УДК 004.6: 004.021: 336.7
УКПП
№ Державної реєстрації 0118U003574
Інв. №

Міністерство освіти і науки України
Сумський державний університет
(СумДУ)
40007, м. Суми, вул. Петропавлівська, 57; тел. 66-50-37

ЗАТВЕРДЖУЮ
Проректор з наукової роботи
д-р фіз.-мат. наук, професор
А.М. Чорноус

ЗВІТ
ПРО НАУКОВО-ДОСЛІДНУ РОБОТУ
КІБЕРБЕЗПЕКА В БОРОТЬБІ З БАНКІВСЬКИМИ ШАХРАЙСТВАМИ: ЗАХИСТ СПОЖИВАЧІВ ФІНАНСОВИХ ПОСЛУГ ТА ЗРОСТАННЯ ФІНАНСОВО-ЕКОНОМІЧНОЇ БЕЗПЕКИ УКРАЇНИ

(проміжний)

Керівник НДР
завідувач кафедри економічної кібернетики
д-р екон. наук, професор О.В. Кузьменко

2019

Рукопис закінчений 24 грудня 2019 р.
Результати цієї роботи розглянуті науковою радою СумДУ,
протокол від 2019.12.26 №6

СПИСОК АВТОРІВ

Зав. кафедри економічної кібернетики, д-р екон. наук, професор (керівник)	24.12.2019	О.В. Кузьменко (підрозділи 1.3, 2.3)
Професор кафедри економічної кібернетики, д-р екон. наук, професор	24.12.2019	С.В. Лєонов (підрозділ 3.2)
Доцент кафедри економічної кібернетики, канд. екон. наук, доцент (відповідальний виконавець)	24.12.2019	Г.М. Яровенко (вступ, підрозділи 2.3, 3.1, 3.2, висновки)
Доцент кафедри банківської справи, фінансів та страхування, канд. екон. наук, доцент	24.12.2019	О.А. Криклій (підрозділ 1.1)
Доцент кафедри економічної кібернетики, канд. техн. наук, доцент	24.12.2019	К.Г. Гриценко (підрозділи 1.2, 2.2)
Доцент кафедри економічної кібернетики, канд. екон. наук	24.12.2019	А.О. Бойко (підрозділи 2.3, 3.2)
Ст.викл. кафедри економічної кібернетики, канд. екон. наук	24.12.2019	О.О. Пушко (підрозділ 2.1)
Аспірант кафедри економічної кібернетики	24.12.2019	Т.В. Доценко (підрозділи 1.3, 2.3, 3.2)
Студент кафедри економічної кібернетики	24.12.2019	Ю.Д. Онопко (підрозділ 3.1)

РЕФЕРАТ

Звіт про НДР: 116 с., 30 рис., 12 табл., 23 формули, 127 джерел.

АУДИТ, БАНК, ІНТЕЛЕКТУАЛЬНИЙ АНАЛІЗ, ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ, КІБЕРБЕЗПЕКА, МОДЕЛЮВАННЯ, МОНІТОРИНГ, КІБЕРЗАГРОЗА, КІБЕРШАХРАЙСТВО.

Об'єкт дослідження – система фінансово-економічних відносин та інформаційних зв'язків між економічними суб'єктами та банківськими установами, а також всередині банку. Предмет дослідження – методичні, організаційні, економіко-математичні та інформаційно-технологічні підходи до удосконалення ефективної системи аудиту та моніторингу банку для боротьби з банківськими кіберзлочинами.

Мета роботи – розвиток методології та міждисциплінарного методичного інструментарію системи внутрішнього аудиту та моніторингу для боротьби з кібершахрайствами в банківській сфері, як превентивної структури в системі кібербезпеки банку.

Методи дослідження – системний підхід, діалектичний метод наукового пізнання, фундаментальні положення аудиту, моніторингу та банківської справи, сучасні математичні методи та моделі, а саме нечітко-множинне моделювання, динамічне моделювання, нейронно-мережеве моделювання та програмування, сучасні концепції моделювання бізнес-процесів, інформаційні технології та системи для розробки прототипів, сучасні концепції кібербезпеки.

В роботі удосконалено механізм внутрішнього аудиту в системі забезпечення кібербезпеки банку. Проведено дослідження особливостей незалежного аудиту для попередження шахрайства банківського персоналу. Визначено роль фінансового моніторингу в сучасній системі кібербезпеки банку. Розроблено динамічний підхід щодо моделювання процесу боротьби з кібератаками у сфері електронного банкінгу. Розроблено нечітко-множинну модель оцінки рівня ризику шахрайства банківського персоналу. Проведено оцінку ризику використання фінансових посередників з метою легалізації кримінальних доходів на основі інтелектуального аналізу даних. Розроблено моделі бізнес-процесів перевірок операцій на предмет шахрайств, які здійснюються персоналом банку. Розроблено модель бізнес-процесу автоматизованої перевірки операцій на предмет ризику легалізації коштів у банку.

ЗМІСТ

ВСТУП

Сьогодні банківська діяльність дуже часто виступає об’єктом фінансових шахрайств, які здійснюються як зовнішніми по відношенню до банку шахраями, так і внутрішніми, в якості яких виступає керівництво та персонал банку. Це відбувається завдяки тому, що в Україні досить багато економічних проблем, які впливають на розмір та постійність доходів громадян. У сукупності із стійким розвитком комп’ютерних та інформаційних технологій це призводить до збільшенню шахрайств з банківськими транзакціями або грошовими ресурсами.

Дуже поширеним видом шахрайства є соціальна інженерія, коли злочинець ошукує клієнтів банку шляхом виманювання даних карток та злому особистих акаунтів клієнтів. Хоча банки активно намагаються протидіяти цьому виду шахрайств, але злочинці знаходять нові способи здійснення шахрайств. Окрім зовнішніх шахраїв значну шкоду завдають й внутрішні. Статистика свідчить, що близько 85% шахрайств в банківський сфері належить банківським працівникам, які мають доступ до різного роду інформації про рахунки, клієнтів та до внутрішньої та зовнішньої документації. Вони також мають змогу вилучати інформацію та продавати її стороннім компаніям, що також сприяє появі слабких місць в системі кіберзахисту банку.

Одним з напрямів банківського шахрайства є також здійснення процесу відмивання коштів, які були отримано незаконним шляхом. Проблема полягає як раз в процесі виявлення таких операцій. Тобто в цьому напрямі повинна працювати система внутрішнього моніторингу, основна мета якої виявлення операцій, що мають ознаки легалізації коштів. Але якщо банківські працівники знаходяться у зговорі з кримінальними структурами або зацікавлені у процесі відмивання коштів через пов’язаних осіб, то цей аспект також потребує врахування в процесі організації системи кібербезпеки банку.

На сьогодні система внутрішнього аудиту банків є досить розвинутою та добре організованою. Але її основна задача – це перевірка фінансово-господарської діяльності банку на предмет її відповідності законодавству,

банківським нормативам, стандартам. Потужний інструментарій аудиту, сформований фахівцями роками, сприяє виявленню різного роду відхилень. Тому цей підхід можна також реалізовувати й для виявлення шахрайств у банку, як з боку зовнішніх шахраїв, так й з боку внутрішніх.

Для боротьби із шахрайствами банківські установи застосовують прийоми та інструменти кібербезпеки, але сучасні реалії свідчать, що є нагальна потреба у створенні нових заходів, які б були комплексними та об'єднували різні прийоми, наприклад, математичні методи, інформаційні технології, прийоми аудиту, моніторингу, психологічні тощо. Тільки їх поєднання та створення інтегрованої системи кіберзахисту, моніторингу та аудиту дозволить сформувати потужну систему протидії банківським шахраям. Особливо дієвою така система може стати у боротьбі з кіберзлочинами, які здійснюють працівники банку, та у протидії процесу відмивання коштів, що відбувається за участю банківських працівників.

Окреслена проблема дозволила обрати об'єкт та предмет дослідження. Об'єктом виступає система фінансово-економічних відносин та інформаційних зв'язків між економічними суб'єктами та банківськими установами, а також всередині банку. Предметом дослідження є методичні, організаційні, економіко-математичні та інформаційно-технологічні підходи до удосконалення ефективної системи аудиту та моніторингу банку для боротьби з банківськими кіберзлочинами.

Відповідно до об'єкта та предмета дослідження було сформовано мету. Так, метою дослідження є розвиток методології та міждисциплінарного методичного інструментарію системи внутрішнього аудиту та моніторингу для боротьби з кібершахрайствами в банківській сфері, як превентивної структури в системі кібербезпеки банку.

Для реалізації поставленої мети необхідно було вирішити наступні завдання:

– удосконалити механізм внутрішнього аудиту в системі забезпечення кібербезпеки банку;

– дослідити особливості незалежного аудиту для попередження шахрайства банківського персоналу;

– визначити роль фінансового моніторингу в сучасній системі кібербезпеки банку;

– розробити динамічний підхід щодо моделювання процесу боротьби з кібератаками у сфері електронного банкінгу;

– розробити нечітко-множинну модель оцінки рівня ризику шахрайства банківського персоналу;

– провести оцінку ризику використання фінансових посередників з метою легалізації кримінальних доходів на основі інтелектуального аналізу даних;

– розробити бізнес-процеси перевірок операцій на предмет шахрайств, які здійснюються персоналом банку;

– розробити модель бізнес-процесу автоматизованої перевірки операцій на предмет ризику легалізації коштів у банку.

Методи дослідження – системний підхід, діалектичний метод наукового пізнання, фундаментальні положення аудиту, моніторингу та банківської справи, сучасні математичні методи та моделі, а саме нечітко-множинне моделювання, динамічне моделювання, нейронно-мережеве моделювання та програмування, сучасні концепції моделювання бізнес-процесів, інформаційні технології та системи для розробки прототипів, сучасні концепції кібербезпеки.

Інформаційно-фактологічну базу дослідження сформували законодавчі та нормативні документи Національного банку України, інструкції банків, наукові праці вітчизняних та зарубіжних фахівців.

Отримані у роботі результати використовуються у діяльності: філії - Сумського обласного управління АТ «Ощадбанк»; відділення «Сумське» ПАТ «Альфа-Банк»; ТОВ Видавництво-газета «Ярославна». Результати впроваджено у навчальний процес при викладанні дисциплін «Інформаційні системи у фінансах», «Бізнес-аналітика та прийняття рішень», «Прогнозування соціально-

економічних процесів», «Моделювання бізнес-процесів», «Інформаційні системи і технології в управлінні».

За результатами наукового дослідження опубліковано 5 статей та 2 подано до друку у журналах, що індексуються БД Scopus та/або Web of Science, 10 статей у фахових виданнях, 3 статті прийнято до друку у фаховому виданні, 2 статті опубліковано у нефахових виданнях, 7 тез доповідей у матеріалах міжнародних та вітчизняних конференцій, 1 монографія за тематикою НДР.

Звіт виконано на основі публікацій виконавців, перелік яких надано у списку літератури.

1 СИСТЕМА ВНУТРІШНЬОГО АУДИТУ ЯК ПРЕВЕНТИВНА СКЛАДОВА В СИСТЕМІ КІБЕРБЕЗПЕКИ БАНКУ

1.1 Механізм внутрішнього аудиту в системі забезпечення кібербезпеки банку

Сектор банківських та фінансових послуг є найбільш привабливим для кібератак та кібершахрайств через можливість отримання зловмисниками значних фінансових та нефінансових вигід.

За даними IBM, фінансовий сектор у 2016 році атакований на 65 % частіше, ніж будь-який інший, у результаті чого втрачено більш, ніж 200 мільйонів записів (на 937 % більше, ніж у 2015 році) [1]. У 2016 році 8,5 % зареєстрованих інцидентів витоку інформації зафіксовано в фінансовому секторі, при чому фінансові установи постраждали від цих інцидентів у 300 разів частіше, ніж підприємства інших галузей [2].

