

**УНІВЕРСИТЕТ ДЕРЖАВНОЇ ФІСКАЛЬНОЇ
СЛУЖБИ УКРАЇНИ**

Кафедра банківської справи та фінансового моніторингу

СЕРІЯ «ПОДАТКОВА ТА МИТНА СПРАВА В УКРАЇНІ»

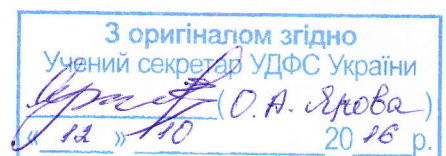
Серію «Митна справа в Україні» засновано в 2001 р. Її продовженням є серія «Податкова та митна справа в Україні», яку започатковано в 2015 р.

**АКТУАЛЬНІ ПИТАННЯ РОЗВИТКУ
БАНКІВСЬКОЇ СИСТЕМИ УКРАЇНИ**

Збірник наукових праць

*За загальною редакцією доктора економічних наук,
професора О. І. Береславської*

**Ірпінь
2016**



УДК 336.711(477)(082)
ББК 65.9(4Укр)262.10я54
A43

*Рекомендовано до друку Вченою радою
Національного університету ДПС України
(протокол № 13 від 28 травня 2015 р.)*

Рецензенти:

Белінська Я. В., д.е.н., професор (Університет ДФС України);

Примостка Л. О., д.е.н., професор (ДВНЗ «Київський національний економічний університет ім. Вадима Гетьмана»;

Шелудько Н. М., д.е.н., професор (ДУ «Інститут економіки та прогнозування НАН України).

Авторський колектив:

Береславська О. І., Горбачова А. О., Ключко Л. А., Ковда Н. І., Корнева І. В., Москаленко Н. В., Перехрест Л. М., Пернарівський О. В., Підсосонна Я. Г., Романенко Л. В., Тат'яніна С. М., Тимошенко О. П., Унінець О. В., Чишко І. С., Шавловська Л. С.

A43 Актуальні питання розвитку банківської системи України : збірник наукових праць / Береславська О. І., Пернарівський О. В., Тат'яніна С. М. та ін.; за заг. ред. д.е.н., проф. О. І. Береславської. – Ірпінь: Університет ДФС України, 2016. – 242 с. – (Серія «Податкова та митна справа в Україні», т. 64).

ISBN 987-966-337-409-3

Тематика збірника присвячена найбільш актуальним питанням розвитку та функціонування банківської системи України, проблемам фінансової стійкості та рефінансування банків, автоматизації процесу фінансового моніторингу в банку. Значна увага приділена питанням агрегування показників ризиків як напряду підвищення банківського менеджменту та діяльності банків з іноземним капіталом.

Збірник розрахований на наукових працівників, викладачів економічних вузів та факультетів, аспірантів та студентів, які спеціалізуються у сфері банківської діяльності, а також професійним банкірам.

УДК 336.711(477)(082)
ББК 65.9(4Укр)262.10я54

Матеріали друкуються в авторській редакції

ISBN 978-966-337-409-3

© Береславська О. І., Пернарівський О. В.,
Тат'яніна С. М. та ін., 2016
© Університет державної
фіскальної служби України, 2016

АВТОМАТИЗАЦІЯ ПРОЦЕСУ ФІНАНСОВОГО МОНІТОРИНГУ В БАНКУ

У статті досліджено та узагальнено зарубіжний досвід функціонування автоматизованих систем для здійснення фінансового моніторингу, розроблено пропозиції щодо автоматизації процесу фінансового моніторингу в банку.

Ключові слова: фінансовий моніторинг; автоматизована система; банківська установа; ідентифікація клієнтів.

Keywords: financial monitoring; automated system; banking institution; identification of customers.

Постановка проблеми. Кредитні організації становлять фундаментальний блок національної системи протидії легалізації (відмиванню) доходів та фінансуванню тероризму, вони є основними фінансовими посередниками при проведенні операцій між господарюючими суб'єктами у процесі економічних відносин. У зв'язку з цим на банки покладаються основні завдання здійснення фінансового моніторингу за проведеними операціями клієнтів і виявлення серед них сумнівних, можливо, пов'язаних з відмиванням доходів та фінансуванням тероризму [1]. Ефективне функціонування у кредитній організації підрозділу фінансового моніторингу неможливе без вирішення цілого комплексу завдань. Вони пов'язані з консолідацією даних про фінансові операції, їх відбором та спрямуванням у єдину базу даних, формуванням в автоматичному режимі на регулярній основі попереджень, правил визначення схем відмивання, розглядом виявлених попереджень та формуванням звітності, а також з поглибленим аналізом для виявлення нових схем відмивання грошей. У зв'язку із зазначеним на сьогодні в банках зростає інтерес до вирішення питань автоматизації процесів протидії легалізації (відмивання) доходів, одержаних злочинним шляхом.

