не притримуються технологічно нейтральних підходів. Респонденти вважають, що відсутність прямої підтримки компетентних

[18] Підтверджено (Richard Grint et al, 2017 [14])

органів та ФАТФ призвела до зменшення інтересу, інвестицій та довіри до нових технологій, незважаючи на їх потенціал.

105. Здатність інтерпретувати та пояснювати[19] нові технології для наглядових органів є ключовим фактором забезпечення підтримки цих інструментів. Перед застосуванням цих нових технологій регулбовані суб'єкти повинні вміти пояснити принципи та технічні деталі інноваційних рішень і повинні нести відповідальність за них. Наглядові органи повинні вміти сприймати моделі, що використовуються інструментами штучного інтелекту, щоб визначити їх точність та відповідність виявленим ризикам. Однак кілька респондентів заявили, що більшість наглядових органів не мають досвіду чи ресурсів, які б дозволили їм зрозуміти та адекватно контролювати нові технології.

106. Респонденти також зазначили, що навіть найбільш грамотні в технологічному відношенні органи нагляду часто повільно відрегульовують практику нормативного регулювання. Дійсно, хоча деякі юрисдикції вже сприяють впровадженню нових технологій за допомогою інноваційних заходів та інших форм нормативної підтримки (див. Вставку 15), ці зусилля не завжди переходять у прийняття наглядовими органами нових процедур та дотримання встановлених правил.

Вставка 15. Використання державної інфраструктури для полегшення процедур електронних заходів належної перевірки клієнтів (CDD)

Нещодавно датська програма оцінки фінансового сектору опублікувала відкриту консультацію щодо технологічних ініціатив, які можуть підтримати компанії, що підпадають під дію норм щодо протидії відмиванню коштів та фінансуванню тероризму у їхніх зусиллях проти фінансової злочинності, «проєкт AML/TEK». Його мета полягає в тому, щоб стимулювати дискусію на цю важливу тему та отримати розуміння для забезпечення аргументованої політичної дискусії щодо подальших дій.

В аналізі представлені плюси і мінуси семи ініціатив, які потенційно можуть зміцнити першу лінію оборони за рахунок використання технологій. Аналіз, як правило, відображає високий рівень оцифрованості датського суспільства, але також порушує питання, що становлять загальний інтерес щодо компромісних ситуацій, зокрема щодо боротьби з фінансовою злочинністю, захисту даних та конфіденційністю.

Аналіз має на меті забезпечити базу для подальшого обговорення. Більшість ініціатив мають юридичні наслідки для суб'єків звітування та клієнтів, а також порушують питання щодо правової основи доступу та обміну даними. Три з цих ініціатив можуть підтримати подальшу оцифровку CDD-процедур:

[19] Для більш детальної інформації розгляньте (EBA, 2020[17])

Розширений доступ до відповідних державних реєстрів

Основною перешкодою для суб'єків звітування щодо своїх CDD-процедур є відсутність перевіреної електронної інформації про клієнтів. Оскільки датські органи мають кілька реєстрів із відповідною інформацією про клієнтів, результат аналізу розглядає надання більш широкого доступу до цих реєстрів. Аналіз розглядає доступ до даних у декількох реєстрах, наприклад, до даних, що зберігаються Датською адміністрацією бізнесу, Датським податковим агентством, реєстрів паспортів та водійських посвідчень, реєстрів Імміграційної служби Данії тощо.

Забезпечення якості даних у датському реєстрі підприємств

Дані, наявні в Датському бізнес-реєстрі, надаються самими суб'єктами звітування. Отже, хоча більшість основних даних компанії доступні через інтерфейс прикладного програмування (API) і підпадають під всебічне середовище контролю, ідентифікація всіх несправних або недобросовісних реєстрацій не є точною, що загрожує застосуванню даних для цілей CDD. Таким чином, аналіз пропонує розглянути, чи можливо створити механізм, за допомогою якого юристи та сертифіковані аудитори можуть перевіряти зареєстровані дані.

Рішення з перевірки Публічних діячів (PEP)

Перевірка PEPs та їх взаємозв'язків є трудомістким ручним процесом для суб'єків звітування, що вимагає від них отримання персональних даних про своїх клієнтів. У Данії такі відносини можуть значною мірою бути відображені через державні реєстри, хоча це викликає серйозні занепокоєння щодо захисту даних. Аналіз розглядає створення державного рішення для перевірки PEP, яке могло б поліпшити якість та знизити вартість перевірки PEP завдяки збільшенню діджитизації, одночасно мінімізуючи збір особистої інформації.

107. Використання нових технологій для ПВК/ФТ може по-справжньому стати ефективним лише в тому випадку, якщо системи базуються на стандартизованих даних, які розробникам технологій легше інтегрувати у свої інструменти, котрі легко зрозуміти та пояснити неспеціалістам, а також у разі потреби легко донести інформацію колегам та компетентним органам. Це питання також свідчить про важливість державних органів, зокрема ПФР, при наданні зворотного зв'язку суб'єктам звітування щодо підозрілої діяльності та випадків злочинності, які можуть бути використані для навчальних цілей. Підготовка системи машинного навчання, заснована на реальних справах, які були позитивно підтверджені як такі, що стосуються відмивання коштів або фінансування тероризму (за умови їх існування), запропонувала б значно кращий коефіцієнт ефективності, ніж навчання штучного інтелекту відтворенню рішень відповідального працівника про відповідний рівень підозр. Крім того, здатність ПФР та інших компетентних органів надавати зворотний зв'язок щодо того, які звіти є найбільш корисними, за допомогою

автоматизованих процесів також допомогла б навчанню фінансових інституцій та інформуванню груп та систем щодо дотримання внутрішніх вимог.

108. Гармонізація даних (або її відсутність) також була згадана як додаткова перешкода, оскільки витрати на інвестування в нові технології та знання зростають в геометричній прогресії, якщо ці системи потребують доопрацювання та адаптації до різних юрисдикційних вимог та форматів. Отже, гармонізація даних дає суттєві переваги у створенні сприятливого середовища для впровадження нових технологій, оскільки це дає змогу учасникам сходитися в таких цілях, як, наприклад, загальний моніторинг транзакцій, надання зворотного зв'язку приватному сектору та оцінка ризиків. Забезпечення якості даних - проблема, яка є спільною для 45% респондентів, згідно із запитальником цифрової трансформації - розглядається як перешкода на шляху до прийняття рішень, заснованих на технологіях ПВК/ФТ.

109. Реальні або передбачувані проблеми інтерпретації також призвели до обмежень у здатності будувати надійні відносини між постачальниками технологій та користувачами, а також відсутністю довіри щодо того, що дані, які обробляються за допомогою нових технологій, можуть бути надійними. Тим не менше, зростаюча кількість суб'єктів реєструє дані у великих масштабах, і це збільшення масштабу операцій означає більшу здатність узгоджувати різні набори складних даних.

110. Роль третіх сторін як постачальників нових технологій була визнана 60% респондентів як достатньо чітка, зідно із запитальником щодо цифрової трансформації, проте респонденти приватного сектору вимагали додаткових вказівок щодо тлумачення чинних норм цифрової ери.

111. Приватний сектор вимагав додаткових роз’яснень щодо питання підзвітності, прозорості та нагляду суб’єктів, що використовують нові технології. Оскільки впровадження технологій у цьому просторі набирає темпів, наглядовим органам слід замислитися над тим, які інструменти регульовані суб'єкти використовують та чи повинні постачальники цих інструментів підпадати під додатковий контроль, наприклад, як постачальники послуг для регульованих суб'єктів або за допомогою окремого регулювання та нагляду. Влада може також розглянути питання про те, чи може інноваційна технологія протидії відмиванню коштів та фінансуванню тероризму, яка використовується регульоаними суб'єктами та/або контролюючими органами, бути більш ефективною за рахунок нових форм співпраці, наприклад, державно-приватного партнерства або розширеного доступу реугльованих суб'єктів до державних баз даних. Однак використання інноваційних рішень не повинно ставити під сумнів кінцеву відповідальність, що лежить на регульованих суб'єктах.

112. Хоча посилене впровадження нових технологій, ймовірно, сприятиме посиленню наглядової практики, респонденти зазначили, що необхідно дотримуватися балансу між важливістю інтеграції технологій та «*важливістю збереження перспективного процесу нагляду за участю*

людини»[20]. З метою впровадження цього підходу, більшість доступних інструментів все ще включають людський ресурс та звіт як ключовий компонент та доказ того, що ці інструменти є не заміною існуючих систем, а їх вдосконаленням.[21]

113. Було визначено, що людський ресурс та розбудова потенціалу продовжують відігравати важливу роль у підтримці прийняття нових технологій ПВК/ФТ, зокрема стосовно елементів, які технологія все ще не може подолати, регіональної нерівності або експертних можливостей з питань, що виникають. У цьому звіті було виявлено численні випадки успішної співпраці з метою ПВК/ФТ, яка отримала технологічну підтримку, але в основному спиралася на діалог та зобов'язання між учасниками з метою досягнення успіху. Такі підходи до співпраці між державними та приватними суб'єктами, наприклад, з метою ідентифікації слабких місць відмивання коштів та фінансування тероризму, змогли продемонструвати безпосередні переваги використання технології для вирішення конкретних проблем, не будучи повністю залежними від цих засобів підвищення ефективності.[22]

114. Подібним чином, системи, засновані на державних засобах цифрової ідентифікації особи, забезпечують більший успіх у застосуванні систем цифрових ідентифікаторів та спільних платформ у порівнянні з системами, які покладаються на збір даних з багатьох джерел. Перевірка даних може бути одним із аспектів, якщо повноваження, виконувані *людьми*, і надалі переважатимуть. Крім того, оскільки використання нових технологій набуває все більшого поширення, учасники також повинні враховувати ступінь прийнятності або неприйнятності *помилки машини*.

115. Серед інших причин, що не пов'язані з ПВК/ФТ, є та, що підвищена ефективність ПВК/ФТ також обмежується неможливістю регульованих суб'єктів обмінюватися інформацією зі своїми колегами та за кордоном. Зрештою, для повного розуміння природи та ризику підозрілих транзакцій учасникам потрібен доступ до їх повного шляху, який часто виходить за певні межі або здійснюється іншими суб'єктами. Нові технології можуть зробити значний вклад у подолання цієї проблеми, про що детальніше йде мова у звіті ФАТФ щодо підбору даних, спільного аналізу та захисту даних.

116. Нарешті, питання безпеки та захисту від втручання злочинців посідає верхнє місце в списку зазначених проблем у відповідях приватного сектору, хоча воно, можливо, більш вагоме з точки зору державної політики та

---

[20] (FSB, 2020[15]), ст. 32.

[21] Детальніше про відповідні події в галузі suptech та їх зв’язки з нормативною звітністю див. Crisanto et al., Від подання даних до обміну даними: наскільки suptech та інші нововведення можуть оскаржити статус-кво нормативної звітності? (BIS, 2020 [18])

[22] Дивіться, наприклад, проект COMCRIM щодо боротьби зі злочинами, що підривають верховенство права, такими як торгівля людьми, відмивання грошей та корупція розумним та всебічним способом, у фінансовому державно-приватному партнерстві та за допомогою штучного інтелекту. Доступно за адресою: www.uva.nl/en/about-the-uva/organisation/faculties/amsterdam-law-school/research/researchthemes/labour-exploitation-human-trafficking/labour-exploitation-and-human-trafficking.html. Дивіться також роботу некомерційної мережі експертів The Knoble, яка працює над запобіганням фінансовій злочинності за допомогою спільних та технічних підходів. Доступно за адресою: www.theknoble.com/

правоохоронних органів. Тим не менше, зростає кількість кримінальних справ, пов'язаних із використанням технологій, наприклад, пов'язаних з шахрайським використанням особистих даних або злочинними операціями, що використовують "мулів", що слід враховувати при оцінці впливу нових технологій на операції регульованих суб'єктів та злочинну діяльність загалом.

4.2. Операційні проблеми

117. Операційні проблеми здебільшого відносяться до застосування практик до нових, а іноді і неперевірених систем, або технологічних рішень. Питання, пов’язані з витратами на нові технології, здатністю суб’єктів розуміти та навчати персонал для їх впровадження, а також заміною застарілих систем новими інструментами, були одними з основних питань, які піднімалися респондентами.