У дослідженні глобальних банків, проведеному Інститутом міжнародних фінансів у партнерстві з Ernst & Young, як голови рад директорів, так і відповідальні за ризик-менеджмент, вважали забезпечення кібербезпеки ключовим стратегічним пріоритетом [3].

Але, попри значну увагу банків до дослідження видів кіберзагроз, причин, що обумовлюють їх появу, ландшафт загроз постійно розвивається, приводячи до складнішої кібер-екосистеми, а наслідки реалізації кіберзагроз експоненційно зростатимуть. Це, насамперед, обумовлено розвитком цифрової інфраструктури, впровадженням фінансових технологій та активною діяльністю FinTech-фірм, що розмиватиме кордони між традиційними банківськими та небанківськими послугами, загострюватиме конкуренцію та створюватиме нові джерела загроз для кібербезпеки банків. Проблема посилюватиметься тим, що банківські інформаційні системи ставатимуть все більш взаємопов’язаними, операційні процеси – більш автоматизованими, при цьому вже наявна інфраструктура

інформаційних та комунікаційних технологій не була розроблена з пріоритетом кібербезпеки, що потребуватиме її адаптації до нових умов діяльності.

Зважаючи на це, формування заходів для запобігання настанню ситуацій, що класифікуються як кіберзагроза або шахрайство, є важливою науковою та прикладною задачею. Але у рамках дослідження рейтингового агентства PwC Україна виявлено, що «…більшість корпоративних рад директорів не дотримуються превентивного підходу до формування стратегій забезпечення кібербезпеки чи інвестиційних планів її розвитку» [4]. Відповідно до цього актуальним для банків України є створення превентивної системи забезпечення кібербезпеки, одним з важливих елементів якої є внутрішній аудит.

Вагомий внесок у становлення та розвиток теоретико-методологічних засад внутрішнього аудиту в банках, на яких мають базуватись розробки у сфері внутрішнього аудиту кібербезпеки, зробили такі вітчизняні та іноземні вчені, як: А. Герасимович [5], О. Кірєєв [6], Л. Костирко [7], М. Маркевич [8], М. Письменна [9], О. Сарахман [10, 11], А. Арсланбеков-Федоров [12], С. Банк [13], Г. Бєлоглазова та інші [14], Н. Соколинська [15], А. Баракат (*A. Barakat*) [16], К. Россітер (*C. Rossiter*) [17] та інші.

Важливість ефективної системи внутрішнього аудиту для попередження шахрайства у сфері електронних банківських послуг та інформаційних банківських систем досліджувало багато іноземних науковців, такі, як О. Дж. Акіньомі (*O. J. Akinyomi*) [18], А. А. Боатенг, Г. О. Боатенг та Х. Акуа (*A. A. Boateng, G. O. Boateng, H. Acquah*) [19], С. Пальфі та М. Мурешан [20], Д. Петрашку та А. Тіану (*D. Petraşcu and A. Tieanu*) [21], Р. Саламе, Г. Аль-Вешах, М. Аль-Нсур та А. Аль-Хіяри (*R. Salameh, G. Al-Weshah, M. Al-Nsour, A. Al-Hiyari*) [22], М. Ула, З. Ісмаїл та З. М. Сідек (*M. Ula, Z. Ismail, Z. M. Sidek*) [23], А. К. Усман та М. Х. Шах (*A. K. Usman and M. H. Shah*) [24] та інші.

Слід наголосити на тому, що переважна більшість досліджень цих та інших іноземних науковців ураховують специфіку банківських систем та загроз кібербезпеки, притаманних конкретним країнам та регіонам. Тому отримані наукові результати можуть лише частково бути враховані при формуванні

системи внутрішнього аудиту для запобігання загрозам втрати кібербезпеки в банках України.

Комплексні теоретичні розробки, що обґрунтовують систему внутрішнього аудиту кібербезпеки як превентивну складову в системі кібербезпеки банку, у вітчизняній науковій літературі практично відсутні.

Увага науковців, в основному, зосереджується на окремих об'єктах системи забезпечення кібербезпеки банку. Так, О. Мельниченком у [25-29] досліджено аудит інформаційної безпеки банку при роботі з електронними грошима. Основна увага акцентується на ключових напрямах перевірки, зокрема, організаційно-технічній та правовій забезпеченості банків для запобігання загрозам стабільного функціонування систем електронних грошей. Крім того, автором досліджуються методи соціальної інженерії та способи попередження цього типу загроз кібербезпеці.

О. Попович та К. Войновська у [30] розробили методологію аудиту електронних грошей в банках України як складової системи контролю інформаційної безпеки, зокрема, ними висвітлено ключові напрями аудиту.

Високо оцінюючи вклад вітчизняних та іноземних авторів у дослідження питань запобігання кіберзагрозам в банківській діяльності, у тому числі з застосуванням внутрішнього аудиту, слід зазначити про необхідність подальшого поглиблення цих теоретичних досліджень з урахуванням специфіки діяльності банків України.

Виходячи з вище зазначеного є необхідність у розробці теоретико-методичних основ системи внутрішнього аудиту кібербезпеки банку, з деталізацією її складових та науковому обґрунтуванні принципів функціонування, на основі чого можна було б вирішувати завдання забезпечення ефективного контролю кібербезпеки.

Зважаючи на зростання зовнішніх та внутрішніх загроз, що впливають на рівень кібербезпеки банків України, постала необхідність розбудови системи внутрішнього аудиту як превентивної складової в системі кібербезпеки. Парадигма превентивності реалізується на основі незалежної та об'єктивної

оцінки поточного рівня захищеності банку від зовнішніх та внутрішніх кіберзагроз, розробки рекомендацій з усунення виявлених недоліків у системі забезпечення кібербезпеки та моніторингу їх своєчасного впровадження.

Внутрішній аудит кібербезпеки банку пропонуємо розглядати як періодичну систему збору та оцінки інформації для визначення того, чи забезпечують всі системи банку належний стан захищеності інформаційних активів та інформаційної інфраструктури, збереження властивостей інформаційних активів (доступності, цілісності чи конфіденційності) на цільовому рівні відповідно до встановлених критеріїв в умовах постійного впливу зовнішніх та або / внутрішніх загроз з дотриманням вимог національного та міжнародного законодавства.

Систему внутрішнього аудиту пропонуємо розглядати як невіддільну складову забезпечення кібербезпеки банку, що являє собою сукупність взаємопов’язаних елементів (цілі та завдання, об’єкт, суб’єкт, механізм), що функціонують на основі загальних та спеціальних принципів та дозволяють об’єктивно оцінити рівень захищеності та збереження властивостей інформаційних активів та інформаційної інфраструктури банку в умовах постійного впливу зовнішніх та або / внутрішніх загроз, а також дотримання вимог національного та міжнародного законодавства.

Об’єктами внутрішнього аудиту є інформаційні активи – матеріальні або нематеріальні об’єкти, що є інформацією або містять інформацію, слугують для обробки, зберігання або передачі інформації та мають цінність для банку.

Для формування об’єктного середовища внутрішнього аудиту в системі забезпечення кібербезпеки банку необхідно враховувати загрози, що генерується як зовнішнім, так і внутрішнім середовищем (табл. 1.1).

Таблиця 1.1 – Класифікація загроз кібербезпеки банку

Ознака	Вид загрози
За джерелом	- внутрішні (втрата, знищення, викрадення, викривлення або розголошення інформації, витік інформації); - зовнішні (модифікація змісту, порушення конфіденційності, порушення логічної цілісності, порушення прав власності на інформацію, порушення фізичної цілісності, природні та техногенні катастрофи, що порушують нормальний режим роботи інформаційних систем тощо)
За походженням	- об'єктивні (природні), що характеризуються впливом на об'єкт захисту фізичних процесів або стихійних природних явищ, що не залежать від людини; - суб'єктивні, що характеризуються впливом на об'єкт захисту діяльністю людини; - результати соціальної інженерії (фішинг, фармінг, претекстинг, скрімінг та ін.)
За ступенем впливу на інформаційну систему	- пасивні без впливу на стан інформаційної системи; - активні з порушенням нормального процесу функціонування інформаційної системи банку
За цілеспрямованістю	- ненавмисні (помилкові, випадкові, необдумані, без злого наміру та корисливих цілей) дії персоналу та користувачів банківських послуг; - навмисні (в корисливих цілях, з примусу третіми особами, зі злим умислом тощо) персоналу, користувачів банківських послуг, злочинних груп та формувань, політичних і економічних структур, а також окремих осіб
За способом реалізації	- розголошення; - витік; - несанкціонований доступ.
За ступенем сформованості	- реальні; - потенційні.
За можливістю прогнозування	- прогнозовані; - не прогнозовані;
За ймовірністю виникнення	- реальна; - ймовірна; - малоймовірна; неймовірна.
За характером впливу	- явна, пряма (загрози, реалізація яких порушує безпеку інформаційних активів); - неявна, опосередкована (загрози, що створюють умови для появи прямих загроз);
За масштабами наслідків	- катастрофічні; - критичні; - середні; - незначні.
За можливістю нейтралізації	можливо нейтралізувати; можливо частково нейтралізувати; нейтралізувати неможливо.

Джерело: розроблено на основі [31, 32].

Перелік способів реалізації загроз кібербезпеки банку, на яких має концентруватись аудит, наведено в таблиці 1.2.

Таблиця 1.2 – Перелік способів реалізації загроз кібербезпеки банку

Рівні кібербезпеки	Способи реалізації загроз
Фізичний рівень	- витік інформації; - знищення / руйнування / диверсії; - несанкціонований фізичний доступ; - розкрадання / крадіжка.
Мережевий рівень	- атаки «відмова в обслуговуванні»; - впровадження апаратних закладок; - підміна довіреного об'єкта мережі та передача за каналами зв'язку; повідомлень від його імені з присвоєнням його прав доступу; - порушення штатних режимів роботи мережевого обладнання.
Рівень мережевих додатків і сервісів	- аналіз трафіку; - атаки «відмова в обслуговуванні»; - використання спеціалізованих програм; - впровадження шкідливого програмного забезпечення; - порушення штатних режимів роботи мережевих додатків; - сканування мережі, спрямоване на виявлення відкритих портів та служб, відкритих з'єднань.
Рівень операційних систем та систем управління базами даних	- копіювання; - крадіжка / втрата паролів; - модифікація / видалення даних; - неправильна (неповна) конфігурація систем захисту інформації; - несанкціонований логічний доступ до операційних систем/ систем управління базами даних з використанням спеціалізованого програмного забезпечення; - підміна ідентифікаторів користувача; - поширення шкідливих програм.
Рівень банківських технологічних процесів та програм	- модифікація / видалення даних; - розповсюдження / передача даних; - друк документів; - крадіжка документів та карток; - крадіжка паролів.
Рівень бізнес-процесів	- саботаж; - халатність та помилки; - шкідництво.

Джерело: розроблено авторами.

Зважаючи на збільшення кількості операційних процесів, у тому числі ключових, що передаються стороннім організаціям (наприклад, інтернет-провайдери, підрядники, що здійснюють монтаж обладнання), зростає залежність банків від кібербезпеки цих сторін. У відповідь на це, в банку має бути передбачена можливість аудиту кібербезпеки сторонніх організацій для забезпечення того, щоб їх діяльність відповідала встановленим стандартам та не створювала загрози втрати кібербезпеки.

До реалізації завдань внутрішнього аудиту кібербезпеки долучається служба внутрішнього аудиту банку. Аудит також може бути проведено шляхом залучення юридичних / фізичних осіб із належним рівнем компетенції та досвіду (аутсорсинг).