Аналіз останніх досліджень та публікацій. Значна кількість науковців досліджувала питання особливостей розвитку системи фінансового моніторингу в Україні, зокрема: Н. Внукова, С. Гуржій, Л. Доля, І. Коломієць, А. Римарук, Ю. Лисенков, В. Капустін, С. Синяньський та інші. Незважаючи на вагомий внесок зазначених авторів у дослідження даних питань, розуміння окремих їх особливостей, раніше сформульовані висновки та пропозиції потребують уточнень та доповнень з урахуванням сучасних проблем у фінансовій системі та процесів легалізації тіньових капіталів.

Метою статті є узагальнення зарубіжного досвіду функціонування автоматизованих систем для здійснення фінансового моніторингу, розроблення пропозицій щодо автоматизації процесу фінансового моніторингу в банку.

Виклад основного матеріалу. Сучасні тенденції у фінансовій системі України та складна політична ситуація, без сумніву, висувують нові вимоги до протидії легалізації доходів незаконного походження. Це, у свою чергу, передбачає нагальну потребу у впровадженні автоматизованих систем проведення фінансового моніторингу в банках, що зумовлено такими факторами:

- значним збільшення обсягу інформації про операції клієнтів до підрозділів фінансового моніторингу, пов'язаним із сучасними економічними процесами як всередині країни, так із посиленням міжнародної інтеграції української економіки;
- ускладненням схем відмивання злочинних доходів, розкриття яких без використання спеціальних апаратно-програмних комплексів стає все більш складним;
- посилення вимог з боку Державної служби фінансового моніторингу та НБУ до здійснення фінансового моніторингу фінансовими посередниками.

На сьогодні основним завданням, яке ставлять кредитні організації перед розробниками і постачальниками автоматизованих систем протидії легалізації доходів незаконного походження, є побудова системи в межах всієї багатofilіальної мережі банку, що працює зі значною кількістю джерел даних та обробляє величезний обсяг інформації. Інвестиції в подібний проект – це забезпечення

надійності бізнесу та репутації банку, захищеності від використання його з метою відмивання грошей та фінансування тероризму.

Нині вимоги банків до автоматизованих систем протидії легалізації доходів незаконного походження та фінансування тероризму передбачають реалізацію таких функцій:

- 1) ідентифікація клієнтів:
 - збір обов'язкової інформації про клієнтів, ведення та періодичне оновлення анкет клієнтів;
 - визначення категорії ризику причетності клієнта до відмивання залежно від зібраної інформації, а в подальшому зміна категорії ризику залежно від діяльності клієнта;
- 2) виявлення осіб, причетних до терористичної діяльності:
 - перевірка клієнта на причетність до терористичної діяльності;
 - перевірка контрагентів у розрахункових операціях клієнтів на причетність до терористичної діяльності, призупинення розрахункових операцій, відмова клієнтам в обслуговуванні;
 - ведення та оновлення списків терористів;
- 3) реалізація документообігу для відділу фінансового моніторингу;
- 4) автоматизація процесу розслідування інцидентів;
- 5) виявлення операцій клієнтів, що підлягають обов'язковому фінансовому моніторингу;
- 6) виявлення незвичайних операцій, а також шахрайських схем, розподілених територіально і розтягнутих у часі;
- 8) запобігання шахрайським операціям;
- 9) підготовка обов'язкової та аналітичної звітності;
- 10) дотримання як українських, так і міжнародних вимог у сфері протидії легалізації доходів злочинного походження та фінансування тероризму.

Проведені дослідження сегмента ринку автоматизованих банківських систем показали, що у світі існує всього кілька великих розробників продуктів у цій сфері [3]. Найпопулярнішими з них є такі:

- 1) *SAS Institute* (США);

2) *Oracle Corporation* (США);

3) *Detica NetReveal* (Англія) (раніше – *Norkom Technologies*).

Автоматизована система *SAS Anti-Money Laundering* (*SAS AML*) використовується у понад 130 банках по всьому світу. Потрібно зазначити, що великими кредитними організаціями, які впроваджують *SAS AML*, є *Bank of America* (США), *Bank of Tokyo Mitsubishi* (Японія), *Qatar National Bank* (Катар), *Bank of China* (Китай), *Mashreq Bank* (ОАЕ). У 6 000 філій *Bank of America* за допомогою *SAS AML* щодня обробляється понад 1,2 млрд транзакцій.