118. Незважаючи на широке визнання переваг, впровадження наглядовими органами нових технологій відстає від рівня впровадження приватним сектором. Респонденти наголошують на тому, що наглядовим органам необхідно оновити власні системи та стратегії контролю, щоб мати змогу краще інтерпретувати та контролювати ПВК/ФТ у цифрову епоху.

119. Наглядові органи визначили як найбільші перешкоди витрати, пов’язані із заміною застарілих систем, наявністю якісних даних про ПВК/ФТ, а також наявністю спеціалізованих ресурсів та кваліфікованого або експертного персоналу.

120. Наприклад, процеси закупівель для оновлення застарілих систем є надто складними, тривалими і часто не спрямовані на потрібних учасників. Кілька респондентів заявили, що процеси державних закупівель для SupTech часто не цікаві або не помітні для провайдерів технологій, оскільки вони потребують знання процесів державних закупівель та конкретних цілей управління, чого бракує розробникам технологій. Більше того, вид технологій, до яких звертається державний сектор, часто або застарілий на той час, коли він доходить до стадії закупівель, або вимагається в дуже директивному порядку і не приваблює постачальників технологій (тобто вимагає ексклюзивності). Така практика стримує розробників від випуску готової продукції, призначеної для наглядових органів.

121. Проблеми в цьому напрямку включають небажання інвестувати в нові технології, які можуть: бути важко інтегровані разом із застарілими системами та/або виходити за рамки технічного потенціалу підконтрольного суб'єкта для належного та ефективного використання; застаріти та вимагати додаткових інвестицій у новіші рішення; не відповідати нормативним очікуванням або не задовольнити конкретного експерта, який може не мати можливості оцінити ефективність рішення або відчувати незручності щодо інноваційних рішень з інших причин; становити небезпеку, включаючи такі ризики як потенційні порушення конфіденційності та порушення законодавства про ПВК/ФТ. Зокрема, меншим фінансовим установам часто не вистачає внутрішньої спроможності чи впевненості для оцінки ефективності даного інноваційного рішення серед великого кола конкуруючих постачальників та товарів, число яких продовжує зростати, щоб визначити, чи

це підходить для характеристики ризиків установи, клієнтської бази та ділової діяльності, або для впровадження моделей та управління їх ризиком.

122. Загалом, респонденти погодились з тим, що деякі наглядові органи не так поінформовані, як приватний сектор, з технологічним сектором про тенденції та нові цифрові рішення. Відсутність спеціальних навичок (і ресурсів) та знань збільшує проблему інтерпретації нових технологій і, здебільшого, обмежує їх потенціал для ефективності ПВК/ФТ.

123. Деякі респонденти також згадували, що внаслідок відсутності гармонізації масштабне використання технологій може бути неможливим. Це потенційно може завадити інноваціям досягти економічної ефективності та перешкодити їх розвитку. Наприклад, найефективніше використання великих даних вимагає, щоб вони були доступні для декількох об'єктів. Без такої масштабованості деякі технологічні інструменти можуть бути фінансово недоцільними.

124. Крім того, неможливість розробити технології відповідно до масштабу ще більше посилює прогалини між рівнем використання великими і меншими підприємствами, та різними регіонами. Респонденти погодились, що більш широке впровадження технологій стане можливим лише за умови наявності більш значних стимулів, чи передбаченого санкціонованим використанням або більш довірчого середовища, які підтримують інвестиції та виправдовують реформування менших фінансових операцій та інших не фінансових суб'єктів звітування.

125. Нові технології покращили якість даних, але і надалі будуть покладатися на людський ресурс та індивідуальні перевірки. Інструменти машинного навчання покладаються на існуючі системи та їх ручне оновлення, таким чином, можливо, створюючи випадки, коли вводяться "невірні дані", які спричиняють негативний вплив на прийняті моделі. Вони включають дані, на яких навчається система машинного навчання, наприклад вмінню виявляти підозрілі операції. Якщо дані навчання включають помилкові позитивні спрацьовування чи інші помилки, ці помилки будуть «вивчені» системою машинного навчання, хоча певне передбачення імовірності помилки все одно знадобиться для тих випадків, коли наявна упередженість людини чи є невстановлені помилки.

126. Автоматизація початкового введення даних за допомогою засобів обробки природної мови може також покращити якість даних, мінімізуючи помилки клієнтів або персоналу, що реєструють дані.

127. Зрештою, потреба клієнтів у нових технологіях у сфері фінансових послуг була визначена як один із найменш значущих рушіїв впровадження нових технологій. Просування ролі та точки зору клієнта може, тим не менш, ставати дедалі актуальнішим, оскільки CDD та інші індивідуальні цифрові рішення стають все більш помітними.

128. Оскільки суб’єкти долають виявлені нормативні та операційні виклики, можливо, варто задуматись про реакцію клієнта на традиційні CDD та процедури моніторингу, а також про нові застосовні підходи та способи впливу на захист даних та конфіденційність. Клієнти можуть не впливати на розвиток цих технологій, але тим не менше на них впливають інструменти, які змінюють досвід взаємодії із клієнтом. Хоча використання нових технологій для ПВК/ФТ може також бути на користь клієнтів, існують ризики

та непередбачувані наслідки для оцифровування, які необхідно враховувати при прийнятті та впровадженні цих інструментів.

129. Серед найчастіше згадуваних ризиків оцифровування виступає зловживання системою злочинцями та наслідки цього у вигляді підвищення вразливості та фінансового виключенняпевних верств суспільства, тобто людей літнього віку, сільських чи віддалених (менш зв'язаних чи далеких) громад.

Вставка 16. Подолання оперативних викликів

Гонконгський валютний орган (HKMA) здійснив низку кроків для виявлення загальних операційних проблем, з якими стикаються банки при впровадженні нових технологій, та впровадив низку заходів з надання допомоги банкам у подоланні цих проблем, починаючи з Форуму ПВК/ФТ у листопаді 2019 р. Протягом 2020 року відбулися обговорення з близько 40 банками між трьома робочими групами відповідно до їх готовності до впровадження технологій - для кращого розуміння того, як до Regtech звертаються як до засобу для вдосконалення процесів ПВК/ФТ.

Ці зусилля кульмінаційно завершилися в січні 2021 р. тим, що HKMA обмінявся практичним досвідом із банками, які впровадили ПВК/ФТ, у формі звіту «*ПВК/ФТ Regtech: тематичні дослідження та ідеї*» (Гонконгський валютний орган/Делойт, 2021 р. [15]). Звіт спрямований на підвищення рівня обізнаності та зниження реальних та можливих бар'єрів для прийняття законів про ПВК/ФТ Regtech шляхом обміну тематичними дослідженнями та ілюстрування різних підходів (наприклад, підходу, який базується на використанні сценарію, призначеного для користувача, та підходу, який заснований на рішенні). Він також дає змогу скласти уявлення про тих, хто впроваджує нові проекти, корисну інформацію про нові технології та вказівки щодо вирішення ключових операційних викликів (таких, як готовність даних та процесів, підтримка з боку зацікавлених сторін та виконавська підтримка, а також фактори, які слід враховувати під час роботи із незалежними постачальниками). Звіт побудований таким чином, щоб банки з різним рівнем готовності впровадження могли перейти до застосування технології, яка їх цікавить, або виклику, який резонує з ними. Продовжуються подальші заходи, спрямовані на різні групи готовності, наприклад, через сумісне використання галузі та інтерактивні лабораторні сесії.

4.3. Непередбачувані наслідки та можливість зловживань

130. Застосування інноваційних технологій у фінансовому секторі приносить не лише значні та потенційно перетворюючі переваги, але й ризики ненавмисних наслідків, потенційної колізії з цілями, що суперечать одна одній, такими як конфіденційність, інтеграція, справедливі результати та вразливість до жорстокого поводження. Хоча штучний інтелект став

важливим інструментом у широкому діапазоні галузей, включаючи фінансові послуги, охорону здоров'я, роздрібну торгівлю та виробництво, де він покращив ефективність, зменшив витрати та пришвидшив дослідження та розробки, його дедалі ширше використання підняло безліч етичних та юридичних проблем, які викликали поширені заклики та численні напрямки роботи спрямовані на розробку відповідних державних та приватних стандартів та гарантій.

131. Рішення ШІ/ВК сильно відрізняються як за технологією, так і за використанням, і можуть представляти значні ризики. Потенційна відсутність пояснень та прозорості може погіршити здатність оцінювати точність рішення ШІ/ВК при виявленні підозрілих транзакцій та інших незаконних дій, тому неможливо встановити його ефективність як інструменту дотримання ПВК/ФТ. Крім того, хоча прийняття алгоритмічних рішень може здаватися об'єктивним способом подолання людської суб'єктивності та упередженості, дослідники виявляють, що багато алгоритмів штучного інтелекту відтворюють свідомі та несвідомі упередження розробників програм і застосовують їх у масштабі, щоб несправедливо виділити їх як підозрілу фінансову діяльність певних типів фізичних чи юридичних осіб, або складають характеристики ризиків та приймають рішення, якими відмовляють їм у доступі до певних фінансових продуктів та послуг.

132. Подібним чином, хоча надійні рішення щодо засобів цифрової ідентифікації особи можуть суттєво посилити ідентифікацію/верифікацію клієнтів при взятті на обслуговування та підтримати інші заходи CDD, а також допомогти в боротьбі з шахрайством та кіберзлочинністю та сприятимуть фінансовому включенню, рішення щодо засобів цифрової ідентифікації особи, які не забезпечують відповідних ризик-орієнтованих технічних гарантій та належного управління, представляють операційні ризики та потенційні непередбачувані наслідки. Вони також відкриті для умисних зловживань.

133. Якщо рішення щодо цифрової ідентифікації особи прийняті без урахування ризико-орієнтованого підходу, або пропорційності, вони можуть сприяти виключенню малозабезпечених громад. Наприклад, шукачі притулку можуть не мати можливості надати початкову документацію, яку іноді вимагають постачальники елетронних посвідчень, щоб створити таке електронне посвідчення особи. Існують подальші потенційні ненавмисні наслідки використання інструментів електронного посвідчення особи, зокрема щодо проблем, пов'язаних з потенційним розкриттям особистої інформації.

134. При використанні для фінансових послуг кількість персональних даних, що вимагається від клієнтів, збільшується, оскільки необхідний високий рівень впевненості щодо справжньої іденьтфікації осіб для цілей CDD та регулювання протидії відмиванню коштів. Однак, для належного забезпечення доступності фінансових послуг, інструменти цифрових ідентифікаторів повинні бути всеохоплюючими у своїй розробці та функціонуванні.[23]

[23] Консультативний комітет Конвенції про захист фізичних осіб щодо автоматичної обробки персональних даних Конвенція 108. Див. (Walshe, 2020 [20]) 24 (FATF, 2020 [8]), с. 35-45.

135. ФАТФ вимагає «надійних та незалежних електронних джерел документів, даних чи інформації». (ФАТФ, 2020 [8]) Це означає, що інструменти електронного посвідчення, що використовуються для проведення CDD, повинні покладатися на технологію, адекватне управління, процеси та процедури, що забезпечують належний рівень впевненості в тому, що система дає точні результати.

136. З цією метою слід визначити та зменшти правові, процесуальні та соціальні бар'єри в системах ідентифікації, приділяючи особливу увагу знедоленим людям та групам, які можуть опинитися під загрозою виключення з культурних, політичних чи інших причин (наприклад, жінки, діти, сільське населення, етнічні меншини, мовні та релігійні групи, мігранти, примусово переміщені особи та особи без громадянства). (Світовий банк, 2021 р. [16])

137. Операційні ризики та засоби зменшення ризику, включаючи ненавмисне виключення та конфіденційні ризики, обговорюються у Розділі V Посібника ФАТФ щодо цифрової ідентичності[24]. Зацікавленим сторонам рекомендується ознайомитися з цим документом. Крім того, оновлені «Принципи Світового банку щодо ідентифікації для сталого розвитку: назустріч цифровій ері» (Світовий банк, 2021 [16]) надають важливий набір принципів для використання при розробці, управлінні та використанні систем цифрової ідентичності з метою забезпеченя того, щоб вони були всеохоплюючими, базувалися на згоді, захищали приватне життя та інші права, а також були чесними та підзвітними.