Слід наголосити на тому, що служба внутрішнього аудиту є третьою лінією захисту від кібер-ризиків, при цьому не бере безпосередньої участі в управлінні ними, а її роль зводиться до оцінки адекватності системи забезпечення кібербезпеки цілям та задачам банку [33], оцінки загальної ефективності дій, що виконуються першою та другою лініями захисту (підрозділи менеджменту та інформаційної безпеки, відповідно) в управлінні та зниженні ризиків кібербезпеки.

Взаємозв'язок суб'єктів забезпечення кібербезпеки банку зі службою внутрішнього аудиту наведено на рисунку 1.1.

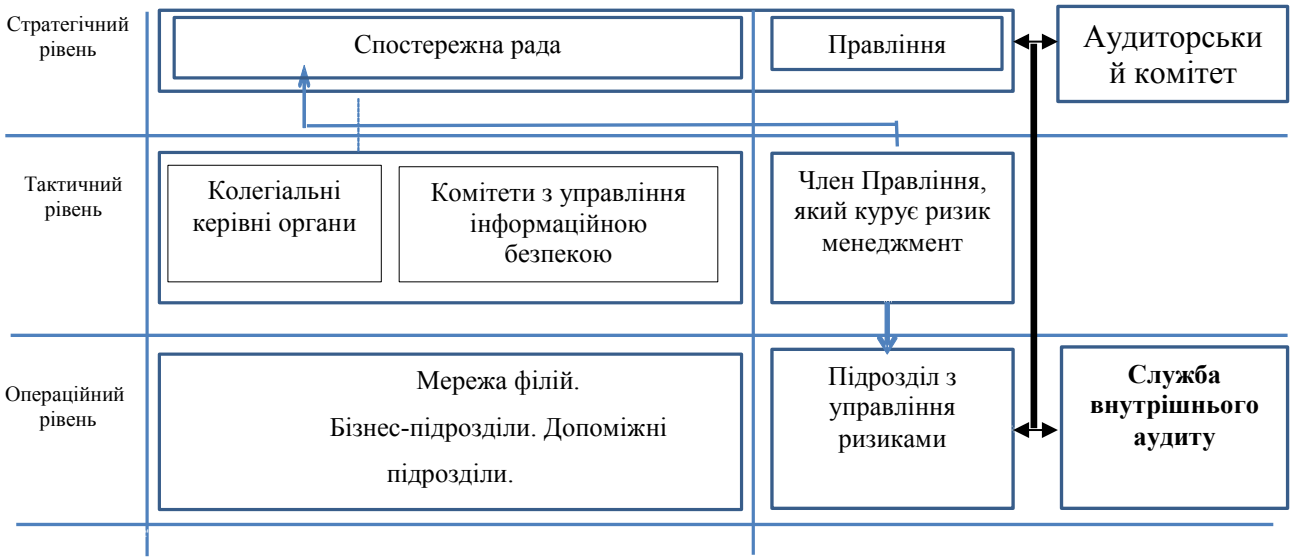

Рисунок 1.1 – Організаційно-управлінська підсистема забезпечення кібербезпеки банку

Джерело: складено авторами.

Отже, внутрішній аудит кібербезпеки має спрямовуватись на оцінку ефективності системи забезпечення кібербезпеки для того, щоб визначити, чи

відповідає вона стратегії та цілям діяльності банку на ринку в поточних умовах кібер-екосистеми. Для досягнення поставленої мети слід виконати значну кількість різноспрямованих завдань, а саме [30, 34, 1, 20, 35]:

– перевірити відповідність наявної політики кібербезпеки чинному законодавству, міжнародним стандартам та рекомендаціям;

– виявити недоліки та оцінити ефективність політики кібербезпеки банку, внутрішньобанківських стандартів, регламентів та процедур;

– оцінити поточний рівень захищеності інформаційних активів банку;

– провести аналіз ризиків, пов’язаних з можливістю реалізації загроз кібербезпеки щодо інформаційних активів;

– оцінити ефективність управління кібер-ризиками;

– на основі результатів аналітичної роботи виявити можливі вразливості інформаційних активів банку до зовнішніх та внутрішніх загроз втрати кібербезпеки;

– вивчити наявні засоби контролю кібербезпеки за операційними, адміністративними та управлінськими аспектами, забезпечити ефективне виконання норм кібербезпеки та відповідність встановленим стандартам кібербезпеки;

– розробити рекомендації щодо впровадження нових та підвищення ефективності наявних механізмів забезпечення кібербезпеки.

У число додаткових завдань служби внутрішнього аудиту можуть також входити розробка політик кібербезпеки та інших нормативних документів щодо захисту інформаційних активів та участь в їх впровадженні; постановка завдань для персоналу, що стосуються забезпечення захисту інформаційних активів та попередження реалізації внутрішніх та зовнішніх загроз кібербезпеці; участь у навчанні персоналу у сфері забезпечення кібербезпеки банку тощо [30, 34, 1, 20, 35].

Досягнення цих цілей та завдань забезпечується через створення та постійну модернізацію механізму внутрішнього аудиту кібербезпеки.

Узагальнюючи розробки науковців, механізм внутрішнього аудиту у сфері забезпечення кібербезпеки пропонуємо визначати як сукупність методологічної, методичної та технічної підсистем, що забезпечують ідентифікацію та структуризацію об’єктів, постановку цілей та завдань, вибір методів та процедур для отримання достатніх та належних аудиторських доказів, які дозволяють аргументувати висновки та рекомендації для забезпечення необхідного рівня кібербезпеки банку, як це представлено на рисунку 1.2.

Цей механізм має функціонувати на основі системи принципів внутрішнього аудиту. При цьому загальні принципи внутрішнього аудиту залишаються важливими. При структуризації принципів вважаємо за доцільне використовувати підхід Ю. Слободяник та виділяти:

– основоположні принципи, що відбивають сутність внутрішнього аудиту як суспільного явища (теоретична складова): незалежність; об’єктивність; системність; комплексність; компетентність; ефективність;

– методологічні принципи, що є основою його практики:

1) принципи професійної етики: чесність; об’єктивність; конфіденційність; професійна компетентність;

2) принципи організації: систематичність; оперативність; планування; збалансованість; документація; комунікація [36].

Окрім наведених вище принципів, доцільно враховувати також більш специфічні принципи, орієнтовані на аудит в системі забезпечення кібербезпеки банку:

– актуальність: відповідність механізму внутрішнього аудиту чинній нормативно-правовій базі, міжнародним рекомендаціям та стандартам та кібер-екосистемі;

– повнота: аудит має охоплювати всі об’єкти та сфери аудиту кібербезпеки, враховувати всі загрози та фактори, що можуть вплинути на ефективність механізму забезпечення кібербезпеки банку;

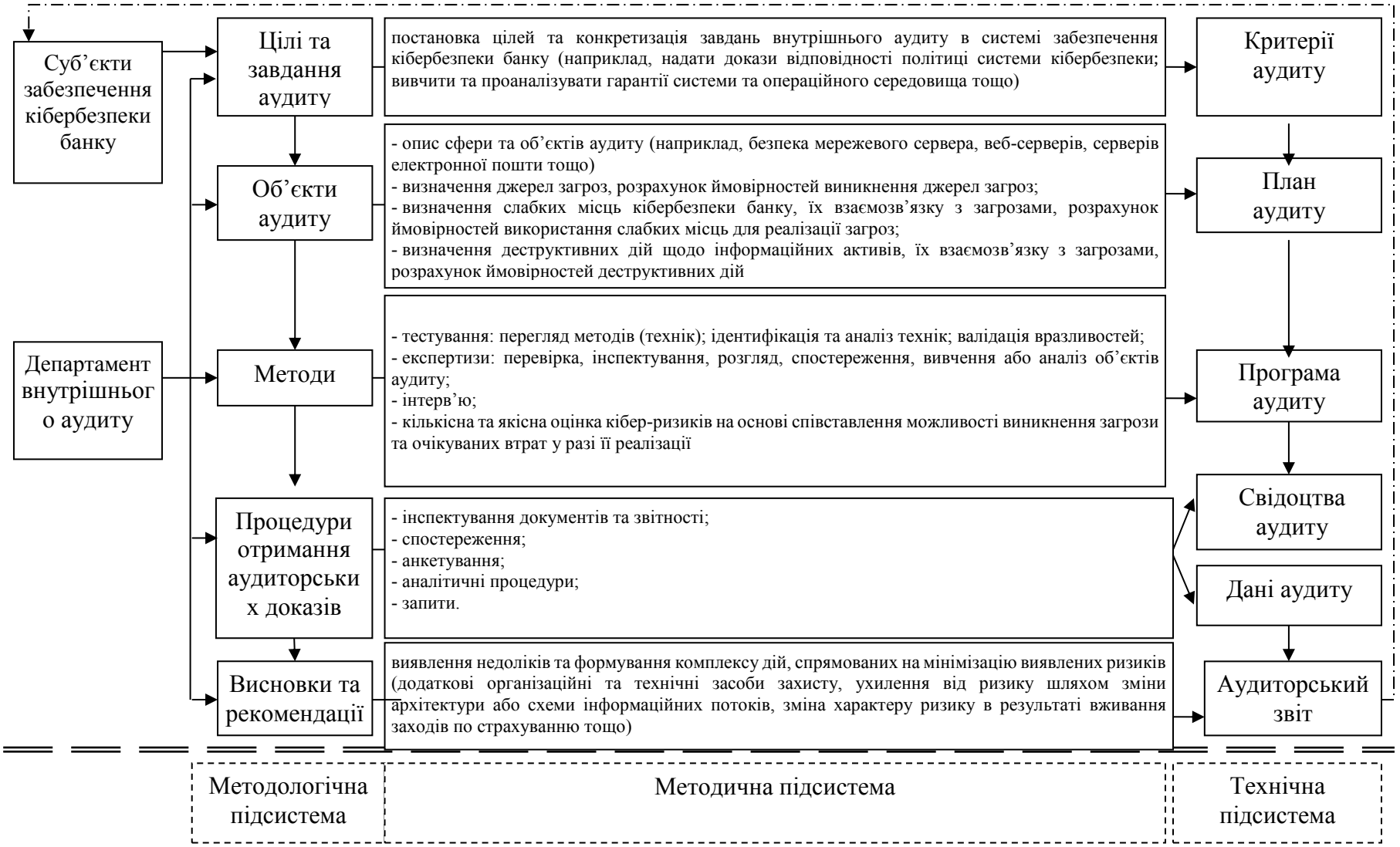

Рисунок 1.2 – Механізм внутрішнього аудиту в системі забезпечення кібербезпеки банку

Джерело: розроблено на основі [1, 38, 39, 36, 39]

– надійність: наявні підсистеми механізму внутрішнього аудиту дозволяють зробити послідовну оцінку кібер-ризиків або вимірювання об’єкта аудиту та обґрунтувати аудиторські висновки;

– періодичність відповідно до цілей внутрішнього аудиту: ефективна система внутрішнього аудиту має передбачати можливість проведення попереднього, регулярного, випадкового та нічного (неробочого) аудиту [34, 35, 37, 38, 39].

За результатами дослідження виявлено, що ландшафт кібер-екосистеми постійно змінюється, створюючи нові загрози втрати кібербезпеки банків та призводячи до зростання рівня кібер-ризиків. У цих умовах банки мають мати ефективну систему забезпечення кібербезпеки для усунення наявних та потенційних зовнішніх та внутрішніх загроз.

У цих умовах важливу роль для попередження кіберзагроз відіграє внутрішній аудит, що надає об’єктивну оцінку поточному рівню кібербезпеки в банку, виявляє слабкі місця в системі забезпечення кібербезпеки та управління кібер-ризиками та виробляє рекомендації щодо їх усунення.

Внутрішній аудит кібербезпеки визначено як періодичну систему збору та оцінки інформації для визначення того, чи забезпечують всі системи банку належний стан захищеності інформаційних активів та інформаційної інфраструктури, збереження властивостей інформаційних активів (доступності, цілісності чи конфіденційності) на цільовому рівні відповідно до встановлених критеріїв в умовах постійного впливу зовнішніх та або / внутрішніх загроз з дотриманням вимог національного та міжнародного законодавства.