Основні можливості *SAS AML* мають такі характеристики:

1) гнучке управління даними:

- ведення записів угод клієнтів банку;
- централізоване зберігання результатів аналізу даних про клієнтів і їх операції, а також забезпечення до них оперативного доступу;

- робота з різноманітними типами даних (нечисловими, географічними координатами, групами ризику тощо);

2) високопродуктивний аналіз даних та візуалізація результатів:

- проведення стрес-тестування банку щодо фінансового моніторингу;

- настройка та моделювання різноманітних сценаріїв у стислі терміни;

- швидкий доступ до відомостей про клієнта, його рахунки та операції;

3) моніторинг підозрілої діяльності клієнтів та інформування відповідального співробітника банку:

- автоматичне виявлення сумнівних операцій на основі нейронної мережі;

- автоматичне попередження відповідального співробітника банку про підозрілі угоди;

- простий у використанні інтерфейс програми;

4) групування клієнтів за ступенем ризику:

- групування клієнтів за ступенем ризику залежно від проведених ними операцій;

- переоцінка клієнтів за групами ризику при появі нових відомостей про нього;

5) порівняння фінансових можливостей клієнтів та операцій за певними наявними шаблонами:

- автоматичне завантаження переліку організацій і фізичних осіб, щодо яких є відомості про їх причетність до екстремістської діяльності або тероризму, а також осіб, що зареєстровані, проживають або перебувають у державі, у якій не передбачено розкриття або подання інформації під час проведення фінансових операцій;

- порівняння операцій за наявними шаблонами злочинних угод;

6) генерація і відправлення звітів: зручна адміністративна консоль дозволяє відповідальному співробітнику банку створювати і відправляти звіти у ПФР у затвердженій формі [3].

Переваги *SAS AML*, порівняно з «ручним» фінансовим моніторингом, проведеним у кредитній організації, полягають у такому:

- відстеженні значної кількості операцій;
- пришвидшенні аналізу даних, що надходять;
- збільшенні точності результатів моніторингу;
- виявленні організованих злочинних груп та їх схем;
- зниженні витрат на організацію і підтримку системи фінансового моніторингу у банку.

Іншою популярною автоматизованою системою протидії легалізації доходів незаконного походження та фінансування тероризму є американська система *Oracle Mantas*. Нині її впроваджено в найбільших банках світу. Так, на сьогодні 5 з 11 провідних банків (*Deutsche Bank AG, ABN AMRO Bank NV, Credit Suisse Group, Barclays Bank, Citibank NA*), що заклали основні директиви з протидії відмиванню злочинних доходів у документі «Вольфсберзькі принципи», використовують *Oracle Mantas* як основну ПВД/ФТ-платформу.

Основні можливості автоматизованої системи *Oracle Mantas*:

- консолідація, очищення та інтеграція будь-яких типів даних про операції та клієнтів кредитної організації, отриманих з різних джерел;
- використання складних моделей виявлення злочинних схем та сумнівних операцій;
- проведення розслідувань підозрілих інцидентів;
- формування звітів про виявлені сумнівні операції та направлення відповідальній особі банку або в ПФР країни [3].

Oracle Mantas складається з трьох основних блоків: модуля КУС («Знай свого клієнта»), модуля *Hotscan* (робота з «чорними списками») і АМЛ-ядра (для протидії легалізації та виявлення шахрайських операцій).

За допомогою модуля КУС здійснюється ідентифікація клієнтів банку. Так, у момент закладання картки клієнта або відкриття рахунку в КУС передається вся необхідна інформація про клієнта, яка в подальшому перевіряється в публічних джерелах, чорних списках і внутрішніх базах даних кредитної організації. Отримані із внутрішніх або зовнішніх джерел відомості можуть додаватися до аналітичних звітів або зберігатися в інформаційному сховищі документів банку. Таким чином, вирішується питання належності клієнта до групи ризику: ця інформація може бути завантажена із системи ризик-менеджменту або визначена модулем КУС відповідно до заданого налаштування. Залежно від присвоєного рівня ризику до клієнта застосовуватиметься різний ряд перевірок. Чим вище рівень, тим частіше проводитиметься переоцінка ризику для цього клієнта.