Вставка 17. Виклики, що виникають у роботі з біометричними даними

Біометричні засоби цифрової ідентифікації особи можуть призводити до потенційного конфлікту з правами людини, здебільшого стосовно прав на приватне життя (наприклад, ЗДПЛ, стаття 12) та свободи від дискримінації (наприклад, ЗДПЛ, стаття 7). Цей потенційний конфлікт знайшов своє відображення у деяких законах та конвенціях, модернізованій Конвенції Ради Європи 108 (108+) та Загальному регламенті захисту даних ЄС (GDPR), який розглядає «біометричні дані» як особливу категорію даних, що вимагають більш високого рівня захисту з метою захисту людей від негативних наслідків його використання. Також було висловлене занепокоєння, що широкий спектр біометричних технологій та їх швидкий розвиток та використання для багатьох цілей можуть поставити під загрозу ключові права людини. (CoE, 2011 р. [17])

Якби рішення щодо цифрової ідентифікації базувались на біометричній основі та стали б обов'язковими, вони могли б стати широко розповсюдженим засобом ідентифікації, відстеження чи контролю, негативно впливаючи на право на приватне життя.

Тому біометричну інформацію, яку збирають приватні сторони, слід визнати захищеною інформацією з урахуванням правових

[24] (FATF, 2020[8]) ст.ст. 35-45.

стандартів, що вимагаються для таких даних відповідно до міжнародно-правових документів, та використання її обмеженим принципами пропорційності та необхідності.

4.4. Оцінка ефективності ПВК/ФТ технологічних рішеннь та способів усунення залишкових ризиків

138. Оскільки суб'єкти починають застосовувати нові технології після подолання зазначених вище проблем, для регульованих суб'єктів важливо постійно вивчати ефективність цих нових технологій для виявлення та боротьби з ризиками ВК/ФТ. Запроваджуючи оцінку ефективності, регульованим суб'єктам буде рекомендовано більше орієнтуватися на результат, а також забезпечувати відповідність впровадження нових технологій власним цілям і їх належне функціонування упродовж всього періоду експлуатації.

139. Ці вимірювання ефективності також слугуватимуть схемою зворотного зв'язку як для державного, так і для приватного сектора, з метою переналаштування власних технологічних рішень, якщо вони не відповідають запланованій меті. У той же час наявність чітких вимірювань допоможе наглядовим органам у оцінці нових технологій, що застосовуються регульованими органами.

140. Крім того, всі учасники повинні оцінити, чи існують залишкові ризики, які можуть виникнути із застосуванням нових технологій, або де є ключовий людський ресурс, який неможливо повністю замінити новими технологіями. Важливо забезпечити відсутність надмірної залежності від нових технологій, і там, де виявляються залишкові ризики, підконтрольні організації повинні продемонструвати обізнаність щодо цих ризиків та здатність управляти ними або реагувати на них, коли це необхідно.

141. Тим не менш, розробку таких показників ефективності та визначення прийнятного рівня ефективності або залишкових ризиків було визнано складним завданням, і існує можливість для обміну передовою практикою та/або керівними вказівками.

5. Створення сприятливого середовища для використання нових технологій у ПВК/ФТ

142. Респонденти погодились з тим, що ФАТФ та компетентні органи повинні робити якомога більше для подолання існуючих регулятивних та оперативних викликів впровадження нових технологій ПВК/ФТ. Однак важливо нагадати про ненавмисні наслідки усунення певних розбіжностей, присутніх у системі[25]. Наприклад, швидше виконання транзакцій означає витрачання менше часу на виявлення злочинної діяльності та посилення тиску на системи, що намагаються виявити та запобігти фінансовим злочинам.

143. Можливості та проблеми використання нових технологій для ПВК/ФТ можуть залежати більше від нормативних та політичних реакцій, ніж від додаткового технологічного розвитку. Обґрунтування використання нових технологій є актуальним як для державного, так і для приватного секторів, оскільки воно покращує загальні можливості ПВК/ФТ, здатність збирати та краще візуалізувати дані, контролювати злочинну діяльність, одночасно ефективніше використовуючи ресурси.[26]

144. Різні способи сприяння впровадженню технологій SupTech та RegTech обговорювались іншими (BIS, 2019 [18]), при цьому наголошувалося на важливості залученості вищого керівництва та необхідності забезпечення зрозумілості та пояснень. Здатність регульованих суб'єктів продемонструвати своїм керівникам переваги нових технологій є ключовою для їх належного прийняття та нагляду. Надалі основна увага повинна бути зосереджена на використанні технологій для вирішення визначених проблем та демонстрації прогресу у досягненні ефективності ПВК/ФТ.

145. Наявні й інші приклади співпраці наглядових органів з сектором, які підтверджують зусилля, спрямовані на подолання питань з приводу пояснень, зокрема, керівні вказівки для галузі щодо вирішення моделі «чорної скриньки». (MAS, 2018[18])

146. Деякі юрисдикції, як проілюстровано у Вставці 18, та переважно великі суб'єкти фінансового сектору вже почали застосовувати та використовувати нові технології як частину регулярного виконання вимог щодо вцідповідності, але наголошують, що їх справжня вартість буде досягнута лише тоді, коли вони будуть прийняті в повному масштабі та більшістю суб'єктів по всьому світу.

[25] (WEF, 2020[24]), ст. 21
[26] Згадане раніше. Стор.8

Вставка 18. Особистий кабінет на вебсайті Росфінмоніторингу

Росфінмоніторинг (Російська Федерація) активно розробляє Особистий кабінет (ОК) на своєму вебсайті як механізм комунікації з приватним сектором. ОК працює як IT-рішення, яке поєднує функції SupTech та RegTech. Спочатку ОК був розроблений для подання повідомлень про підозрілі операції та для розповсюдження списку визначених осіб.

У 2018 році після закінчення випробувального режиму ОК став обов'язковим для всіх суб'єктів звітування. На даний час це 80 тис. суб'єктів звітування, у тому числі 60 тис. ВНУП, які регулярно використовують ОК. Це виявилось ефективним інструментом зменшення ризику для приватного сектору.

ОК дозволяє передавати інформацію, створену в автоматизованій системі віддаленого моніторингу (ARMS), що використовується Росфінмоніторингом для розрахунку оцінки ризику з метою нагляду. Кожен суб'єкт звітування може отримувати інформацію про недоліки у своїй діяльності, що стосуються усіх аспектів внутрішнього контролю (подання повідомленнь про підозрілі операції, управління ризиками, використання списку визначених осіб тощо). Це дозволяє організаціям віддалено усувати недоліки.

Ця функція особливо актуальна для сектора ВНУП. Щорічно близько 2 тис. ВНУП вдається пом'якшити недоліки в результаті використання інформації, отриманої в ОК.

ОК працює як механізм зворотного зв'язку на повідомлення про підозрілі операції. Він надає фінансовим установам індекс якості потоку інформації, який включає ряд критеріїв, що визначають ефективність звітування про повідомлення про підозрілі операції суб'єктами звітування.

ОК дозволяє ПФР обмінюватися інформацією щодо ризиків та типологій ВК/ФТ, розповсюджувати результати національних та галузевих оцінок ризиків.

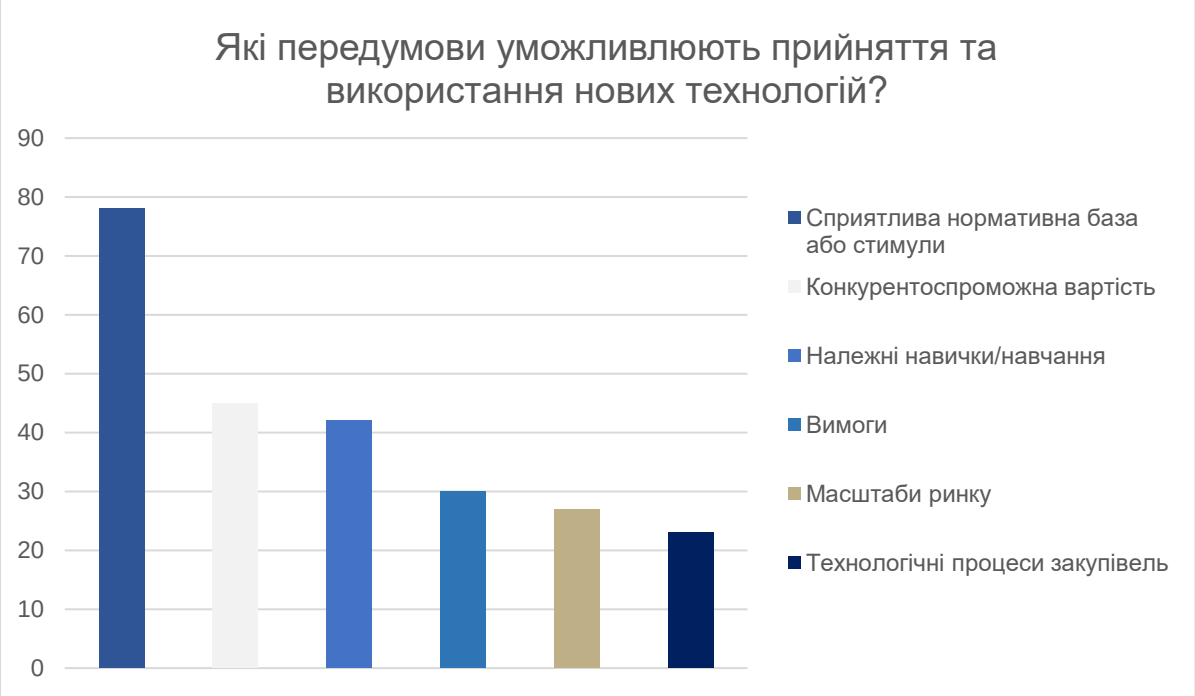
Функціональна мета ОК спрямована на підвищення рівня обізнаності приватного сектору із законодавчими вимогами. Дистанційне електронне навчання відіграє значну роль у цьому процесі.

Існує ряд навчальних курсів, розроблених Міжнародним навчально-методичним центром фінансового моніторингу та розміщених в Особистому кабінеті. Незабаром будуть запроваджені спеціальні курси щодо управління ризиками політичних діячів (PEP) та бенефіціарних власників.

У 2018 році було запущено ОК для керівників. Це сприяє обміну операційними ризиками між Росфінмоніторингом та наглядовими органами.

147. Сприятливе нормативне середовище, конкурентоспроможні витрати, досвід (навчання) та масштаби були визначені як ключові передумови до впровадження нових технологій, про що свідчить рисунок 4.

Рисунок 4. Які передумови уможливлюють прийняття та використання нових технологій?



148. Органи нагляду повинні застосовувати ініціативний підхід до технологій. Це сприятиме передумовам, які дозволять прийняти та використовувати нові технології, та допоможе членам у більш ефективному впровадженні стандартів ПВК/ФТ.

5.1. Технологічно активні наглядові органи [27]

149. Якщо наглядові органи та ФАТФ виявлять більш активну підтримку новим технологіям, це допоможе реагувати на занепокоєння стосовно невирішених проблем щодо ризиків та довіри, висловлені регульованими суб'єктами. Підтримка нових технологій вже здійснюється у багатьох юрисдикціях у формі технологічних ривків, акселераторів, інноваційних центрів та інших спільних ініціатив, де приватний сектор може розробляти, представляти та тестувати свої інструменти, а також отримувати відгуки про їх здатність застосовуватися до систем ПВК/ФТ (див. вставку 19 нижче). Ні ФАТФ, ні окремі керівники не повинні займати певної позиції по відношенню до окремих технологій або постачальників. Відповідальність за дотримання вимог ПВК/ФТ залишається за регульованими суб'єктами. Навпаки, роль ФАТФ та окремих національних органів влади повинна полягати в тому, щоб забезпечити інновації та нові підходи, що дозволяють ринку підтримувати

[27] Не слід плутати з підтримкою конкретних технологій або цифрових рішень. ФАТФ та наглядові органи повинні залишатися нейтральними до технологій.