Автори визначили, що система внутрішнього аудиту кібербезпеки являє собою сукупність взаємопов’язаних елементів (цілі та завдання, об’єкт, суб’єкт, механізм), що функціонують на основі загальних та спеціальних принципів та дозволяють об’єктивно оцінити рівень захищеності та збереження властивостей інформаційних активів та інформаційної інфраструктури банку в умовах постійного впливу зовнішніх та або / внутрішніх загроз, а також дотримання вимог національного та міжнародного законодавства.

1.2 Дослідження особливостей незалежного аудиту для попередження шахрайства банківського персоналу

Згідно зі звітом Асоціації сертифікованих фахівців із розслідування шахрайства [41], в 2018 році шахрайства нанесли організаціям у всьому світі фінансових збитків на загальну суму понад 7 млрд. доларів США. Згідно цього звіту найбільша кількість випадків шахрайства у фінансовому секторі фіксується в банках, причому кількість виявлених випадків шахрайства за участі банківського персоналу набагато перевищує кількість випадків зовнішнього шахрайства. На жаль, попередити шахрайство банківського персоналу на рівні внутрішньобанківських технологічних засобів або регламентів сьогодні практично неможливо [42]. У зв'язку з цим надзвичайно актуальною та практично значущою є проблема організації системи незалежного аудиту для попередження шахрайства банківського персоналу. Втрати від шахрайств у банках зростають швидшими темпами, ніж витрати на боротьбу з ними [43].

Гострота проблеми шахрайства персоналу в банківській діяльності обумовлює необхідність активної протидії та запобігання йому. Шахрайство є результатом непостійного та неповного контролю загального процесу управління функціонуванням банку [44]. Як зазначено в роботі [45], моніторинг шахрайства персоналу банку поєднує в собі алгоритми виявлення видів шахрайства, що зустрічаються найчастіше, а також комплексну аналітику з поведінковим профілюванням для виявлення найбільш складних випадків шахрайства. Потужна система внутрішнього контролю банку являється найефективнішим способом попередження шахрайств і зменшення збитків від них.

В роботі [46] внутрішній аудит кібербезпеки банку розглядається як система збору та аналізу інформації для визначення рівня захищеності об'єктів внутрішнього аудиту – інформаційних активів та інформаційної інфраструктури, а також збереження властивостей інформаційних активів (доступності, цілісності та конфіденційності). Його метою є визначення відповідності системи

кібербезпеки банку стратегії та цілям діяльності банку, а завданнями – надання доказів відповідності системи кібербезпеки політиці банку, вивчення гарантій системи кібербезпеки та операційного середовища тощо.

Ми вважаємо, що система кібербезпеки банку повинна відповідати міжнародному стандарту ISO/IEC 27001 «Управління інформаційною безпекою» [47], який містить специфікації щодо обов'язкових політик безпеки, яких слід дотримуватися банку, а також документацію щодо процесів та процедур, які повинні застосовуватися в банку на постійній основі. Внутрішній аудит кібербезпеки банку повинен визначити ступінь відповідності банку вимогам стандарту ISO/IEC 27001 «Управління інформаційною безпекою», а також базовий рівень кібербезпеки для подальшого вдосконалення системи кібербезпеки банку. Для цього внутрішній аудит кібербезпеки банку повинен використовувати відповідні методи оцінювання поточної ситуації в сфері кібербезпеки банку, необхідні для прийняття обґрунтованих управлінських рішень [48].

Метод аналізу розривів може бути використаний для оцінки того, наскільки банк дотримується вимог кібербезпеки. Отриманий в результаті аналізу розривів аудиторський звіт містить сфери діяльності банку, в яких вимоги кібербезпеки успішно виконуються, а також рекомендації щодо задоволення вимог кібербезпеки, що не виконуються.

Метод оцінки ризику може бути використаний для оцінювання рівня потенційного ризику кібершахрайства в розрізі персоналу, банківських процесів і технологій, а також впливу, який він може мати на функціонування банку. Цей метод дозволяє отримати відповідь на питання, наскільки ефективно система кібербезпеки банку зменшує ризики кібершахрайства, а також наскільки захищеними є інформаційні активи та інформаційна інфраструктура банку.

Як зазначено в роботі [49], у випадку шахрайства персоналу службі внутрішнього аудиту банку важко забезпечити повну незалежність в діях і неупередженість у судженнях, тому особливого значення набуває зовнішній аудит банку незалежними експертами, що є поширеною практикою в іноземних

банках. До того ж в Міжнародному стандарті професійної практики внутрішнього аудиту 1200 «Професійна компетентність та належна ретельність» зазначено, що «внутрішні аудитори повинні мати достатні знання для того, щоб оцінити ризик шахрайства та спосіб управління таким ризиком в організації, але не передбачається, що внутрішній аудитор повинен володіти такою ж компетенцією, що й особа, основним обов'язком якої є виявлення та розслідування фактів шахрайства» [50]. Основними характеристиками зовнішнього аудиту є:

1) незалежність і об'єктивність (незаангажованість у судженнях);

2) вдосконалення системи кібербезпеки банку, що передбачає можливість оцінити ризики шахрайства банківського персоналу, слабкі сторони системи кібербезпеки банку та дати рекомендації, спрямовані на підвищення ефективності системи кібербезпеки банку.

Залучені незалежні експерти, що спеціалізуються на виявленні шахрайства в банку, часто використовують системи фрод-моніторингу інформації, отриманої банком під час ведення бізнесу [51]. Метою фрод-моніторингу в банку згідно [45] є попередження шахрайства при наданні кредитів, шахрайства при здійсненні депозитних операцій, шахрайства в сфері дистанційного банківського обслуговування, шахрайства з банківськими платіжними картками, шахрайства при здійсненні розрахункових операцій, шахрайства, пов'язаного з неправомірними діями персоналу тощо. В роботі [52] наведено перелік об'єктів, які на думку автора доцільно перевіряти системою фрод-моніторингу:

– активність рахунку, коли персонал у власних цілях використовує «сплячі рахунки»;

– власників рахунків, якщо власник присутній у «чорному списку» або є іноземцем, померлим тощо;

– ліміти по операціям, що здійснюються у відповідності з вимогами Національного банку України, політикою банку, посадовими інструкціями тощо, в результаті чого виявляються надлишки по лімітам;

– активності банківських співробітників на предмет дотримання банківських нормативів, які співробітник може перевищувати чи недовиконувати;

– операції працівників на відповідність належним їм правам доступу;

– операції працівників на відповідність політиці безпеки банку.

Результати роботи системи фрод-моніторингу накопичуються в базі даних шахрайств, обробляються та надсилаються відповідним підрозділам банку. Це дозволяє більше ніж на 50% знизити фінансові збитки від шахрайства персоналу [41]. Як зазначено в роботі [51], виявлення аномалій поведінки співробітників банку є приводом для додаткової перевірки діяльності цих співробітників. Ми вважаємо, що в ході зовнішнього аудиту доцільно оцінювати ефективність системи кібербезпеки банку в напрямку зменшення ризику шахрайства персоналу банку.

Згідно Положення з міжнародної практики аудиту 1006 «Аудит фінансових звітів банку» типові шахрайські дії управлінського персоналу та працівників банку включають в себе [49]:

– незаконне привласнення активів:

1) депозитні операції: маскування вкладів; невідображення депозитів у обліку; крадіжка депозитів клієнтів; неправильне визначення відсотків за вкладами;

2) кредитні операції: надання кредиту на підроблені чи незаконно отримані документи; позики фіктивним позичальникам; продаж заставного майна за ціною, що нижча за ринкову; підкупи для отримання звільнення від застави чи для зменшення суми позову; не подання інформації про заставне майно для внесення її у державні реєстри обтяжень; завищення вартості активів, що оцінюються з метою передачі у заставу для отримання кредиту; помилки у визначенні фінансового стану та класу позичальника;

3) поточні рахунки: незаконне привласнення коштів з рахунків, за якими часто проводяться транзакції;

– неправдиве відображення фінансової звітності:

1) навмисні викривлення;

2) пропуск загальних сум;

3) виправлення облікових записів;

4) некоректне відображення позик на рахунках простроченої чи строкової заборгованості.

Як показано на рисунку 1.3, найбільше збитків у світі в 2018 році було заподіяно через такі типи шахрайства персоналу [41]: неправдиве відображення фінансової звітності (10% випадків), корупція (38% випадків), незаконне привласнення активів (89% випадків).

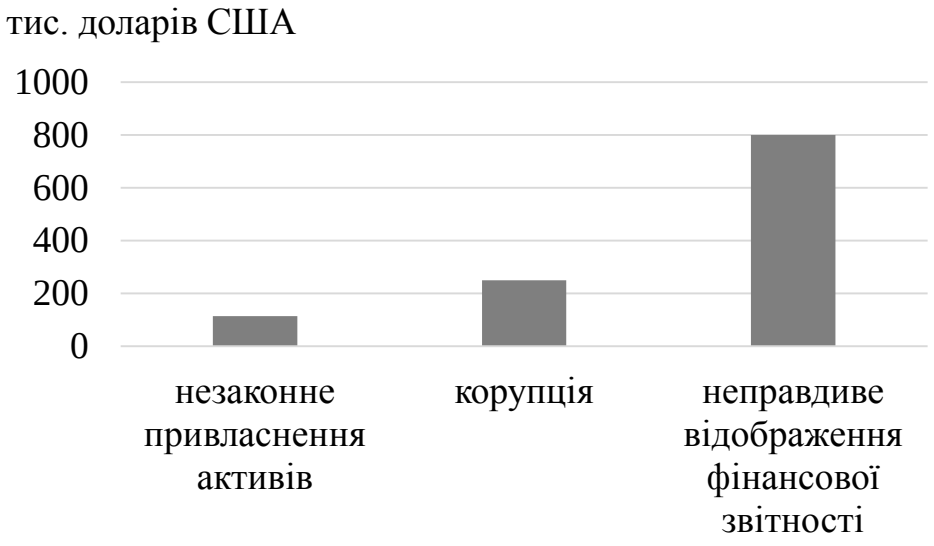

Рисунок 1.3 – Медіана фінансових збитків за типами шахрайства персоналу

Таким чином, для попередження шахрайств банківського персоналу складовою частиною системи незалежного аудиту має бути оцінювання ризику шахрайства персоналу в напрямах неправдивого відображення фінансової звітності та незаконного привласнення активів. Це створює умови для використання ризик-орієнтованого підходу при побудові плану аудиту. В роботі

[53] представлена нечітко-множинна модель, побудована на основі індикаторів ризику шахрайства персоналу, наведених, наприклад, в [54], яка надає системі незалежного аудиту можливість оцінити ризик шахрайства банківського персоналу та визначити основні сфери, що найбільше сприяють шахрайству. На нашу думку, система незалежного аудиту для попередження шахрайств банківського персоналу повинна використовувати базу даних, заповнену системою фрод-моніторингу, а також перевіряти реакцію відповідних підрозділів банку на випадки шахрайств банківського персоналу.

Для виявлення шахрайства персоналу в ході незалежного аудиту доцільно також використовувати так звані «золоті правила» аудитора, що вимагають від нього [55]:

– намагатись з’ясувати причину відхилень;

– не розглядати питання довіри до людей тільки в залежності від їхнього становища в суспільстві;

– не припускатися думки, що шахрайство неможливе на цьому підприємстві;

– відчувати особисту відповідальність за виявлення шахрайства;

– при виявленні потенційних проблем посилити контроль з метою зниження ризику;

– знати ситуації, що супроводжуються значним ризиком шахрайства, та їх ознаки.