Модуль *HotScan* призначений для роботи з чорними списками осіб та організацій, що пов'язані з протиправною діяльністю. При цьому у банку є можливість використовувати як власні чорні списки, так і списки різних урядових і міжнародних організацій. Залежно від вимог банку автоматичне сканування на наявність у чорному списку може виконуватися на будь-якому з етапів обслуговування клієнта: у момент збереження його відомостей, при зміні клієнтської інформації, у процесі періодичного сканування клієнтської бази даних, моніторингу платіжних повідомлень та ін.

Крім того, за наявності підозр співробітник банку може в будь-який момент перевірити клієнта. Усі попередження система *HotScan* надає у відповідній екранній формі, у якій відповідальна особа може переглянути їх і вжити необхідних заходів. Щодо обсягів, то *HotScan* може обробляти в режимі реального часу понад 720 000 платіжних повідомлень на годину.

Основним функціональним блоком системи *Oracle Mantas* є AML-ядро, за допомогою якого обробляються та аналізуються вхідні дані про клієнтів і їх операції, а також зберігаються в централізованому сховищі. У процесі аналізу до цих даних системою застосовуються спеціальні сценарії – складні логічні моделі, що дозволяють виявити підозрілу поведінку клієнта банку або можливе відмивання злочинних доходів. Саме сценарії надають банку можливість виконувати комплексний моніторинг операцій і рахунків у розрізі продуктів та напрямів його діяльності. У системі є спеціальний конструктор, який дозволяє кредитним організаціям створювати нові сценарії або вносити зміни в наявні без затрат на перепрограмування. На сьогодні у системі є понад 300 сценаріїв, які можна застосовувати в таких сферах: обслуговування юридичних та фізичних осіб, брокерські операції, інвестиційні банківські послуги і контроль співробітників банку. Однак основною відмінною особливістю *Oracle Mantas* є її можливість проводити розслідування випадків відмивання злочинних доходів. Так, для того щоб ініціювати розслідування, система заводить нову справу при виявленні підозрілої поведінки, так званого інциденту. Крім того, *Oracle Mantas* дозволяє об'єднати кілька однотипних інцидентів у єдине діловодство. Для розслідування інцидентів система *Oracle Mantas* містить набір звітів і специфічних інструментів, зокрема аналіз зв'язків клієнта, що дозволяє ідентифікувати всі рахунки, залучені в його угоди, усіх кореспондентів, банки та ін. Для аналізу зв'язків будується мережа, що візуально показує напрям руху коштів і зв'язки між кореспондентами. Залежно від результатів розслідування система може автоматично сформулювати звіт для подальшого відправлення до відповідного органу фінансового моніторингу, закрити справу.

Ще одним відомим програмним забезпеченням автоматизованих систем протидії легалізації доходів та фінансування тероризму є *Detica NetReveal AML* англійської компанії *BAE Systems Detica*. Цей програмний продукт використовується в понад 100 найбільших фінансових організацій світу, у тому числі канадською корпорацією *Home Capital Group Inc.* і французьким страховим холдингом *AXA Group*.

Варто зупинитися на основних можливостях *Detica NetReveal AML*:

- 1) реалізація стандартів і рекомендацій міжнародних організацій у сфері протидії легалізації доходів та фінансуванню тероризму: ФАТФ, ООН, Європейського Союзу та інших;
- 2) обмін виявленими злочинними схемами з відповідними органами країни;
- 3) автоматичне створення та заповнення форм звітностей, які прийняті у країні, реєстрація кредитної організації;
- 4) можливість розширення обсягу функцій програми з метою реалізації всіх вимог фінансового моніторингу до протидії легалізації доходів та фінансуванню тероризму;
- 5) складні алгоритми виявлення сумнівних операцій у режимі реального часу, засновані на нейронних мережах і евристичному аналізі даних і спрямовані на підвищення продуктивності та автоматизації роботи підрозділу фінансового моніторингу [3].

Таким чином, упровадження у роботу кредитних організацій автоматизованих систем фінансового моніторингу дозволяє значно спростити внутрішній контроль за протидією легалізації доходів та фінансуванню тероризму, знизити витрати на персонал підрозділів, а отже, істотно підвищити якість фінансового моніторингу. Крім того, скорочується комплаєнс-ризик як для окремих банків, так і всієї країни в цілому.