надійні та перевірені технології в межах відповідного регулювання та нагляду та з урахуванням цілей державної політики, встановлених державними органами.

150. Хоча ці можливості заслуговують на увагу (*додаткові приклади в Додатку С*), респонденти вважають, що співпраця у цій галузі повинна виходити за рамки конкретних подій і мати форму постійних обмінів та співпраці між наглядовими та підконтрольними суб'єктами. Подолання страху перед мірами покарання або санкціями регулюючих органів вимагає більш постійної взаємодії, ніж взаємодія респондентів, наприклад, у формі повної реформи стратегії регулювання, яка пристосовується до цифрової ери, або конкретних вказівок щодо впровадження, як пропонується у Вставці 20.[28]

151. Таке сприйняття підтверджується звітом, поданим до Європейської комісії, де пропонується «Тридцять рекомендацій щодо регулювання, інновацій та фінансів» (ЕС, 2019 [19]), багато з яких підтверджуються висновками цього звіту. Серед них необхідність: роз'яснити пояснення та інтерпретацію штучного інтелекту та супутніх технологій, сприяти використанню цифрових посвідчень та скасувати паперові вимоги за замовчуванням, сприяти використанню технологічних фінансових послуг, а також розробляти та впроваджувати заходи для підтримки RegTech та SupTech.

Вставка 19. Інноваційні центри, приклади технологічних ривків та середовища для тестування (пісочниця)

BAFIN – Німеччина

BaFin ініційовано у 2020 році проєкт під назвою «TechBridge», який створив нові інституціоналізовані формати обміну для інноваторів, у тому числі з питань ПВК/ФТ. Основний компонент включав конфіденційні індивідуальні семінари, в яких брали участь новатор та група обраних експертів BaFin.

Семінари можуть проводитися вже на етапі досліджень та розробок інноваційного інструменту. Перш за все, нові інструменти повинні потенційно підняти нові наглядові та/або нормативні проблеми.

Подальші критерії відбору включають питання, чи можуть нові інструменти мати значний вплив на фінансовий ринок та потенційно потягнути за собою високі ризики.

Управління фінансової поведінки (FCA) - Великобританія

FCA вжила низку кроків, щоб заохотити відповідальне використання нових технологій для виконання зобов'язань у сфері ПВК/ФТ:

Регулятивна пісочниця FCA дозволяє регульованим суб'єктам випробовувати інноваційні продукти, послуги та бізнес-моделі в умовах реального ринку, забезпечуючи при цьому відповідні гарантії. Воно відкрилося для подання заявок з червня 2016 року, і зараз існує шість повних груп пісочниці. У всіх цих групах реугльовані суб'єкти перевірили інноваційні рішення у сфері протидії відмиванню коштів як щодо

[28] Див. Також досвід НКМА як приклад найкращої практики. (НКМА, 2020[26])

моніторингу транзакцій, так і щодо перевірки особи. Регульовані суб'єкти тісно співпрацюють із пісочницею, щоб забезпечити ідентифікацію та належне пом'якшення ризиків. Основними втручаннями є надання попередніх рекомендацій щодо застосування норм протидії відмиванню коштів; надання можливості регульованим суб'єктам повторювати свої бізнес-моделі; та ндання пвказівок регульованим суб'єктам через нормативні процеси, критичні для запуску нового бізнесу, послуги або продукту.

У липні 2017 року FCA опублікувала звіт, який вона замовила у PA Consulting, про те, як використовуються нові технології для впорядкування дотримання вимог протидії відмиванню коштів.

Надання чітких повідомлень у промовах про можливості, які технологія пропонує для поліпшення дотримання норм протидії відмиванню коштів, та заохочення FCA до експериментів та впровадження таких інновацій. Меган Батлер, виконавчий директор з нагляду - інвестицій, оптової торгівлі та спеціалістів FCA, розповіла про думку FCA, що звичні для використання технології можуть бути поворотним моментом у боротьбі з фінансовою злочинністю під назвою «застосування технологій проти фінансової злочинності».

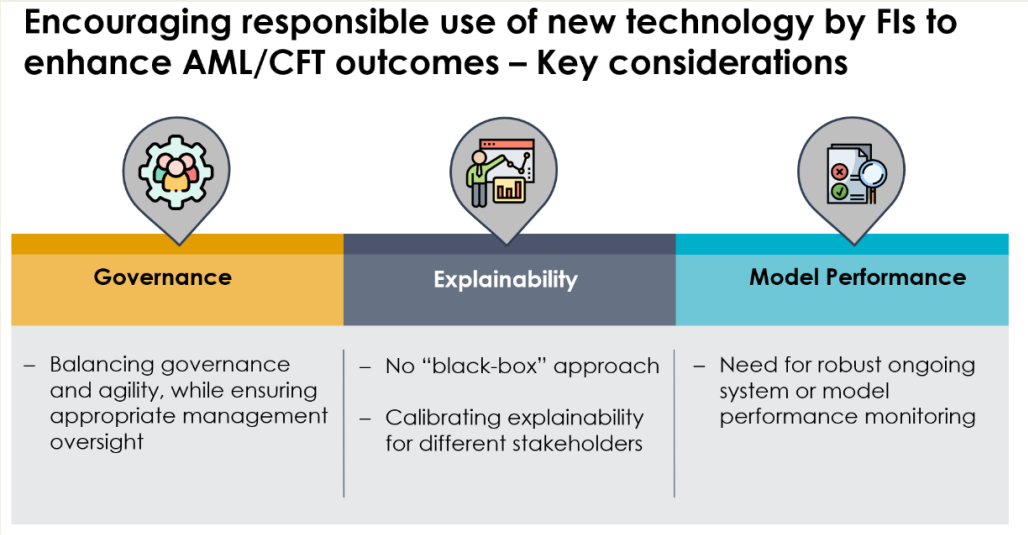
Заохочення взаємодії та обміну знаннями між наглядовими органами та постачальниками послуг RegTech щодо використання технологій регульованими суб'єктами. Проведення «TechFairs», на якому існуючі та потенційні учасники ринку демонструють рішення, що розробляються та застосовуються на ринку, щоб наглядові органи могли краще зрозуміти переваги, а також висловити занепокоєння. Активно заохочуючи дискусію про те, як нові технології, які у фінансових послугах або не використовуються в даний час, або використовуються не дуже широко, можуть забезпечити вигоду, наприклад, TechSprint 2019 для вивчення потенціалу PET для боротьби з фінансовою злочинністю та відмиванням грошей, демонструючи тим самим інституційну прихильність до прийняття нових рішень.

Орган фінансового нагляду Швеції

Finansinspektionen у 2018 році створив Інноваційний центр з метою надання рекомендацій, інформації та підтримання постійного діалогу з регульованими суб'єктами та стартапами, які пропонують інноваційні продукти та послуги у фінансовому секторі. Інноваційний центр також організовує семінари та інформаційні збори та бере участь у зовнішніх заходах, що стосуються інновацій у фінансовому секторі. Одним із поточних прикладів є участь у дискусіях за круглим столом з різними постачальниками послуг з приватного сектору в області віртуальних активів, яка швидко розвивається. Останнім часом темами для обговорення на таких заходах були відповідні нові нормативні акти та переглянуті Європейською Бізнес Асоціацією керівні принципи щодо заходів із зменшення та пом'якшення ризиків у сфері ПВК/ФТ. Finansinspektionen дотримується позиції, що фінансове регулювання не повинно перешкоджати розвитку та інноваціям у фінансовому секторі, за умови, що первинні завдання, надані Finansinspektionen, не ігноруються. Finansinspektionen позитивно ставиться до інновацій, які посилюють

захист споживачів, водночас сприяючи фінансовій стабільності, нормальному функціонуванню ринків та сталому розвитку.

Вставка 20. Валютно-фінансове Управління Сінгапуру



Разом з фінансовою галуззю Валютно-фінансове Управління Сінгапуру (MAS) розробило набір принципів для сприяння справедливості, етиці, підзвітності та прозорості (FEAT) у використанні штучного інтелекту (ШІ) та аналітики даних у фінансовому секторі. Цей набір принципів надає керівні вказівки фінансовим установам (FI) щодо відповідального використання штучного інтелекту та аналізу даних для посилення внутрішнього управління щодо обробки та використання даних.

Що стосується сфери ПВК/ФТ, MAS активно працює з сектори для вирішення ключових проблем у впровадженні аналітики даних про ПВК/ФТ. У 2019 році MAS співпрацювала з фінансовими органами через сингапурське партнерство у галузі ПВК/ФТ (ACIP) для обміну думками з питань аналізу даних. Під час семінару MAS та сектор досягли трьох ключових принципів для заохочення відповідального впровадження нових технологій - а саме управління, пояснюваність та ефективність моделі. Існував консенсус щодо того, що компромісу щодо надійного управління не повинно бути, оскільки фінансові установи застосовують більш інноваційні підходи до боротьби з фінансовими злочинами. Пояснюваність також повинна бути пріоритетом проекту, щоб система була ефективною, і її слід враховувати на початку розробки системи.

152. У більшості найновіших галузей сучасних технологій також були відзначені інноваційні підходи та спільний нагляд. Технологія розподіленого реєстру (TPP) була визначена такою, що має особливе значення у нагляді за віртуальними активами. Ряд ініціатив розроблено у всьому світі з метою підтримки розвитку цих технологій та створення сприятливого середовища, що дозволяє вести діалог із зацікавленими сторонами та долати деякі проблеми, пов'язані з інноваціями.

153. На відміну від транзакцій через звичайних посередників, таких як банки, операції з віртуальними активами (VA) на основі TPP часто проводяться без використання або участі посередників та інших суб'єктів звітування, і вони стикаються з перешкодами для досягнення цілей регулювання, особливо тих, що пов'язані з ПВК/ФТ, через труднощі з відстеженням та моніторингом операцій, які можуть виникнути через його унікальний характер. Через поширення віртуальних активів зменшення ризику за допомогою посередників може стати складним завданням у середньо- та довгостроковій перспективі.

154. Таким чином, серед операцій VA та фінансування, заснованого на блокчейні, одним з перспективних напрямків є вивчення шляхів забезпечення розробки протокольних та комп'ютерних кодів, що сприяють дотриманню ПВК/ФТ, зі збереженням переваг інновацій (Yuta Takanashi et. Al, 2020 [20]). Оскільки розробники, дизайнери протоколів та сторонні постачальники явно не підпадають під зобов'язання щодо ПВК/ФТ згідно з Рекомендаціями ФАТФ, ФАТФ повинна розглянути питання про необхідність додаткових дискусій з іншими зацікавленими сторонами, наприклад, щодо ролі постачальників технологій та зростаючого використання блокчейну у фінансах у сфері ПВК/ФТ для забезпечення відповідності та ефективності стандартів ФАТФ в середньостроковій перспективі.

155. Зрештою, ФАТФ також визначила «*Запропоновані заходи щодо підтримки використання технологій у сфері ПВК/ФТ*» (див. Додаток B), які сприяють застосуванню Принципу Сан-Хосе 2017 року щодо *впровадження* позитивних та *відповідальних інновацій*. У цих Заходах зазначається, що нові технології для ПВК/ФТ повинні розроблятися та впроваджуватися таким чином, щоб відображати загрози, а також можливості, забезпечуючи сумісність їх використання з міжнародними стандартами захисту даних та приватного життя, а також кібербезпеки.

Вставка 21. Наглядові органи та ТРР

JFSA – Японія

Мережа Ініціативи у Блокчейн-Управлінні "BGIN" була створена в березні 2020 року, і JFSA внесла активний вклад у її реалізацію. Ця ініціатива вирішує проблеми децентралізованої фінансової системи, підкріпленої технологіями блокчейну, застосовуючи так званий підхід з участю багатьох зацікавлених сторін. Важливість змісцення діалогу між зацікавленими сторонами була підтримана FSB (FSB, 2019 [21]) і отримала позитивні відгуки G20 під головуванням Японії в 2019 (G20, 2019 [22]). Дана концепція має на меті сформувати єдине розуміння питань, з якими зацікавлені сторони стикаються через діалог в рівних умовах між різними зацікавленими сторонами, такими як контролюючі органи, розробники технологій, суб'єкти звітування, наукові кола тощо, враховуючи обмеження загальноприйнятої нормативної бази: повідомлення в односторонньому порядку від контролюючих органів до суб'єктів звітування.