Проаналізуємо економіко-математичні методи, що можуть бути використані для виявлення шахрайств персоналу в банківській сфері. Найбільш поширеними шахрайствами в банках є відмивання «брудних» грошей, шахрайства з кредитами та незаконне привласнення активів [50]. Першою причиною вчинення шахрайства є фінансові труднощі шахрая. Другою – існування можливості для вчинення шахрайства. Третьою – впевненість шахрая в існуванні вагомих причин для вчинення ним шахрайських дій.

Левова частка банківських шахрайств відбувається з кредитними картками. Відомо, що шахрайство з кредитними картками включає незаконне використання кредитної картки чи її інформації без відома власника. У роботі [56] зазначено, що сьогодні для виявлення таких шахрайств широко застосовуються: логістична регресія, яка здатна розв'язувати категоріальні класифікаційні задачі; метод опорних векторів (SVM, Support Vector Machine), який здатний обробляти незбалансовані дані та складні зв'язки між змінними; зручні у використанні дерева рішень; випадковий ліс (random forest); самоорганізовані карти Кохонена (SOM, Self-Organizing Map), які використовуються для класифікації та кластеризації; нечітка логіка, яка підвищує ефективність управлінських рішень. На нашу думку, при наявності невизначеностей найкращі результати дає застосування нечітких методів [53]. Однак слід зважати на те, що основним недоліком останніх є їх не надто висока точність, тому з метою її підвищення краще використовувати гібридні нейро-нечіткі системи (ANFIS, Adaptive Neuro-Fuzzy Inference System). Незважаючи на цілком пристойні результати, що дає метод опорних векторів, він чутливий до збільшення кількості даних і не може підтримувати великі набори даних [56].

В свою чергу для виявлення викривлень фінансової звітності в банківській сфері широко застосовуються: нейронні мережі, які здатні впоратися з задачами без алгоритмічного рішення; байєсові мережі, що використовуються для виявлення аномалій; генетичні алгоритми, які використовуються для бінарної класифікації; текст майнінг (text mining), який використовується для кластеризації та виявлення аномалій. В роботі [56] зазначається також, що сучасною тенденцією виявлення шахрайства є використання гібридних методів, які використовують сильні сторони різних методів.

Виявлення фінансового шахрайства включає моніторинг поведінки власників карткових рахунків із метою виявлення їх небажаної поведінки. В роботі [57] для цього використовується генетичний алгоритм, у якому замість максимізації кількості правильно класифікованих транзакцій, визначається цільова функція зі змінними, що представляють втрати від помилкової

класифікації. Таким чином правильна класифікація одних транзакцій являється більш важливою ніж інших. На першому кроці запропонованого в [57] алгоритму вводяться початкові дані – транзакції власника карткового рахунку, кожна з яких має набір стандартизованих атрибутів, шо описують поведінку власника карткового рахунку. До початкових даних включаються, наприклад, такі змінні: кількість разів, що використовувалась картка; місцезнаходження картки в момент її використання; баланс, доступний на картковому рахунку; середньодобова сума грошей, що знімалася власником карткового рахунку тощо. На другому кроці в результаті роботи генетичного алгоритму розраховуються критичні значення вищезазначених змінних. Далі ці критичні значення використовуються разом з технологіями Data Mining. Ми вважаємо, що аналогічний підхід може бути використаний також для виявлення шахрайств з рахунками, що здійснюються персоналом банку.

В роботі [58] для моніторингу поведінки власників карткових рахунків використовується прихована марківська модель (HMM, Hidden Markov Model), яка спочатку навчається нормальним діям власника картки, а потім використовується для виявлення шахрайської поведінки. В роботі [59] для моніторингу поведінки власників карткових рахунків використовується теорія нечіткої логіки.

Підсумовуючи вищенаведене, можемо представити результати порівняльного аналізу економіко-математичних методів виявлення шахрайств у банках, що здійснюються персоналом банку, у вигляді наступної таблиці 1.3. Оптимальними для врахування невизначеності та виявлення шахрайств у банках є гібридні методи, що використовують сильні сторони різних підходів.

Отже, за результатами проведеного дослідження можна зробити такі висновки та рекомендації. Підтверджено, що незалежний аудит є важливим елементом протидії шахрайству, яке здійснюється персоналом банку. Він оцінює ефективність системи кібербезпеки банку з точки зору зменшення ризику шахрайства персоналу банку. Встановлено, що в системі незалежного аудиту доцільно використовувати сучасні методи виявлення та попередження

шахрайства персоналу. До них відносяться стандарт ISO/IEC 27001 «Управління інформаційною безпекою», метод аналізу розривів, метод оцінки ризиків, система фрод-моніторингу тощо. Якісні методи враховують невизначеність за допомогою суб'єктивних експертних оцінок. Кількісні методи базуються на традиційному математичному апараті, а методи машинного навчання – на технологіях штучного інтелекту. Вони враховують невизначеність за допомогою засобів статистики та теорії ймовірностей.

Таблиця 1.3 – Порівняльний аналіз економіко-математичних методів виявлення шахрайств у банках, що здійснюються персоналом банку

Група методів виявлення шахрайств у банках	Основні характеристики	Урахування невизначеності
Кількісні (використання закону Бенфорда, асоціативний аналіз, логістична регресія, прихована марківська модель)	Базується на традиційному математичному апараті	Невизначеність враховується за допомогою засобів статистики та теорії ймовірностей
Машинне навчання (метод опорних векторів, дерево рішень, нейронні мережі, самоорганізовані карти Кохонена, байєсові мережі, генетичні алгоритми, текст-майнінг)	Базуються на технологіях штучного інтелекту (навчання з учителем і без нього)	Невизначеність враховується за допомогою засобів статистики та теорії ймовірностей
Якісні (нечітка логіка)	Базуються на експертних оцінках	Невизначеність враховується за допомогою експертних оцінок
Гібридні (нейро-нечіткі системи)	Базуються на синергетичному підході (використовуються сильні сторони різних методів)	Невизначеність враховується за допомогою кількісного та якісного математичного апарату

Оптимальними для врахування невизначеності та виявлення шахрайств у банках є гібридні методи, що використовують сильні сторони різних підходів. Своєчасне проведення заходів незалежного аудиту із використанням цих методів дозволяє знизити рівень шахрайства та підвищити відповідальність банківського персоналу. Особливо перспективним є ризик-орієнтований підхід, на основі якого доцільно складати план аудиту. Він використовує модель оцінки ризику,

побудовану на основі індикаторів ризику шахрайства персоналу, та дає можливість визначити сфери, які найбільше сприяють шахрайству банківського персоналу.

1.3 Роль фінансового моніторингу в сучасній системі кібербезпеки банку

У ринкових умовах господарювання національну економіку можна розглядати як цілісну відкриту систему, що функціонує у доволі складному зовнішньому та внутрішньому середовищі, якому притаманні постійна динаміка, нестабільність та ризик. Ці чинники спричинюють необхідність оперативної трансформації економіки України до нових умов та виникаючих загроз, передбачають обов'язковий пошук стратегічних орієнтирів і шляхів провадження ефективної економічної діяльності, своєчасного забезпечення потрібного рівня економічної безпеки.

Для вирішення вищезазначених питань у країні повинна існувати ефективна, дієва система економічної безпеки, що являє собою багатоскладове поняття, яке потрібно розглядати як сукупність певних частин, що формують її загальний стан. А одним з головних елементів в сучасній системі забезпечення економічної безпеки національної економіки повинен бути фінансовий моніторинг. Зважаючи на особливості здійснення фінансового моніторингу, керівництву держави, установ, організацій і підприємств потрібно враховувати ряд важливих питань стосовно наукового, інформаційно-аналітичного, інноваційного, стратегічного, прикладного забезпечення відповідного рівня їх економічної безпеки. Забезпечення зваженої та обґрунтованої політики в області здійснення моніторингу фінансових процесів і операцій є надзвичайно актуальним питанням на сучасному етапі провадження ефективної трансформації національної економічної системи, особливо в частині підтримання її безпеки.

У світовій науковій літературі вивченням загальнотеоретичних питань забезпечення економічної безпеки займаються такі науковці Небава М.І., Міронова Ю.В., Лук'янова В.В., Головач Т.В., Підхомний О.М., Мадзіновська Х.О., Корелін В.В., Габуніа Н.Г. та інші [61, 62, 63, 64, 65].

Окрема група науковців Іващенко Г.А., Кавун С.В., Прокопішина О. В. [66, 67, 68] досліджують більш вузьке поняття стосовно забезпечення економічної безпеки підприємств, їх специфіку, особливості, інструменти. Ряд авторів приділяють увагу дослідженню питань фінансової безпеки Василишин Т.С., Небава М.І., Міронова Ю.В., Підхомний О.М. [69, 61, 65].

Дослідженню проблеми фінансового моніторингу присвячено праці наступних вчених Новак О.С., Дмитров С.О., Кузьменко О.В., Куришко О.О., Петрк О.М. та багато інших [70, 71, 72, 73]. Більш вузьким питанням, що направлені на протидію легалізації (відмиванню) коштів, одержаних злочинним шляхом та фінансуванню тероризму особливу увагу приділяють такі вітчизняні та зарубіжні науковці як Зеленецький В.С., Гуржій С.Г., Клюшке С.М., Кірсанов В.М., Шнейдер Ф. [74, 75, 76].

Загальне поняття економічної безпеки передбачає забезпечення захищеного від негативного впливу зовнішніх і внутрішніх загрозливих факторів, стабільного економічного та фінансового розвитку суспільства, метою яких є найефективніше використання наявних ресурсів шляхом виробництва необхідних населенню продуктів і послуг, що задовольнятимуть як суспільні, так і індивідуальні потреби, для покращення добробуту громадян [61, 62, 64]. Економічна безпека є невід'ємною частиною національної безпеки.

Зауважимо, що складовими економічної безпеки виступають виробнича, продовольча, інвестиційна, зовнішньоекономічна, макроекономічна, науково-технологічна, соціальна, демографічна, енергетична, а також фінансова безпека [61, 64]. Так, виробнича безпека передбачає дотримання певного рівня промисловості держави, за якого економіка країни буде відтворюватись, матиме сталий розвиток та почне зростати. Під забезпеченням продовольчої безпеки розуміємо необхідний рівень продовольчого забезпечення населення, що

підтримує постійний розвиток у країні, налагодження економічної, політичної, соціальної стабільності серед населення, якісний розвиток особистості та нації. Інвестиційна безпека – це відповідний розмір національних та іноземних інвестицій, їх оптимальне співвідношення, які можуть підтримувати позитивну економічну динаміку в довгостроковій перспективі, за умови належного рівні фінансового забезпечення наукової та технічної сфери, інноваційних проектів. Вагомим елементом економічної безпеки виступає зовнішньоекономічна безпека, яка передбачає забезпечення відповідності зовнішньоекономічних процесів національним економічним інтересам держави, а також направлена на мінімізацію державних збитків від впливу негативних зовнішніх економічних факторів, налаштування позитивних умов для росту економіки шляхом активної співпраці з країнами світу. Під макроекономічною безпекою розуміється встановлення такого економічного стану, що може збалансувати макроекономічні пропорції у економічних процесах держави. Досить вагомим елементом економічної безпеки є науково-технологічна безпека, що являє собою стан науково-технологічного, а також виробничо-технічного потенціалу країни; надає можливість організовувати та підтримувати належну роботу національної економіки, що має достатній рівень, щоб створювати конкурентоздатну спроможність вітчизняних товарів та послуг; забезпечує державну незалежність через застосування власних науково-інтелектуальних та техніко-технологічних ресурсів країни. Соціальна безпека передбачає стан державного розвитку, за якого вона спроможна, не залежачи від будь-яких негативних зовнішніх і внутрішніх чинників, підтримувати якісний життєвий рівень для свого населення. За демографічної безпеки налаштовується захищеність країни та населення від можливих демографічних загроз; досягаються розвиток держави зі взяттям до уваги сукупних інтересів країни, суспільства, кожної особистості згідно до законодавчо-нормативних прав громадян. Не менш важливою є й енергетична безпека – це такий певний економічний стан, що спроможний забезпечити належний захист національних інтересів від існуючих та можливих внутрішніх та зовнішніх небезпек у сфері енергетики; дозволяє задовольняти

існуючі потреби в необхідних паливно-енергетичних ресурсах з метою підтримання життєдіяльності населення країни, а також відповідного позитивного функціонування національної економіки як за звичайних умов, так і в режимі надзвичайного та, навіть, воєнного стану. Одним з найважливіших елементів економічної безпеки виступає фінансова безпека, що передбачає такий стан грошово-кредитної, валютної, бюджетної, банківської системи, а також фінансових ринків, якому притаманні стійкість до негативних внутрішніх і зовнішніх шоків, збалансованість, спроможність налагодити ефективну діяльність системи національної економіки, а також забезпечити стале економічне зростання [61, 65, 69].