Разом з тим, незважаючи на всі позитивні характеристики розглянутих продуктів у сфері автоматизації процесів фінансового моніторингу в банку, існує ряд недоліків, пов'язаних зі специфікою застосування їх у банківській системі України, що не дозволяє повсюдно впроваджувати автоматизовані системи у кредитні

організації. Зауважимо, що більшість кредитних організацій у нашій країні не володіє достатніми ресурсами для придбання зарубіжних автоматизованих систем фінансового моніторингу. Ці системи орієнтовані насамперед на найбільші банки та фінансові групи, як наслідок, функціональні та обчислювальні можливості систем не можуть бути використаними дрібними банками. Крім того, багато постачальників (*Oracle*, *SAS* та ін.) вимагають укладення спеціальних ліцензійних угод, які передбачають здійснення періодичних ліцензійних платежів за використання їх автоматизованих систем фінансового моніторингу, що певною мірою збільшує фінансову залежність кредитних організацій.

Іншим недоліком зарубіжних автоматизованих систем є їх недостатня функціональність в умовах зростання терористичної загрози. Так, жодна з них не передбачає забезпечення оперативного доступу слідчих до даних, що становлять банківську таємницю, що не дозволяє правоохоронним органам проводити ефективні оперативно-розшукові заходи. Разом з тим, наприклад, оператори зв'язку (стільникового, інтернет-зв'язку та ін.) надають державним органам, які здійснюють оперативно-розшукову діяльність, інформацію про їх клієнтів і про надані їм послуги за допомогою спеціальних програмно-апаратних комплексів, що встановлюються в обов'язковому порядку [2].

Зниження ефективності зарубіжних автоматизованих систем фінансового моніторингу також пов'язане з тим, що здебільшого кінцеве рішення про направлення системою повідомлення про сумнівну операцію до Держфінмоніторингу ухвалює відповідальний співробітник банку, який може помилитися, мати відмінну від системи суб'єктивну думку про відсутність ознак підозрілості операції, а в деяких випадках навіть перебуває у злочинній змові з особою, яка здійснює відмивання злочинних доходів. А отже, існує реальна загроза розголошення відомостей, що становлять державну таємницю, унаслідок використання цих систем банками.

Висновки. Підводячи підсумок, зазначимо, що, на нашу думку, застосування зарубіжної автоматизованої системи фінансового

моніторингу, яка не пройшла належної перевірки українськими компетентними службами, може призвести до фактичної втрати захисту відомостей, що становлять державну таємницю. Зокрема, за наявності в ній нерегламентованих пристроїв і програмного забезпечення, призначених для прихованої передачі даних за кордон, в іноземних фахівців з'явиться повний доступ до всіх грошових потоків кредитної організації, інформації про позичальників і предмети кредитування, у тому числі й об'єкти військового призначення, що має нині важливе значення.

Отже, зазначене свідчить про те, що наявні на ринку автоматизовані системи фінансового моніторингу орієнтовані насамперед на великі банки і фінансові групи. У більшості дрібних і середніх кредитних організаціях автоматизація процесу фінансового моніторингу обмежується лише простими програмними продуктами, які передбачають автоматичне виявлення операцій, що підлягають обов'язковому фінансовому моніторингу без можливості виявлення складних схем відмивання. Таке нерівномірне впровадження сучасних банківських технологій у сфері фінансового моніторингу не дозволяє державі підвищити прозорість банківської системи і призводить лише до переходу злочинців з великих банків у недостатньо технічно розвинені дрібні кредитні організації.

Ураховуючи викладене, варто наголосити на тому, що вдосконалення національної системи фінансового моніторингу є вкрай важливим завданням. Необхідно створити та впровадити в банках спеціалізовану державну автоматизовану систему протидії легалізації доходів незаконного походження та фінансування тероризму, яка забезпечуватиме виявлення підозрілих операцій та ідентифікацію клієнтів, аналізуватиме ризики, що виникають при цьому, та здійснюватиме управління ними, а також формуватиме регулярну звітність та направлятиме її до Державної служби фінансового моніторингу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, або фінансуванню тероризму : Закон України : від 28 листопада 2002 року № 249-IV [Електронний ресурс]. – Режим доступу : <http://zakon4.rada.gov.ua/laws/show/249-15>.

2. Про затвердження форм обліку та подання інформації, пов'язаної із здійсненням фінансового моніторингу, та Інструкції щодо їх заповнення : наказ Державної служби фінансового моніторингу України : від 26 серпня 2010 року № 148 [Електронний ресурс]. – Режим доступу : http://sdfm.gov.ua/documents.php?cat_id=34&doc_id=326&lang=uk&page=1.

3. Global Anti-Money Laundering Vendor Evaluation: A Reinvigorated Market [Електронний ресурс] // WatersRankings. – 2010. – Режим доступу : http://www.waterstechnology.com/digital_assets/1638/Waters_Rankings_2010.pdf