BGIN пояснює свої цілі (BGIN, n.d. [23]) як «взяти на себе провідну роль у розробці корисного врядування, де зацікавлені сторони розвивають спільне розуміння, посилюють діалог та працюють разом, і здійснюють реальний позитивний вплив на екосферу та суспільство в цілому» і орієнтовно фокусується на:

- створенні відкритої, глобальної та нейтральної платформи для діалогу із зацікавленими сторонами,
- розвитку спільної мови та взаєморозуміння серед зацікавлених сторін з різними точками зору, та
- створенні навчальних зв'язків шляхом постійного надання надійних документів та кодів на основі підходу з відкритих джерел.

BGIN займається різними питаннями, пов'язаними з діяльністю ФАТФ, включаючи, наприклад, визначення потенційних нормативних підходів щодо ПВК/ФТ в DeFi (децентралізоване фінансування) з урахуванням нових технологій та розвитку ринку. ФАТФ та її членам може бути корисно брати участь у її діяльності в якості місця для посилення діалогу з різними зацікавленими сторонами, включаючи тих, хто розробляє технології, і з доступом до яких у контролюючих органів зазвичай виникають проблеми. Така безперервна взаємодія із зацікавленими сторонами, як зазначено у звіті FSB, врешті-решт забезпечить дотримання вимог ПВК/ФТ, уникаючи стримування інновацій та сприятливих умов.

5.2. Прикінцеві зауваження

156. Цей звіт пропонує огляд на високому рівні можливостей та викликів нових технологій для ПВК/ФТ, з наданням, де це можливо, прикладів існуючих найкращих практик та/або конкретних проблем. Висновки цього звіту не є всеосяжними, і є можливість для вдосконалення взаємозв'язку між стандартами ФАТФ та цифровою трансформацією.

157. Технологічні інновації відкривають великий потенціал для ефективності ПВК/ФТ. Однак це може також призвести до посилення фінансового виключення певних верств суспільства - людей похилого віку, сільських громад тощо, а також створити перешкоди суспільству, зокрема з точки зору прав людини, демократії та верховенства права. ФАТФ пам'ятає, що подальші перешкоди можуть виникнути внаслідок надання безвідповідальної або неправильної підтримки суб'єктів та надмірного покладання на нові технології.

158. ФАТФ закликає юрисдикції співпрацювати між собою та з суб’єктами приватного сектору для розгляду цілісного підходу до нових технологій, беручи до уваги його потенціал, а також його обмеження.

Додатки

- Додаток A – Словник
- Додаток B - Пропоновані заходи щодо підтримки використання технологій у сфері ПВК/ФТ
- Додаток C - Тематичні дослідження SupTech
- Додаток D - Додаткові тематичні дослідження RegTech щодо використання нових технологій ПВК/ФТ приватним сектором

Додаток А: Словник

- **Розширена аналітика**: Розширена аналітика відноситься до автономної або напівавтономної перевірки даних або вмісту, де використовуються складні технічні засоби та цифрові інструменти, які, як правило, виходять за межі традиційної бізнес-аналітики, щоб глибшие проаналізувати інформацію, зробити прогнози або сформувати рекомендації. До передових аналітичних методів належать такі, як видобуток даних/тексту, машинне навчання, узгодження шаблонів, прогнозування, візуалізація, семантичний аналіз, аналіз тональності тексту, мережевий та кластерний аналіз, багатовимірна статистика, аналіз графіків, моделювання, обробка складних подій, нейронні мережі. Розширена аналітика зазвичай вдається до використання великої кількості даних.
- **Застосунок:** Застосунок – це комп'ютерне програмне забезпечення, призначене для того, щоб допомогти користувачеві виконувати певні завдання.
- **Інтерфейс прикладного програмування (API):** ***API*** **-** це набір визначень та протоколів для побудови та інтеграції прикладного програмного забезпечення. API дозволяють цифровим продуктам або послугам легко комунікувати з іншими продуктами та послугами.
- **Алгоритм:** Комп’ютерний алгоритм - це набір покрокових інструкцій для виконання конкретного завдання.
- **Штучний інтелект (ШІ):** Система ШІ - це машинна система, яка може для певного набору визначених людиною цілей робити прогнози, рекомендації або приймати рішення, що впливають на реальне або віртуальне середовище (і працювати з різним рівнем автономності). (OECD, 2020 [24]) Мета ШІ полягає в тому, щоб дати комп’ютерам можливість автоматизувати деякі аспекти аналізу, потенційно заощаджуючи людську працю для більш складних завдань та отримуючи результати, яких люди можуть не досягти. В рамках ШІ існує декілька компонентних технологій, всі з численними додатками. Немає єдиної думки щодо того, що таке «мислення» та «інтелект», а що є «цілком автономним», також існує декілька категорій ШІ, але загалом системи ШІ будують «розумні машини», що поєднують у собі спрямованість на предмет, інтелект та пристосованость. На даний час машинне навчання є найбільш звичною та розвиненою формою ШІ.
- **Великі дані:** Рада з фінансової стабільності визначає великі дані як «величезний обсяг даних, що генерується внаслідок все більшого використання цифрових інструментів та інформаційних систем», таких як дані про фінансові операції, дані соціальних мереж та машинні дані (наприклад, Інтернет речей, дані комп’ютера та мобільного телефону. (FSB, 2017[25])
- **Чорна скринька**: Чорна скринька стосується ШІ/машинного навчання та інших технологій, які є непрозорими, неінтуїтивними та не надають адекватної інформації щодо прийняття рішень та прогнозів/результатів – тобто, технології чорної скриньки не можна пояснити.
- **Бенчмаркінг:** Бенчмаркінг - це підхід до визначення фактичних та відносних можливостей технологічного процесу, продукту чи послуги та виявлення прогалин у продуктивності шляхом тестування їх на основі найкращих показників, які досягаються для функції, завдання чи цілі - в межах конкретного суб'єкта або організації, загальногалузевої або досягнутої іншою галуззю - з використанням жорстких даних про ефективність, виміряних заданими критеріями порівняльного

аналізу. Бенчмаркінг може бути використаний для вимірювання ефективності нових технологій у порівнянні із застарілими системами або однієї нової технології на противагу альтернативним новим технологіям.

- **Спільна аналітика:** Щодо спільної аналітики, то дані не переміщуються в централізоване місце, щоб аналізувати їх разом з іншими ресурсами даних. Натомість аналітичні інструменти приходять до даних, а не навпаки. Це полегшує захист даних та контроль за тим, хто з якими цілями отримує доступ до яких даних.
- **Кібербезпека:** Кібербезпека, ширший термін, ніж безпека даних, відноситься до всебічного процесу захисту даних та систем переміщення, зберігання та автентифікації цих даних.
- **Пул/пул даних:** Пул даних відноситься до процесу, коли цифрові дані з різних джерел поєднуються, що призводить до більш повного та практично використовуваного набору даних для аналізу (у тому числі кількома сторонами). Ці пули організовані централізовано.
- **Безпека даних:** Захист даних відноситься до процесу захисту даних від несанкціонованого доступу та пошкодження даних упродовж їх життєвого циклу. Він включає шифрування даних, хешування, токенізацію та ключові практики управління, які захищають дані у всіх програмах та платформах. Безпека даних вужча, ніж кібербезпека.
- **Стандартизація даних:** Стандартизація даних - це процес перетворення даних в єдиний формат, що дозволяє користувачам обробляти та аналізувати їх. Стандартизація даних має важливе значення для обробки великих даних та вдосконаленої аналітики, а також для розробки та застосування інших інноваційних цифрових інструментів та методологій. Наприклад, фінансові дані можуть різнитися як всередині суб'єктів господарювання, так і між ними; стандартизація даних перетворює їх у загальноприйняту форму, що дозволяє розвинути масштабну аналітику.
- **Системи/рішення цифрової ідентифікації (Digital Identity - ID):** Системи/рішення Digital ID - це системи ідентифікаційних даних або продукти та послуги, що здійснюють процес ідентифікації/перевірки особи (фізичної чи юридичної) особи, прив’язки підтвердженої ідентифікації до цифрових ідентифікаційних даних та використання цифрових посвідчень та потенційно інших факторів автентифікації для встановлення (підтвердження) того, що особа, яка надає ідентифікаційну інформацію, є людиною, чия особа перевірена і підтверджена (тобто, є тією особою, якою вона себе заявляє).
- **Технологія розподіленого реєстр (ТРР) (також відома як блокчейн):** ТРР відноситься до типу технологічного протоколу, який забезпечує одночасний доступ, перевірку та оновлення незмінного реєстру (цифрового запису), розподіленої між кількома комп'ютерами (і, як правило, між різними об'єктами або місцями) - тобто, ТРР створює розподілену цифрову базу даних.
- **Глибинне навчання (DL):** DL - це вдосконалений тип машинного навчання, в якому штучні нейронні мережі (алгоритми, натхненні людським мозком) на численних (глибоких) рівнях навчаються на великих обсягах даних вкрай автономно. Алгоритми DL виконують завдання неодноразово, кожного разу трохи підправляючи його для поліпшення результату, дозволяючи машинам вирішувати складні проблеми без участі людини.

- **Діджиталізація:** Діджиталізація - це використання цифрових технологій та оцифрованих даних для зміни бізнес-моделі, впливу на те, як виконується робота, перетворення способу взаємодії клієнтів та компаній та надання нових можливостей для отримання доходу та вартості.
- **Діджитизація:** Діджитизація - це перетворення даних, інформації, тексту, зображень, звуку чи інших зображень в аналоговій формі в цифрову форму (тобто двійковий код), яку можна обробити комп'ютером.
- **Динамічні дані:** Динамічні дані відносяться до безперервного цифрового потоку точок даних в режимі реального часу, які, як відомо, знаходяться в постійному русі, так що набір даних постійно змінюється з часом, на відміну від статичних або постійних даних, на які час здебільшого не впливає.
- **Пояснюваність:** У контексті нових технологій пояснюваність означає, що технологічні процеси, рішення чи системи можуть бути пояснені, зрозумілі та враховані. Пояснюваність забезпечує адекватне розуміння того, як рішення працюють та приносять результати. Пояснюваність є основною умовою довіри та відповідального використання. Пояснювана технологія ШІ забезпечує прозорість даних, змінних та моментів прийняття рішень, що використовуються для досягнення результату.
- **FinTech:** FinTech в основному стосується використання нових цифрових технологій у фінансовому секторі для будь-яких найрізноманітніших цілей. Спочатку «FinTech» основним чином відносився до застосування технологічних інновацій для надання нових фінансових продуктів та послуг, спрямованих на клієнтів [наприклад, мобільні платіжні рішення, кредитування в Інтернеті, алгоритмічні заощадження та інструменти інвестування, платежі у віртуальній валюті, залучення капіталу (краудфандінг) та отримання депозитів (дистанційний збір чеків, мобільний банкінг)]. Зараз FinTech також охоплює використання нових технологій для забезпечення автоматизованих функцій середнього та допоміжного бізнесу, таких як використання алгоритмів, великих даних, штучного інтелекту та машинного навчання, а також аналітики посилань для оптового оформлення, розрахунків та іншого посередництва оптових продажів, для, наприклад, цінних паперів, деривативів, оптового фінансування та платежів, а також діяльність із дотримання законодавства (див. визначення RegTech нижче) Інші програми ще потрібно розробляти.
- **Нечітка логіка:** Нечітка логіка - це підгрупа ШІ, яка приймає відкритий, неточний спектр даних (неточний ввід) і обробляє декілька значень таким чином, що дає результат, який включає цілий ряд проміжних можливостей між ТАК та НІ (наприклад, звичайно так, можливо так, не можу сказати, можливо ні, звичайно ні). Системи нечіткої логіки дають певний результат у відповідь на неповні, неоднозначні, спотворені або неточні (нечіткі) вхідні дані, симулюючи прийняття людських рішень більш точно, ніж звичайна логіка так/ні. Нечітка логіка може бути реалізована в апаратному, програмному забезпеченні або в поєднанні обох.
- **Інтернет речей (IoT):** Глобальна мережа всіх пристроїв та машин з підтримкою Інтернету, які підключені до Інтернету і можуть збирати, надсилати, ділитися даними та діяти за допомогою вбудованих датчиків, процесорів та комунікаційного обладнання без взаємодії людини. IoT генерує величезну кількість даних у режимі реального часу, які можна проаналізувати та

використовувати для створення бажаних дій або результатів бізнесу (див. Великі дані).