Разом з тим, зазначимо, що сучасній глобальній економіці [61, 71] притаманні ряд процесів, таких як: комплексна автоматизація, механізація, інформатизація. Крім того, сучасній світовій економічній безпеці характерні нові проблеми, які спричинюють загострення глобальної економічної та фінансової небезпеки країн, можливе подальше економічне відставання країн, виникнення продовольчої кризи, збільшення потоків нелегальних коштів, загострення питань фінансового моніторингу, направлення значної кількості ресурсів на подолання ризиків, пов’язаних із воєнною та терористичною діяльністю та інші. Ці питання можливо вирішити через вивчення та аналіз міжнародної економічної ситуації, сформованої під впливом певних особливостей різних країн.

Поняття міжнародна економічна безпека характеризується процесами взаємодії країн, що передбачають навмисне нанесення збитків економічним та фінансовим інтересам країн. До таких процесів збільшення міжнародної економічної небезпеки входять: порушення у відносинах міжнародної торгівлі; недоступність стратегічних ресурсів певним країнам із-за їх здороження або за певних політичних умов; поширення позитивних умов одними країнами для відтоку висококваліфікованого персоналу з інших держав; створення штучних перешкод в процесі обміну досвіду новими технологіями [61, 71].

Для розуміння процесів міжнародної економічної безпеки та впливу на її формування, необхідно дослідити проблеми становлення національної

економічної безпеки, що трактується як спроможність економіки країни забезпечити собі стабільний, незалежний розвиток, забезпечити стале суспільне становище, підтримати необхідне оборонне забезпечення держави, здатність країни захищати національні інтереси від загроз зовнішнього та внутрішнього характеру, а особливо стимулювати та підтримувати науково-інтелектуального та інноваційно-проектного розвитку [64, 69, 77].

Більш вузьке поняття, що допомагає забезпечувати національну економічну безпеку, є економічна небезпека регіонів [61] описується таким негативними чинниками, як: нерівномірність фінансового забезпечення різних регіонів, виникнення продовольчої залежності, деградація виробничо-технічних можливостей, зростання кількості безробітних, загострення екологічної ситуації.

Таким чином, зазначимо, що основою загальної економічної безпеки є економічна безпека суб'єктів господарювання [66, 67, 68], що являє собою забезпечення захищеності їх діяльності від руйнівних чинників зовнішнього та внутрішнього середовища, спроможність оперативно подолати загрози, пристосуватись до актуального стану; найбільш результативні способи використання існуючих ресурсів для стабільної діяльності.

Отже, між різними ієрархічними рівнями забезпечення економічної безпеки наявні тісні взаємозв'язки, що формуються залежно від національних особливостей країн світу, які мають якісно різні принципи, підходи та чинники забезпечення економічної безпеки кожної держави.

Аналізуючи досвід різних країн світу щодо забезпечення економічної безпеки національної економіки, необхідно виділити певні чинники економічної безпеки в першу чергу для розвинених країн. Таким чинниками налагодження економічної безпеки країни виступають: розробка ефективних стратегій роботи суб'єктів економіки та захисту від можливих ризиків; створення та забезпечення сприятливого, прозорого та відкритого ринкового, економічного, правового середовища; зосередження уваги та ресурсів на теоретико-прикладних інноваційних програмах і проектах; забезпечення та підтримання соціального захисту суспільства.

Додатково до виділених чинників забезпечення економічної безпеки держави, для протистояння та боротьби з ризиками, пов'язаними з економічною небезпекою, урядами розвинених країн провадяться певні організаційні заходи [63, 66, 68, 77]. Для більшості розвинених країн світу спільним є забезпечення відповідних гарантій по інвестиціям в акціонерний капітал підприємства, а також надання гарантій за запозичення підприємств, не привабливих для звичайного банківського кредитування. Особливе місце у безпеці країн займають страхові фонди та організації, що виступають основними ризико знижуючими факторами. Економічні ризики завдають певні дії з боку монополістів великого бізнесу, які законодавчо контролюються та регулюються законодавствами багатьох країн. Для всебічного аналізу регулювання економічних ризиків, розглянемо приклади державного контролю у таких країнах як США, Японія, Франція та Великобританія. Аналіз цих країн дозволить комплексно охарактеризувати систему регулювання та контролю економічних ризиків в країн з різними економічними моделями розвитку. Ці країни мають розвинуту підприємницьку діяльність, а разом з тим є інвестиційно привабливими, що збільшує ймовірність економічних ризиків. Розглянемо детальніше кожну з країн.

Так, у США створюються конкретні структурні одиниці, що займаються забезпечення економічної безпеки за галузево-територіальною направленістю, такі як Адміністрація малого бізнесу та відповідні регіональні підрозділи Міністерства внутрішньої безпеки малих підприємств.

У економічному досвіді Японії використовують поряд з офіційно закріпленою Міністерством економіки, торгівлі та промисловості стратегічною документацією з питання економічної небезпеки, додаткові офіційні документи, розроблені у складі одного з основних напрямків, а саме спеціальні тактичні документи щодо операційних завдань посилення фінансової підтримки підприємств, покращення умов заснування нових організацій, всебічний розвиток національної системи забезпечення економічної безпеки.

Що стосується Європи, то у Франції наприкінці 1990-х уряд Франції прийняв низку нормативних законів для поліпшення соціально-економічної

безпеки бізнесу. Соціально-економічна безпека Франції регулювалася наприкінці 20 століття трьома способами [66]. По-перше, закон визначає захист ділових активів, інтелектуальної власності та захист ділової інформації та систем управління, тобто захист усіх ділових активів. Іншим напрямком було запровадження постійного моніторингу конкурентів на внутрішньому та зовнішньому ринках та встановлення критеріїв, за якими компанії підпорядковуються конкуренту. Останнім напрямом було регулювання кризових явищ в економіці державою, з одного боку, та економістами, з іншого. Особлива увага приділяється виявленню та своєчасному запобіганню загроз внаслідок неефективних управлінських рішень, оскільки бракує інформації, необхідної для управління бізнесом.

Соціально-економічні заходи забезпечення економічної безпеки підприємств Великобританії ґрунтується на ефективній правовій базі, яка включає в себе дієву нормативно-правову базу.

Таким чином, спільним для Японії, Великобританії, Франції та США є захід, що передбачає проведення систематичного моніторингу як зовнішнього, так і внутрішнього ринків, і відповідне створення рекомендацій для державних органів і підприємств для захисту економічних інтересів і покращення конкурентної позиції національних підприємств [66, 68, 77].

На основі вищезазначеного аналізу сутності економічної безпеки та її складових, можемо обґрунтувати роль фінансового моніторингу в сучасній системі забезпечення економічної безпеки національної економіки. Завдяки своїй розподільчій функції фінансова сфера виступає особливо вагомим фактором національної економіки. Тому більш детально розглянемо особливості саме фінансової безпеки.

Фінансова безпека як елемент економічної безпеки представляється в багатьох аспектах, з урахуванням ряду питань, що в свою чергу включають її складові елементи [61, 65]:

– грошово-кредитна безпека (являє собою стан грошово-кредитної системи країни, що передбачає стійкість національної грошової одиниці,

доступна ціна кредитних коштів, помірний рівень інфляції, за якого досягається ріст реального доходу населення держави),

– валютна безпека (передбачає стан курсоутворення у країні, що забезпечує стабільний розвиток експорту, залучення до країни іноземних інвестицій, забезпечує надійний захист від коливань на міжнародних валютних ринках, обумовлює влиття країни до економічної системи світу),

– бюджетна безпека (обумовлює належний стан платоспроможності економіки країни шляхом збалансування дохідної та витратної частин державного та місцевих бюджетів, а також за допомогою ефективного використання коштів з відповідних бюджетів),

– боргова безпека (це такий оптимально співвіднесений стан зовнішнього та внутрішнього боргу країни, що є достатній, щоб мати змогу для вирішення соціально-економічних потреб суспільства, за умови недоторканності суверенітету національної фінансової системи, а також покриття витрат на обслуговування такого зобов'язання).

Інша градація [69]:

– безпека страхового ринку (включає забезпечення належного стану достатності фінансових ресурсів у страхових компаній, що є можливим для здійснення страхових виплат за укладеними угодами),

– безпека фондового ринку (це такий оптимальний розмір капіталізації національного ринку, що спроможний налаштувати стійке фінансове становище всіх учасників ринку цінних паперів окремо та країни загалом),

– безпека банківської системи (визначає певний стан на ринку банківських послуг, що забезпечує задоволення фінансових потреб держави та населення, шляхом здійснення необхідних банківських операцій із застосуванням обов'язкових вимог фінансового моніторингу).

В межах дослідження фінансової безпеки пропонується окремо розглянути основні інструменти забезпечення фінансової безпеки:

– інструменти роботи з ризиками (страхування, диверсифікація, хеджування та ін..);

– інструменти забезпечення технічного захисту (безпека інформації, охорона, політика роботи з персоналом);

– фінансові інструменти (фінансовий моніторинг, бюджетування, управлінський контроль) [62].

Особливої уваги потребують інструменти забезпечення фінансової безпеки, що безпосередньо пов’язані з регулюванням процесів фінансового моніторингу [62]:

– фінансовий моніторинг (забезпечує облік аналіз та контроль грошових потоків, контроль за відхиленнями фінансового стану організацій),

– бюджетування (прогнозування доходів та видатків, резервування грошових коштів для покриття можливих загроз),

– управлінський контроль (проведення стимулювання суб’єктів фінансових процесів).

Вивчаючі приведені інструменти забезпечення фінансової безпеки, наголосимо, що серед них вагоме значення має саме фінансовий моніторинг. А отже, пропонується фінансовий моніторинг розглядати як систему заходів, що передбачає підвищення рівня фінансової, а відповідно і економічної безпеки держави шляхом здійснення контролю за фінансовими операціями зменшення обсягів фінансових злочинів, а саме: зростання рівня конкурентоздатності держави, скорочення розмірів тіньової економіки, зростання надійності банків, збільшення надходжень до бюджету держави від конфіскованого нелегального майна, сплати податків від виявлених незаконних доходів, скорочення корупції, збільшення ефективності застосування бюджетних ресурсів [70, 71, 73]. Так фінансовий моніторинг з однієї сторони допомагає держаним органам мати чітке уявлення про економічну активність у країні, а також з іншої сторони виступає засобом здійснення фінансового контролю за економічними процесами.

Фінансовий моніторинг дає можливість не лише фіксувати наявну небезпеку, а й прогнозувати, виявляти загрози, що можуть виникнути у майбутньому.

Вивчаючи особливості практичного застосування фінансового моніторингу, варто зауважити, що на даний час у світовій економіці налагодились доволі розгалужені, складні підпільні банківські системи, що здійснюють перекази значних коштів уникаючи систему фінансового моніторингу, не використовуючи необхідних затверджених банківським процесів [72, 73, 75]. Цілями незаконного обігу коштів виступають, наприклад, і ухилення від податків підприємцями, і укриття коштів фізичних осіб, фінансування злочинної діяльності, фінансування терористичної діяльності, та багато інших.