- **Сумісність:** відноситься до здатності різних систем інформаційних технологій та програмних забезпечень взаємодіяти, обмінюватися даними та використовувати інформацію безперешкодно в режимі реального часу, що дозволяє всім учасникам працювати в усіх системах.
- **Машинне навчання:** Машинне навчання - це тип (підгрупа) штучного інтелекту, який «навчає» комп'ютерні системи для вивчення даних, виявлення закономірностей та прийняття рішень із мінімальним втручанням людини. Машинне навчання передбачає розробку послідовності дій для автоматичного вирішення проблеми за допомогою досвіду та вдосконалення алгоритмів розпізнавання образів з обмеженим втручанням або без участі людини - тобто, це метод аналізу даних, який автоматизує побудову аналітичної моделі.
- **Машиночитабельний регламент:** Машиночитабельний регламент замінює правила, написані природною юридичною мовою, на комп'ютерний код, що дозволяє використовувати штучний інтелект для цілей нормативної звітності.
- **Обробка природної мови (NLP):** NLP - це розділ ШІ, який дозволяє комп'ютерам розуміти, інтерпретувати та використовувати людську мову. NLP дозволяє людям розмовляти з машинами.
- **Технології підвищення рівня приватності:** «Спеціалізовані криптографічні можливості, які дозволяють проводити обчислення базових даних, без того, щоб власник даних обов'язково розкривав ці базові дані. Ця ж технологія може гарантувати, що власник даних не може бачити пошуковий запит, при цьому запит та результати залишаються зашифрованими (або не розголошуються) і видимими лише для запитувача». (Maxwell, 2020 [26]) Отже, цей термін охоплює безліч технологій, що використовують шифрування, і були б корисними, перш за все, для забезпечення конфіденційності при використанні даних.
- **Аналітика в реальному часі:** Аналітика в реальному часі - це процес машинного навчання, в якому система обробляє та аналізує дані, які завантажуються миттєво і майже відразу (майже в реальному часі), генерують істотні результати (наприклад, інформацію, прогнози або рішення).
- **Дані в реальному часі (RTD):** RTD **-** це інформація, яка доставляється відразу після збору, забезпечуючи своєчасність наданої інформації. RTD забезпечує аналітику в режимі реального часу і може бути динамічним або статичним (наприклад, нові данні, що вказують конкретне місце розташування в певний час).
- **Технологія нормативного регулювання (RegTech):** RegTech **–** це підгрупа FinTech, яка використовує нові технології, щоб відповідати нормативним вимогам, більш ефективно та дієво, ніж існуючі можливості.
- **Відповідальна інновація:** Інновація є відповідальною, коли вона є придатною для певних цілей та відповідає чинним нормативним вимогам, включаючи ПВК/ФТ, захист споживачів, кібербезпеку та приватного життя.
- **Розумні машини:** Комп'ютерні системи апаратного та програмного забезпечення, що використовують алгоритми ШІ. Розумні машини призначені для прийняття рішень, часто з використанням даних в режимі реального часу. На відміну від

пасивних машин, які здатні лише до механічних або заздалегідь визначених реакцій, розумні машини використовують датчики, цифрові дані та віддалені вхідні данні, поєднують інформацію з цих різних джерел, миттєво аналізують ці данні і діють на основі отриманих даних. Розумні машини імітують людський інтелект, використовуючи вдосконалений обчислювальний процес, щоб зробити висновки на основі їх миттєвого аналізу.

- **Статичні дані:** статичні дані стосуються фіксованого набору даних - даних, які залишаються незмінними після їх збору.
- **Контрольоване навчання:** Контрольоване навчання - це процес машинного навчання, який навчає алгоритми моделям прогнозування, подаючи вхідні дані алгоритму з відомими результатами - тобто, контрольоване навчання вчить алгоритми на прикладах. Пара введення/виведення (марковані дані) забезпечує зворотний зв'язок для алгоритму, який використовує набір навчальних даних для коригування моделі з метою мінімізації помилок. Наприклад, навчальний набір може містити зображення різних видів тварин з позначкою, пов’язаною з кожним зображенням, що дозволяє алгоритму порівнювати прогнозовану позначку із правильною. Контрольоване навчання використовує набір даних перевірки для вимірювання прогресу алгоритму у вивченні моделі та набір тестових даних для оцінки ефективності моделі на раніше небачених даних, щоб визначити, чи ефективно модель засвоїла свої навчальні дані та чи може узагальнити їх до нових даних.
- **Технологія нагляду (SupTech):** SupTech - це використання інноваційних технологій наглядовими органами для підтримки нагляду та аналізу.
- **Навчання без нагляду (тобто машинне навчання без нагляду):** Навчання без нагляду - це процес машинного навчання, який дозволяє алгоритмам аналізувати та групувати *немарковані* набори даних, щоб виявляти приховані закономірності, групування даних чи відхилення без втручання людини. Алгоритм аналізує наявні дані та визначає кореляції та взаємозв'язки без відповіді, роблячи висновки та групуючи подібні речі на основі необмеженого спостереження та інтуїції. По мірі збільшення кількості даних, яким піддається алгоритм, його моделювання стає більш точним та вдосконаленим.

Додаток B - Пропоновані заходи щодо підтримки використання технологій у сфері ПВК/ФТ

Відповідальне використання нових технологій, включаючи цифрові ідентифікатори та найсучасніші рішення для моніторингу та аналізу транзакцій (включаючи спільну аналітику), може допомогти ефективному впровадженню стандартів ФАТФ державним та приватним секторами, а також сприяти фінансовому включенню.

Наступні принципи активно просувають принцип Сан-Хосе *розвивати позитивні та відповідальні інновації,* затверджені ФАТФ у 2017 році. Нові технології для ПВК/ФТ повинні розроблятися та впроваджуватися таким чином, щоб відображати загрози та можливості, забезпечуючи сумісність їх використання з міжнародними стандартами захисту даних, конфіденційності та кібербезпеки.

1. Створити сприятливе середовище як урядом, так і приватним сектором для відповідальних інновацій задля підвищення ефективності ПВК/ФТ:

i. *Інноваційні рішення, що сприяють впровадженню заходів ПВК/ФТ, включаючи оцінку ризиків, CDD та інші вимоги, а також посилюють їх нагляд та перевірку.*
ii. *Передові практики оновлення внутрішніх застарілих систем або заміни їх новими технологіями.*
iii. *Відповідні запобіжні заходи та особливості для нових рішень щодо ПВК/ФТ, включаючи: пояснюваність та прозорість процесів та результатів; нагляд з боку людей; повага до приватного життя та захисту даних; сильна кібербезпека; та узгодження зі світовими, національними та технічними стандартами та найкращими практиками.*

2. Забезпечте конфіденційність та захист даних при впровадженні нових технологій:

i. *Переконатися, що існує діюча правова основа для обробки персональних даних при впровадженні нових технологій.*
ii. *Захищати особисту інформацію відповідно до національних та міжнародних правових рамок.*
iii. *Обробляти дані для явних, конкретних та законних цілей, відповідно до національного та міжнародного законодавства.*
iv. *Підтримувати відповідальний розвиток та впровадження інноваційних технологій збереження конфіденційності, щоб забезпечити надійний обмін та аналіз інформації щодо ПВК/ФТ, одночасно зберігаючи конфіденційність.*

3. Сприяти інноваціям у сфері ПВК/ФТ, які підтримують фінансове включення відповідно до задуму.

i. Зменшити перешкоди на шляху фінансового включення через розробки та впровадження інноваційних рішень.

ii. Забезпечити відповідальні інновації, що відповідають меті ФАТФ щодо сприяння фінансовому включенню.

4. Розробляти та поширювати політику та нормативні підходи до інновацій, які є гнучкими, нейтральними до технологій, заснованими на результатах та відповідають ризик-орієнтованому підходу.

i. Розглядати вплив нових технологій цілісно, в контексті структурних та організаційних змін, які їх супроводжують, їх можливі непередбачувані наслідки та їх загальний вплив на ефективність ПВК/ФТ та фінансове включення.

ii. Випускати та/або оновлювати чіткі політичні заяви, вказівки, випадки використання, найкращі практики чи правила, якщо це необхідно для інформування та заохочення відповідального використання нових технологій для ПВК/ФТ.

iii. Консультуватися з колегами та регульованими суб'єктами, щоб інформувати про відповідну політику та процеси прийняття рішень.

5. Здійснювати інформований нагляд

i. Накопичувати досвід у галузі нових технологій, щоб забезпечити обгрунтоване регулювання та нагляд за їх використанням, у тому числі для конкретних цілей дотримання ПВК/ФТ.

ii. Визначити прямо сформульоване, чітко визначене використання нових технологій для нагляду та вивчення ПВК/ФТ.

iii. Розуміти ризики та вигоди, пов'язані з новими технологіями, та відповідні заходи щодо зменшення ризиків, які зберігають їх переваги.

iv. Використовувати технології для посилення нагляду у сфері ПВК/ФТ.

6. Просувати та сприяти співпраці

i. Співпрацювати та координувати свою діяльність з усіма відповідними органами влади для сприяння всебічному, скоординованому підходу до розуміння та вирішення ризиків та вигод від використання нових технологій для ПВК/ФТ, включаючи органи захисту даних та конфіденційності.

ii. Розглянути можливість створення середовищ для співпраці для сприяння міждержавному та/або державно-приватному дослідженню та розробці нових технологій та інноваційних рішень.

iii. Брати участь у міжнародних заходах з розробки глобальних принципів, що регулюють використання нових технологій для ПВК/ФТ, щоб допомогти забезпечити їх узгодження з правами людини, вдосконалення впровадження глобальних заходів з ПВК/ФТ, кібербезпеки, заходів щодо конфіденційності та захисту даних, а також технічних стандартів та рамок довіри.

Додаток С – Тематичні дослідження SupTech

Бразилія

Інтегрована система підтримки нагляду Центрального банку Бразилії (SisCom, APS-Siscom з 2018 року) - це веб-система 2014 року, що підтримується потужною методологією, яка дозволяє взаємодіяти з суб'єктами нагляду (SE) в безпечному середовищі та сприяє наглядовій роботі в таких аспектах:

- Простий та безпечний спосіб запитувати та отримувати від SEs правила, посібники, управлінські звіти, звіти про аудит, файли щодо KYC (Знай свого клієнта) конкретних клієнтів та конкретних транзакцій, а також відповіді контрольованих суб'єктів, записані в систему;
- Особливості взаємодії під час перевірки з метою з'ясування будь-якого питання та надсилання запиту щодо додаткової інформації чи пояснень;
- Стандартизація процедур перевірки, що дозволяє одночасно проводити різні перевірки;
- Шаблони перевірок: органи нагляду BCB можуть створювати спеціальні форми заявок для груп SE, сектору SE або SE, зокрема, які зберігаються у портфоліо для подальшого використання. Функція запиту дозволяє органу нагляду знати, до скількох SE було надіслано будь-який запит;
- Підготовка звітів: APS-Siscom автоматично забезпечує звіти з нагляду, які можна легко зібрати як досьє для аудиту;
- В кінці перевірки про недоліки та порушення повідомляється через Систему, а SE повинні подавати, також через APS-SisCom, план виправлення, що підлягає затвердженню керівником;
- Усі терміни виконання контролюються та сигналізуються APS-SisCom, який надає актуальний підрахунок недоліків та порушень відповідно до стану їх завершення у звіті про бізнес-аналітику;
- Функції запитів дозволяють органу нагляду збирати інформацію про кожну перевірку, проведену на певних SE, з метою відстеження прогресу.

У 2018 році Siscom було включено до нової платформи нагляду BCB SisAPS, яка інтегрує кілька систем та баз даних. SisAPS було впроваджено для інспекторів, органів нагляду та керівників, і забезпечувала вікно записів про те, що команда проводить або проводила під час кожної перевірки, а також управлінську інформацію та звіти про моніторинг.

APS-SisCom забезпечила надзвичайний приріст продуктивності для наглядових груп BCB, полегшивши процедури нагляд та дозволивши BCB не здійснювати трудомістких відвідувань SE.

Дані, зібрані APS-Siscom, також використовуються в методології, яка дає можливість BCB сегментувати та контролювати банки та небанківські фінансові установи (NBFI) за різними категоріями ризику. Кількісні та якісні дані обробляються та аналізуються органами нагляду, і забезпечують їм різні перспективи:

- рівень відповідності конкретним нормативним вимогам;
- оцінка ризику з використанням рейтингової категорізації.

Як результат, цей інструмент та методологія забезпечують ефективний нагляд ПВК/ФТ за сотнями середніх та малих SE, розповсюджених по всій великій території Бразилії.

НКМА: Роль регулятора в заохоченні використання мережевої аналітики

Тісно співпрацюючи з банками, Гонконгський валютний орган (НКМА) протягом останніх кількох років вжив низку кроків, щоб заохотити розвідку та відповідальне прийняття програмних додатків ПВК/ФТ Regtech, в тому числі через наглядову пісочницю і чат Fintech, та Форум Regtech з питань ПВК/ФТ у листопаді 2019 року. Серед багатьох застосунків, НКМА визначила розробку програм мережевої аналітики як один із наглядових пріоритетів НКМА, який підтримує банки для збільшення цінності результатів, досягнутих за рахунок державно-приватного партнерства Гонконгу - Групи з питань розвідки щодо шахрайства та відмивання грошей. Протягом 2020 року НКМА залучає банки для кращого розуміння факторів та залежностей, що впливають на застосунки мережевої аналітики, що допомагає НКМА як наглядовому органу підготувати відповіді, особливо тим банкам, які запитують: «*Як нам підготуватися до початку використання мережевої аналітики*?»

НКМА нещодавно поділився тематичним дослідженням банку, який вже кілька років вивчає потенційні застосунки мережевої аналітики. (НКМА, 2021 [27]) Прийняття банком аналітики відстежується з 2013 року, де детально описується, як воно використовувалося для підвищення здатності банку виявляти мережу, що демонструє високий ризик ВК/ФТ. НКМА продемонструвала, як цей банк долає певні виклики та деякі отримані ним результати.

Щоб продовжувати виконувати план дій для прискорення прийняття у банківському секторі, НКМА відзначив Regtech як ключовий акцент у своїй наглядовій програмі ПВК/ФТ на 2021 рік та докладно розповів, як він буде використовувати деякі практики, описані в його нещодавній публікації, для формування прийнятності ключових технологій та створення умов для вивчення та використання Regtech всіма банками у роботі з ПВК/ФТ, включаючи аналітику мережі.

Валютно-фінансове Управління Сінгапуру (MAS)

Постановка проблеми

MAS здійснює нагляд за тим, як фінансові установи управляють ризиками відмивання грошей та фінансування тероризму (ВК/ФТ). Для підвищення нашої наглядової ефективності ми проводимо нагляд за ризиками для виявлення системних ризиків та націлення на зони з підвищеним ризиком та фінансовими установами для більш пильного наглядового контролю. Наші фінансові служби подають повідомлення про підозрілі операції (STRs) щодо потенційно незаконних потоків коштів та питань фінансової злочинності, і вони містять корисну інформацію для наших цілей спостереження за ризиками. Складні типології часто включають кілька облікових записів у декількох фінансових установах, і це може проявлятися в декількох STRs, поданих протягом певного періоду. Тому ми розробили інструмент мережевої аналітики STR, який допоможе нам провести зв'язок між фінансовими установами протягом тривалого часу.

Підсумки та результати

Використання інструменту мережевої аналітики STR допомогло MAS визначити відповідні кластери фізичних/юридичних осіб, які виявляли підозрілу поведінку, а також фінансових служб, задіяних для нашого наглядового аналізу та перевірки. Це допомогло посилити нашу здатність визначати пріоритети та націлюватись на ризики під час нагляду у сфері ПВК. Підсумки та нові ризики, виявлені в результаті аналізу мережі, також передаються фінансовому сектору через різні платформи, включаючи наше галузеве партнерство у сфері ПВК/ФТ (ACIP), галузеві семінари або через консультативні записки та наглядові вказівки для всіх фінансових служб. Ці проекти, засновані на даних, підвищили рівень обізнаності про ризики в галузі, і в свою чергу спонукали фінансові органи пришвидшити прийняття інноваційних підходів до аналізу даних для боротьби з фінансовою злочинністю.

Окрім досягнення наших наглядових цілей, інформація, отримана за допомогою інструменту аналітики мереж STR, також допомогло в наших національних зусиллях по боротьбі з фінансовою злочинністю. У Сінгапурі існує міжвідомчий комітет, який об'єднує відповідні правоохоронні та наглядові органи для розслідування та розробки планів зменшення ризику для пріоритетних справ у справах щодо ВК/ФТ. Декілька питань щодо мереж, виявлених за допомогою нашої аналітики мереж STR, були передані до цього міжвідомчого комітету для обговорення та узгоджених дій між агенціями.

Вхідні дані для нашого аналізу мережі на початковій фазі включають в основному інформацію зі структурних полів даних в STRs. Ми перебуваємо в процесі вдосконалення набору даних для збільшення впливу нашого інструменту мережевої аналітики. По-перше, ми розробляємо моделі обробки природних мов (NLP) для вилучення інформації з неструктурованих текстових даних

всередині STR, наприклад, викладення фактів, що пояснюють незвичний характер транзакцій замовника та взаємовідносини між контрагентами для потрапляння у наш аналіз мережі. По-друге, наш інструмент аналітики також почав отримувати більше даних про транзакції та інформацію про профіль компаній. Ці вдосконалення зміцнять нашу здатність виявляти приховані зв'язки, виявляти та визначати пріоритети проблем системного ризику для наглядових та міжвідомчих заходів.

Малайзія

Структура пісочниці для сприяння ефективному впровадженню нормативних вимог e-KYC

Пісочниця регулювання фінансових технологій (Пісочниця), створена Банком Негара Малайзія (BNM), відіграє ключову роль у просуванні інновацій у фінансовій галузі з 2016 року. Вона служить ефективною платформою для BNM для моніторингу потенційного впливу інновацій на галузь до встановлення формальних нормативних вимог до галузі.

Переваги Пісочниці проявляються, серед іншого, у зростанні інноваційної бізнес-моделі в установах, які надають грошові послуги (MSB). До 2017 року малайзійським учасникам MSB не дозволялося здійснювати будь-які транзакції без особистого контакту з новими клієнтами, якщо тільки спочатку не були встановлені ділові відносини з клієнтом та не були проведені заходи належної перевірки клієнтів. За допомогою Пісочниці двоє гравців цифрових MSB змогли випробувати свою інноваційну бізнес-модель, включаючи використання процесу дистанційного взяття на обслуговування клієнтів за допомогою рішення e-KYC, в середовищі, де ризики, пов'язані з новою інновацією, можуть бути адекватно пом'якшені.

Беручи до уваги уроки, отримані з Пісочниці, BNM в кінці 2017 року запровадив нормативну вимогу щодо безконтактної перевірки для сектора MSB. Це дозволило більшому набору кваліфікованих учасників MSB впроваджувати перевірки e-KYC із належними гарантіями, такими як встановлення незалежного контакту із клієнтом та встановлення лімітів транзакцій. На сьогоднішній день, сім компаній, що здійснюють грошові перекази, отримали дозвіл на проведення e-KYC для взяття на обслуговування нових клієнтів. BNM також застосовував поступовий підхід до впровадження нормативних вимог на підтримку інноваційного рішення відповідно до готовності галузі. Наприклад, перевірка e-KYC була вперше представлена в сегменті грошових переказів і була поширена на сегмент обміну грошей у 2019 році.

На додаток до цього, прискорюючи та впорядковуючи практики суб'єктів галузі, BNM видав останню редакцію документу про політику ПВК/ФТ та політичний документ e-KYC, який можна застосовувати до всіх фінансових установ у 2020 році, викладаючи нормативні очікування щодо впровадження технологій e-KYC серед установ.

Додаток D - Додаткові тематичні дослідження RegTech щодо використання нових технологій для ПВК/ФТ приватним сектором

Тематичне дослідження: Управління інтелектуальним сповіщенням на основі машинного навчання для ПВК моніторингу транзакцій та перевірки імен

Фінансова установа об'єдналася з компанією з нормативних технологій (RegTech) із Сінгапуру у протидії відмиванню коштів (ПВК). Результатом співпраці стало цілісне рішення машинного навчання, яке дозволило б фінансовим установам отримувати швидшу та точнішу інформацію для запобігання та виявлення підозрілої діяльності з відмивання грошей. Рішення стосувалося двох основних процесів у рамках ситеми ПВК Банку - моніторингу транзакцій та перевірки імен - ефективно створюючи робочі процеси для пріоритетності попереджень на основі їх рівня ризику, щоб допомогти команді відповідальних працівників зосередитися на тих попередженнях, які мають найбільше значення.

Рішення поєднує контрольовані та неконтрольовані техніки машинного навчання, які мають на меті виявляти підозрілу діяльність та швидше та точніше виявляти клієнтів з високим ризиком. Він пропонує інтелектуальний спосіб зіставлення сповіщень про моніторинг транзакцій та відстеження імен шляхом їх розподілу на три сегменти ризику - L1, L2 та L3 - де L3 є сегментом найвищого ризику.

Програма моніторингу транзакцій здатна визначати пріоритети відомих попереджень на основі їх оцінок ризику та виявляти нові, невідомі підозрілі моделі. Програма перевірки імен складається з трьох основних компонентів – удосконалене співставлення імен за допомогою більш широкого спектру складних перестановок імен, зменшення невизначених звернень за допомогою функцій підсумування та точне виявлення попереджень за допомогою первинної та вторинної інформації. Ці можливості допомагають точно розрізнити фальшиві і справжні співпадіння.

Цей інструмент має механізм самонавчання для автоматичного, безперервного навчання та роз’яснювальну систему штучного інтелекту, що заявлена патентом, для глибокого розуміння та проведення якісного дослідження. Структура пояснює мотиви кожного попередження, зроблені моделлю машинного навчання таким чином, щоб це було зрозуміло для бізнес-користувачів.

Якщо виявлено випадок підозрілої діяльності, AMLS також створює розумне правило і додає його до бібліотеки ПВК типологій , що дозволяє моделям машинного навчання виявляти подібні шаблони для майбутніх попереджень. Це означає, що з часом рішення буде продовжувати фільтрувати кількість помилково спрацьованих даних і забезпечувати більш точне відстеження. Таким чином, працівники Банку зможуть використовувати заощаджений час для проведення поглиблених розслідувань підозрілих справ або для швидкого та ефективного фокусування на інших випадках.

Тематичне дослідження: Рішення щодо управління ризиками

Багатонаціональна фінансова установа використовує великі дані та автоматизований моніторинг контексту для виявлення та припинення фінансової злочинності у міжнародній торгівлі.

Контекстний моніторинг - це здатність об'єднувати та з'єднувати дані з різних систем та джерел для створення контексту та значення з метою виявлення значущих зв'язків та підвищення точності. Він використовує вдосконалені алгоритми, що дозволяють здійснювати більш складні підрахунки та застосовувати аналітичні підходи.

Використовуючи цю технологію, діяльність клієнтів можна постійно оцінювати на ризик. Цей рівень контекстного моніторингу покращує точність та прийняття рішень, забезпечуючи при цьому аналіз взаємозв'язків даних, який до цього при застосуванні аналітичних та інтелектуальних рішень ПВК не був можливим.

Його головними перевагами є: підвищена концентрація уваги на клієнтах завдяки меншій кількості та вищій якості сповіщень, виявлення активності з високим рівнем ризику, пов'язаної з відмиванням грошей, здатність надати повний зміст транзакціям клієнта та характеристиці ризиків, можливість забезпечити транзакційний та нетранзакційний аналіз подій.