Слід наголосити, що негативний небезпечний вплив таких дій стосується не тільки економічної безпеки конкретної держави, а й безпеки інших країн і світової економіки взагалі. Небезпечність таких злочинів посилюється ще й їх міжнародним характером, так як кошти перераховують з країни у країну, негативно впливаючи на національну безпеку як мінімум двох країн. В подальшому легалізовані незаконні кошти вливаються у проведення наступних злочинів. Країни, що не залучаються до міжнародного співробітництва з питань фінансового моніторингу, підлягають жорстким заходам впливу, санкціям, що призводить до отримання такими країнами чималих збитків, спричиняє ускладнення зовнішньої діяльності, погано впливає на рейтинги та авторитет певних країн серед світового співтовариства [73, 75]. Тому що тільки спільними зусиллями можливо боротися з незаконними діями, нелегальними коштами, небезпечною діяльністю, що підривають фінансово-економічну систему.

Варто зазначити, шо в Україні розроблено та затверджено нормативно-правові законодавчі акти і документи щодо організації та здійснення фінансового моніторингу сумнівних та ризикових операцій. Зауважимо, що національна система фінансового моніторингу заснована та функціонує на базі наступних принципів: виділено конкретний перелік ознак по ризиковим операціям, що підлягають фінансовому моніторингу; затверджено мінімальні суми операцій,

при досягненні чи перевищенні яких операції, що відповідають певним критеріям, підлягають обов'язковій фіксації та перевірці; закріплено відповідальність інформувати спеціальний державний орган певними працівниками фінансових установ, банків щодо операцій, що відповідають визначеним характеристикам; встановлено право фінансових установ, банків зупиняти та відмовляти у проведенні сумнівних фінансових операцій; організовано та наділено відповідними повноваженнями спеціальний державний орган виконавчої влади щодо організації та координації роботи державних контролюючих і правоохоронних органів стосовно протидії легалізації (відмивання) коштів, отриманих злочинним шляхом та фінансування тероризму [70, 74, 76].

В національній економічній системі нашої країни створена та функціонує Державна служба фінансового моніторингу України [65, 73] (далі ДСФМУ), що забезпечує, організовує, координує національне і міжнародне співробітництво у сфері протидії легалізації (відмивання) коштів, одержаних злочинним шляхом та фінансування тероризму. ДСФМУ разом з іншими державними органами, що додатково залучаються до реалізації національної системи боротьби з відмиванням нелегальних доходів, на постійній основі щорічно аналізує та узагальнює існуючі типології легалізації доходів, враховуючи наявний практичний міжнародний досвід, а також досвід державних та комерційних органів та установ України.

Отже, для забезпечення належного рівня фінансової, а, відповідно, й економічної безпеки держави застосовують певні заходи впливу у сфері фінансового моніторингу, такі як: скорочення кількості фінансових злочинів і відповідних втрат від них; зниження об'єму тіньової економіки; посилення надійності банків; посилення контрою за міждержавними переказами; контроль за діяльністю конвертаційних центрів; збільшення сум сплачених податків від викритих нелегальних доходів; покращення ефективного застосування бюджетних ресурсів; скорочення корупційного рівня; зростання показника конкурентоспроможності країни; боротьба з кіберзлочинністю; контроль

операцій з цінними паперами; зосередження уваги на можливих шахрайствах у страховій сфері; посилена протидія фінансуванню тероризму, військових дій.

Застосування позитивного існуючого досвіду зміцнення економічної безпеки національної економіки, особливо через призму фінансового моніторингу, надасть можливість налагодити високоефективну, фінансово стійку, конкурентоспроможну роботу підприємств; підтримання всебічної правової захищеності бізнесу; забезпечити достатньо незалежну технічну і технологічну діяльність; створення ефективно діючих організаційної структури, підтримання висококваліфікованого менеджменту, кадрів, зростання високоінтелектуального потенціалу на підприємствах; створення надійної захищеності інформаційної бази, комерційної таємниці, забезпечення повної безпеки коштів і майна як підприємства, так і його учасників.

2 МОДЕЛЮВАННЯ АЛГОРИТМІВ ПЕРЕВІРОК ОПЕРАЦІЙ НА ПРЕДМЕТ ШАХРАЙСТВА, ЯКІ ЗДІЙСНЮЮТЬСЯ ІЗ ЗОВНІШНІХ ДЖЕРЕЛ

2.1 Динамічний підхід щодо моделювання процесу боротьби з кібератаками у сфері електронного банкінгу

Відсутність належної уваги до безпеки проведення онлайн-операцій може зробити їх уразливими для злочинців.

Сьогодні більшість фінансових операцій здійснюються через Інтернет. Розвиток електронної комерції призвів до того, що ці тенденції поширилися і на банківський сектор. З початку 80-х термін «електронний банкінг» увійшов в економічну термінологію.

З надходженням коштів через Інтернет-канали зв'язку, шахраї, які придумують все нові і нові схеми кібератак, стали активнішими. З появою нових кібератак з'являються нові протидіючі інструменти.

Вивчення цього питання хоча і є актуальним, але, на жаль, знаходиться на базовому рівні. Це пов’язано з тим, що, в першу чергу, вся інформація про кібератаки, які здійснюються в банківському секторі, є конфіденційною.

У той же час теоретично і практично виправдано, що поява нових шахрайських схем призводить до розробки нових інструментів боротьби з ними. Таким чином, існує своєрідна гонка, яка може тривати назавжди.

Таким чином, перед вченими стоїть завдання вивчити динаміку виникнення кібератак у банківському секторі та розробити інструменти протидії шахрайству в електронному банку.

Інноваційний розвиток економіки будь-якої країни залежить від спрямованості суспільства до інформаційного простору. На сьогодні головним напрямком інновацій у бізнесі є передача комерційної діяльності в Інтернет-просторі. Щороку від 30% до 70% бізнесу в будь-якій країні (незалежно від рівня

розвитку) переходить в онлайн сферу. Тобто компанії все частіше використовують системи електронної комерції для ведення бізнесу.

Початок Інтернет економіки може бути пов’язаний з проривом під час появи системи Всесвітньої павутини в середині 1990-х. Сьогодні для опису економічних відносин в Інтернеті використовується поняття «електронна комерція», яке є частиною Інтернет економіки. Таким чином, Організація економічного співробітництва та розвитку дає таке визначення цього терміна (у широкому розумінні): будь-яка форма ділових відносин, де взаємодія між суб'єктами відбувається за допомогою Інтернет-технологій [81].

Отже, електронну комерцію можна визначити як відносини, спрямовані на отримання прибутку, здійснювані дистанційно за допомогою інформаційно-телекомунікаційних систем, внаслідок чого учасники мають права та обов'язки майнового характеру [82].

Загалом електронна комерція поділяється на:

- електронний обмін даними (EDI);
- електронний переказ коштів (EFT);
- електронна торгівля;
- електронна готівка;
- електронний маркетинг;
- електронне страхування;
- і, нарешті, електронний банкінг.

Електронний банкінг – це технологія віддаленого банкінгу, яка дає можливість отримувати банківські послуги через Інтернет [83]. Для підключення клієнта до системи Інтернет-банкінгу достатньо мати доступ до глобальної мережі, встановленої на програмі браузера комп’ютера, укласти договір з банком, отримати набір паролів або спеціальних пристроїв для входу та операцій, перейти на захищену сторінку електронного банкінгу, підпишіться та підключіться до системи.

Традиційно електронний банкінг включає такі операції: здійснення банківських операцій на будь-якому комп’ютері, підключеному до Інтернету; оплата кабельного та супутникового телебачення, операторів мобільного зв’язку, телефонії; онлайн ігри; здійснення комунальних платежів; отримання виписок про рух коштів карткою чи рахунком за останні кілька днів, календарний місяць, довільний часовий період; відкриття депозиту; повернення позики; здійснення переказу коштів між власними рахунками; різні операції з кредитними картками; перегляд курсів валют, банківських оголошень; подання заявки на купівлю / продаж / конвертацію валюти; блокування картки клієнтом, наприклад, у випадку крадіжки або втрати тощо.

Згідно зі статистикою, понад 80% усіх банківських операцій може здійснювати людина, яка сидить за комп’ютером вдома або в офісі. Користь від такого виду діяльності отримують усі залучені особи: клієнти банків, банки, розробники програмного забезпечення та власники компаній, що представляють свої продукти та послуги в Інтернеті.

У той же час активізація фінансової діяльності через Інтернет призводить до того, що велика кількість особистої інформації, в тому числі фінансової, проходить каналами зв'язку. Це, у свою чергу, призводить до посилення шахрайства з електронним банкінгом.

Нині розробка різних схем шахрайства досягла глобального рівня. У зв'язку з розвитком інформаційних технологій, шахраї переходять на новий рівень, організовуючи кібератаки на автоматизовані системи різних компаній та підприємств.

Кібератаки проникли абсолютно у всі сфери бізнесу. На рисунку 2.1 показано 5 напрямків бізнесу, які понесли найбільші витрати через кібершахрайства у серпні 2018 року. З рисунка 2.1 можна побачити, що найбільш збитковими кібератаки були для фінансового сектору. У той же час, близько 90% нападів припадає на банківський сектор. Особливо активно шахрайства проводяться у сфері електронного банкінгу.

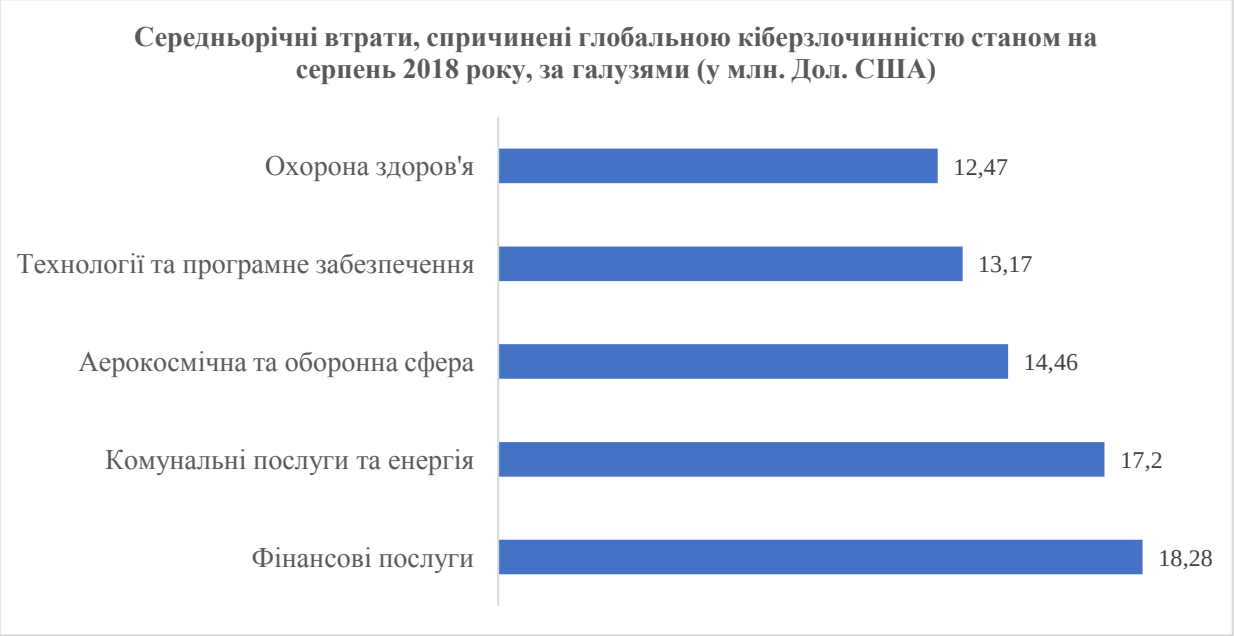

Рисунок 2.1 – Середньорічні витрати, спричинені глобальною кіберзлочинністю станом на серпень 2018 року, за галузями (у млн. дол. США) [5]

Найпоширенішим видом шахрайства в секторі електронного банкінгу є фішинг та його підвиди (рис. 2.2).