Тематичне дослідження: Робототехнічні рішення для автоматизації процесів

Фінансова установа розробляє ініціативи, засновані на рішеннях роботизованої автоматизації процесів (RPA), які дозволяють підвищити ефективність процесів, такі як розслідування підозрілих транзакцій, перевірка імен для ідентифікації пуюлічних діячів, KYC взяття на обслуговування та ресертифікація. Також використовуються деякі рішення природної мови (переклад).

Поточні рішення машинного навчання, що застосовуються спеціально для сфери виявлення ПВК, включають моделі на основі правил у поєднанні з аналітикою даних, моделі на основі правил у поєднанні з методологією оцінки сповіщень, збагачені моделі на основі правил (із зовнішніми даними, такими як дані реєстру компаній) (в даному випадку не пов'язані з RPA).

Тематичне дослідження: Рішення Digital ID

Членський орган пропонує рішення, що сприяють інноваціям. Цей проект спрямований на розробку схеми, яка дозволить створити єдиний цифровий ідентифікатор, який відповідає всім відповідним нормативним вимогам (KYC та ПВК) та позиціонується серед споживачів як основний засіб надійної ідентифікації фінансових послуг Великобританії.

Організація тісно співпрацює з урядом для розробки Національної системи довіри, завдяки чому схема дозволить клієнту використовувати свій цифровий ідентифікатор у багатьох секторах, завдяки сумісним стандартам та технологіям, вона буде покладатися на різні точки доступу та розповсюдження пристроїв, що вимагають ID аутентифікацію для синтезу послуг та досвіду. Це також залежатиме від збільшення використання біометричних даних/відео KYC, машинного навчання, NLP та технології блокчейн/технології розподіленої реєстру.

Ця схема цифрового ідентифікатора дозволить споживачам повторно використовувати свою підтверджену особу та пов'язані з нею атрибути KYC для відкриття та доступу до фінансових онлайн-послуг.

Тематичне дослідження: Фірма з оцінки ризиків та дотримання вимог займається питаннями якості та несуперечності даних

Однією з ключових складових для належного оцінювання ризику даних транзакцій є ідентифікація всіх зазначених сторін та географічних регіонів. Це може виявитися складним завданням, враховуючи різні формати транзакцій, у поєднанні з людськими помилками та/або спробами ненадійних суб'єктів приховати свою особу. Для подолання цих проблем команда RegTech використовує різні методи з метою вилучення та нормалізації даних.

Ці регульовані суб'єкти пропонують послугу обробки даних, засновану на технологіях, для полегшення дотримання зобов'язань у сфері ПВК/ФТ. На початку будь-якого проекту та до збору даних відбувається низка бесід із зацікавленими сторонами, SMEs та необхідними технічними групами для визначення ключових елементів даних (KDE). Після отримання даних команда створює копію оригіналу (Золоте джерело), щоб зберегти цілісність та відстежуваність. Потім вона виконує аналітику високого рівня, щоб краще зрозуміти цілісність даних та виявити прогалини.

Нормалізація ряду також є важливою частиною цього процесу. Видалення спеціальних символів, зайвого пробілу та загальних корпоративних термінів (ТОВ, ООО, Limited) - це лише декілька кроків, вжитих для кращого групування, класифікації та ідентифікації.

Вилучення суб’єктів є важливою складовою будь-якої моделі ризику і ускладнюється “брудними” або неповними даними. Хоча основна увага приділяється KDE, ідентифікованим у процесі збору даних, покладаючись виключно на це можна пропустити "приховані" суб'єкти.

Один із методів, який зазвичай використовується, - це обробка природної мови або NLP для ідентифікації частин мови. NLP надає можливість сканувати весь набір даних на наявність власних імен, які можуть вказувати на особу чи компанію. Хоча NLP корисний, результати все одно вимагають додаткового аналізу та очищення, оскільки в даних транзакцій рідко спостерігається дотримання правил граматики. Отже, ці скани доповнюються внутрішнім інтелектом маркованого ряду.

Використовуючи нормалізовані суб'єкти, вилучені з раннього періоду, команда створює унікальний список, зберігаючи при цьому лінію походження від вихідного джерела.

Список літератури

BGIN (n.d.), *Blockchain Governance Initiative Network (BGIN), About*, https://bginglobal.org/about/. [23]

BIS (2020), *FSI Insights on policy implementation*, http://www.bis.org/fsi/publ/insights29.pdf. [31]

BIS (2019), *Suptech applications for ПВК, FSI Insights N.8*, https://www.bis.org/fsi/publ/insights18.pdf. [34]

Broeders D. and Prenio J. (2018), *Innovative technology in financial supervision (SupTech) – the experience of early users*, https://www.bis.org/fsi/publ/insights9.pdf. [36]

Chase, I. (2020), *Doing What is Right: Financial Inclusion Needs Better Incentives*, RUSI, https://rusi.org/commentary/doing-what-right-financial-inclusion-needs-better-incentives. [12]

CoE (2011), *Resolutions 1797 (2011), The need for a global consideration of the human rights implications of biometrics*, https://pace.coe.int/pdf/8b5e492cf90ea25e1c1f2f459c42bc9570713dd10154b339883da5da4c3 09a89/resolution%201797.pdf. [17]

Coelho et al. (2019), *Suptech applications for anti-money laundering*, https://www.bis.org/fsi/publ/insights18.htm. [4]

EBA (2021), *Opinion of the European Banking Authority on the risks of money laundering and terrorist financing affecting the European Union's financial sector*, https://www.eba.europa.eu/eba-highlights-key-money-laundering-and-terrorist-financing-risksacross-eu. [11]

EBA (2020), *European Banking Authority, Big Data and Advanced Analytics*, http://www.eba.europa.eu/sites/default/documents/files/document_library/Final%20Report%20 on%20Big%20Data%20and%20Advanced%20Analytics.pdf. [30]

EC (2019), *30 Recommendations on Regulation, Innovation and Finance*, https://ec.europa.eu/info/sites/default/files/business_economy_euro/banking_and_finance/docu ments/191113-report-expert-group-regulatory-obstacles-financial-innovation_en.pdf. [19]

FATF (2021), *Second 12-month Review Virtual Assets and VASPs*. [38]

FATF (2020), *Guidance on Digital ID*, http://www.fatf-gafi.org/publications/fatfrecommendations/documents/digital-identity-guidance.html. [8]

FATF (2020), *Priorities for the Financial Action Task Force Under the German Presidency*, http://www.fatf-gafi.org/media/fatf/documents/German-Presidency-Priorities.pdf. [3]

FATF (2020), *Stocktake on Data Pooling, Collaborative Analytics and Data Protection*, https://www.fatf-gafi.org/publications/fatfrecommendations/documents/data-poolingcollaborative-analytics-data-protection.html. [37]

FATF (2019), *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, FATF, http://www.fatf-gafi.org/publications/fatfrecommendations/documents/Guidance-RBA-virtual-assets.html. [1]

FATF (2014), FATF *clarifies risk-based approach: case-by-case, not wholesale de-risking*, http://www.fatf-gafi.org/documents/documents/rba-and-de-risking.html. [5]

FATF (n.d.), FATF *Guidance - The Risk-Based Approach*, http://www.fatf-gafi.org/documents/riskbasedapproach/?hf=10&b=0&s=desc(fatf_releasedate). [6]

FSB (2020), *The Use of Supervisory and Regulatory Technology by Authorities and Regulated Institutions*, p. 32, http://www.fsb.org/2020/10/the-use-of-supervisory-and-regulatorytechnology-by-authorities-and-regulated-institutions-market-developments-and-financialstability-implications/. [28]

FSB (2019), *Decentralised financial technologies – Report on financial stability, regulatory and governance implications*, http://www.fsb.org/wp-content/uploads/P060619.pdf. [21]

FSB (2017), *Artificial intelligence and machine learning in financial services*, https://www.fsb.org/wp-content/uploads/P011117.pdf. [25]

G20 (2019), *G20 Osaka Leaders' Declaration*, http://www.mofa.go.jp/policy/economy/g20_summit/osaka19/en/documents/final_g20_osaka_leaders_declaration.html. [22]

G20 (2016), *High Level Principles for Digital Financial Inclusion*, https://www.gpfi.org/sites/gpfi/files/documents/G20-HLP-Summary_0.pdf. [9]

HKMA (2021), *AML/CFT Regtech: Case Studies and Insights*, http://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-andcircular/2021/20210121e1a1.pdf. [27]

HKMA (2020), *AML/CFT Supervision in the Age of Digital Innovation*, http://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-andcircular/2020/20200929e1a1.pdf. [35]

Hong Kong Monetary Authority/Deloitte (2021), *AML/CFT Regtech:Case Studies and Insights*, http://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-andcircular/2021/20210121e1a1.pdf. [15]

Kazzaz, Z. (2020), *Emergency Disbursements during COVID-19: Regulatory Tools for Rapid Account Opening and Oversight*, p. 13, http://www.findevgateway.org/sites/default/files/publications/submissions/72016/Emergency%20. [13]

MAS (2018), *Industry Perspectives – Adopting Data Analytics Methods for AML/CFT*, http://www.mas.gov.sg/regulation/external-publications/industry-perspectives-adopting-dataanalytics-methods-for-ПВКФТ. [18]

Maxwell, N. (2020), *Innovation and discussion paper: Case studies of the use of privacy preserving analysis to tackle financial crime*, http://www.futurefis.com/uploads/3/7/9/4/3794525/ffis_innovation_and_discussion_paper_case_studies_of_the_use_of_privacy_preserving_analysis_-_v.1.3.pdf. [26]

OECD (2020), *ШІ Principles*, https://www.oecd.IIII/IIII-principles. [24]

Richard Grint et al (2017), *New Technologies And Anti-Money Laundering Compliance*, FCA, http://www.fca.org.uk/publication/research/new-technologies-in-ПВК-final-report.pdf. [14]

SAS (n.d.), *Five ШІ technologies that you need to know*, https://www.sas.com/en_us/insights/articles/analytics/five-IIII-technologies.html. [29]

UN (2019), *United Nations Security Council (UNSC) Resolution 2462 (28 March 2019), UN Doc S/RES/2462, para.20*, https://undocs.org/en/S/RES/2462(2019). [2]

UN (2018), *Compendium Of Recommended Practices For The Responsible Use & Sharing Of Biometrics In Counter Terrorism*, https://www.un.org/sc/ctc/wpcontent/uploads/2018/06/Compendium-biometrics-final-versionLATEST_18_JUNE_2018_optimized.pdf. [10]

Vyjayanti T DesIIII et al. (2018), "The global identification challenge: Who are the 1 billion people without proof of identity?", https://blogs.worldbank.org/voices/global-identification-challengewho-are-1-billion-people-without-proof-identity. [7]

Walshe, P. (2020), *Digital Identities*, https://rm.coe.int/t-pd-2020-04rev-digital-identity-tcen/1680a0c051. [32]

WEF (2020), *Forging New Pathways: the next evolution of innovation in financial services*, http://www.weforum.org/reports/forging-new-pathways-the-next-evolution-of-innovation-infinancial-services. [33]

World Bank (2021), *Principles On Identification For SustШInable Development: Toward The Digital Age*, https://documents.worldbank.org/en/publication/documentsreports/documentdetIIIII/470971616532207747/principles-on-identification-for-sustIIIInable-dev. [16]

Yuta Takanashi et. al (2020), *Call for Multi-Stakeholder Communication to Establish a Governance Mechanism for the Emerging BlockchШIn-Based Financial Ecosystem, Part 2 of 2*, https://stanford-jblp.pubpub.org/pub/multistakeholder-comm-governance2/release/1. [20]

Можливості та виклики нових технологій для ПВК/ФТ

Нові технології можуть покращити швидкість, якість та ефективність заходів щодо ПВК/ФТ. Вони можуть допомогти фінансовим установам та наглядовим органам оцінити ці ризики більш точно, своєчасно та всебічно. Застосовуючи відповідальний підхід, що ґрунтується на оцінці ризику, нові технології також можуть покращити фінансове включення.

Цей звіт визначає нові та існуючі технологічні рішення. У ньому висвітлено необхідні умови, політику та практику, які мають бути створені для успішного використання цих технологій та підвищення ефективності та результативності ПВК/ФТ. Він також вивчає перешкоди, які можуть стояти на заваді успішного впровадження нової технології.

www.fatf-gafi.org | ЛИПЕНЬ 2021