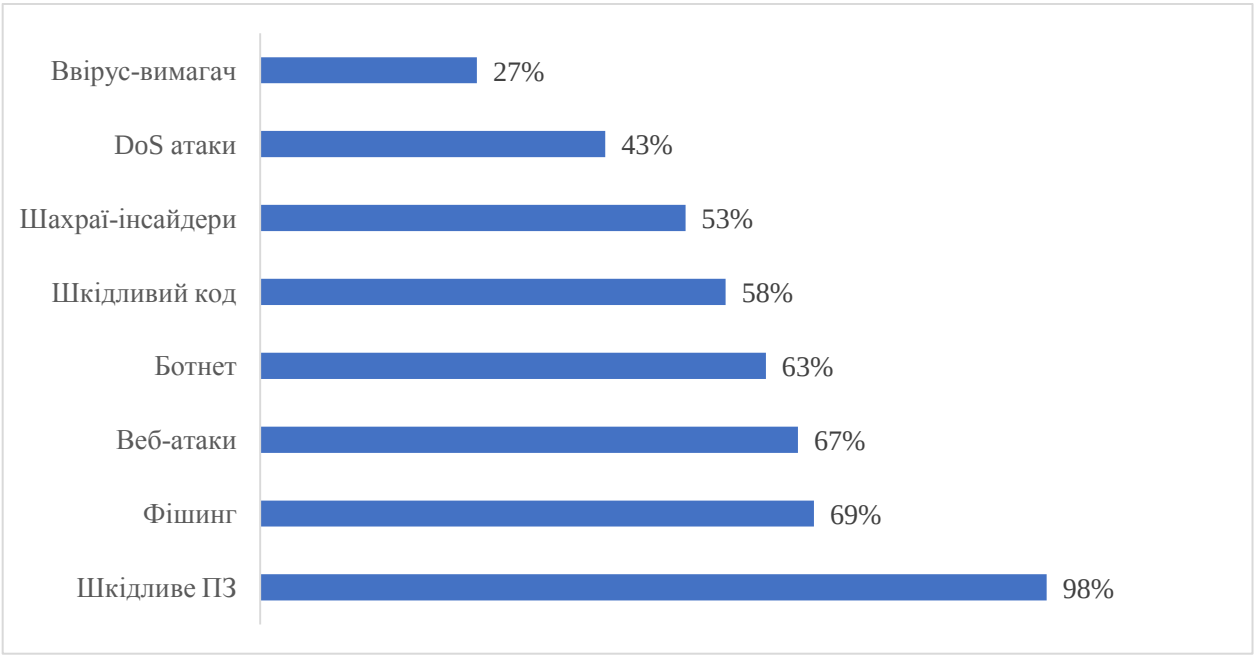

Рисунок 2.2 – Типи кібератак, які зазнавали компанії у всьому світі станом на серпень 2018 року [84]

Як правило, фішинг можна визначити як масштабований акт обману, за допомогою якого оманливість використовується для отримання інформації від цілі [85]. Точніше, фішинг – це форма соціальної інженерії, в якій зловмисник, також відомий як фішер, намагається шахрайським шляхом отримати конфіденційні дані законних користувачів шляхом автоматичної імітації електронних комунікацій або телефонних дзвінків від надійних або громадських організацій [86].

Загалом є два основних принципи фішингу:

– на мобільний телефон, іноді навіть не прив’язаний до рахунку, дзвонить працівник банку або навіть його служба безпеки. Клієнту повідомляють про сумнівні рухи на картці і просять повідомити CVV-код підтвердження платіжної картки. Ніколи не слід нічого повідомляти, якщо дзвінок не робив сам клієнт на номер служби підтримки, будь-яка інформація може бути використана для крадіжки. Краще перервати дзвінок і зателефонувати самому своєму менеджеру банку;

– лист надходить на пошту клієнта, підписаний його обслуговуючим банком. Запропоноване посилання переводить клієнта до аналогу особистого кабінету, в якому потрібно ввести свій логін та пароль. Банки ніколи не використовують такий спосіб роботи з клієнтами, будь-які листи на особисту пошту з пропозицією надати персональні дані, номер картки або ввести ім’я користувача та пароль, підписані працівником банку, завжди надсилаються шахраєм.

Повна фішинг-атака включає три ролі фішерів. По-перше, фішери-поштарі розсилають велику кількість шахрайських електронних листів (як правило, через ботнети), які направляють користувачів на шахрайські веб-сайти. По-друге, фішери-колектори встановлюють шахрайські веб-сайти (зазвичай розміщуються на компрометованих машинах), які активно спонукають користувачів до надання конфіденційної інформації. Нарешті, фішери-касири використовують конфіденційну інформацію для заволодіння коштами [87]. Потік інформації показаний на рис. 2.3.

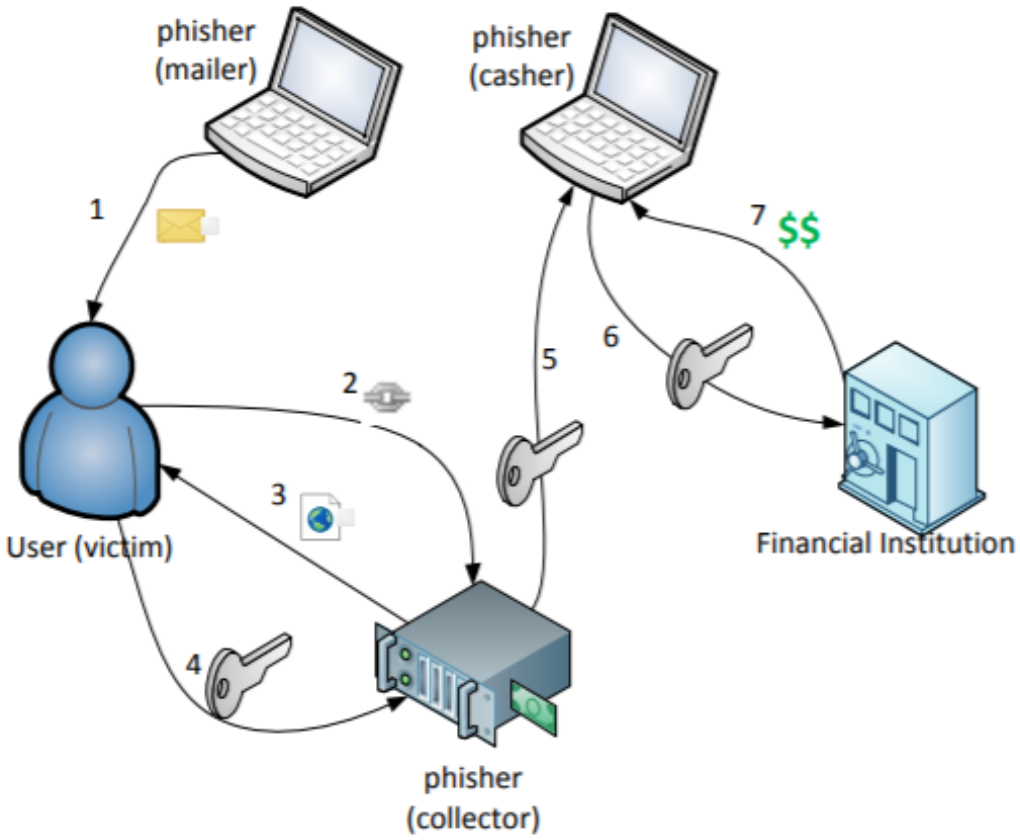

Рисунок 2.3 – Інформаційний потік при фішингу [87]

Фішинг також можна розділити на такі типи залежно від використовуваних механізмів:

– атака «людина всередині» – хакери розміщуються між банками та клієнтами, поки клієнти використовують свої банківські рахунки в Інтернеті [88];

– оманлива фішинг-атака – надсилання шахрайських повідомлень електронною поштою [89]. Під час такого типу фішинг-атаки, зловмисник надсилає електронним повідомленням користувачам, маскуючись як один із представників банку [90].

– фармінг – цей спосіб складніший і працює лише з невеликими банками, призначений для перенаправлення трафіку на підроблений Інтернет-хост. Існують різні методи нападу типу фармінг, серед яких найчастішим є модифікація налаштувань DNS [87]. Таким чином, шахрай «замінює» реальний

Інтернет-банк на той самий візуально, але підроблений, де клієнт вносить свої дані, а шахрай, відповідно, отримує всі необхідні персональні дані.

– фішинг на основі зловмисного програмного забезпечення – зловмисне програмне забезпечення – це програмне забезпечення, розроблене або з метою заподіяння шкоди обчислювальному пристрою, або для отримання користі від нього на шкоду своєму користувачеві [91]. Зловмисне програмне забезпечення може використовуватися безпосередньо для збору конфіденційної інформації або для допомоги іншим методам фішингу.

– фішинг через PDF докумнти - зловмисник або хакер може використати деякі ключові функції мови програмування PDF, щоб створити новий документ на власну користь та отримати бажану особисту інформацію від потерпілого [87].

Аналіз статистики щодо загальної кількості фішинг-атак у всьому світі показує, що їх кількість поступово збільшується (рис. 2.4).

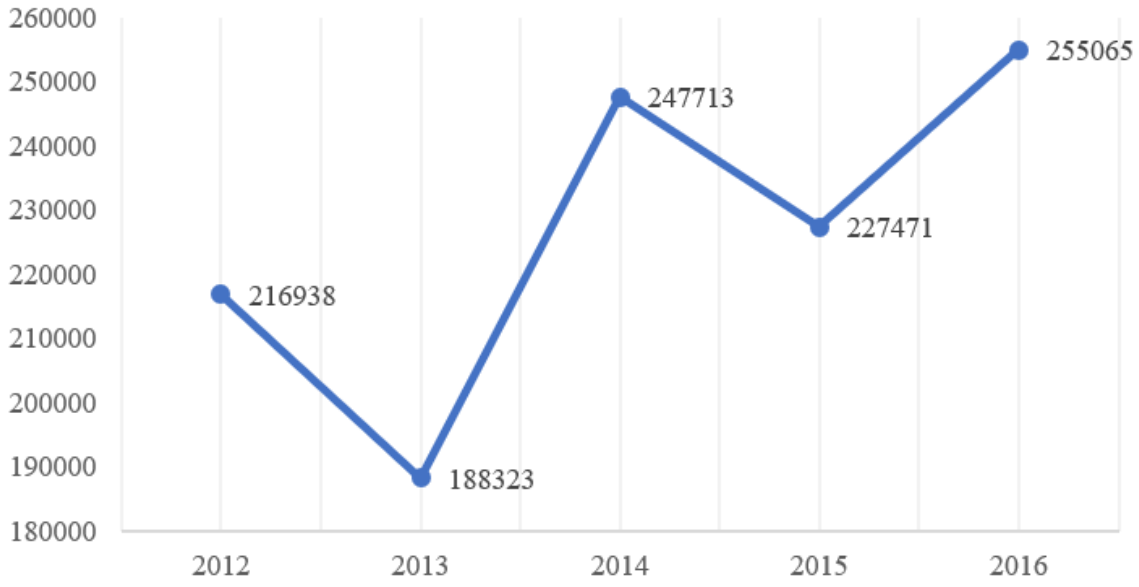

Рисунок 2.4 – Кількість глобальних фішинг-атак з 2012 по 2016 рік у всьому світі [85]

Варто зауважити, що часовий ряд має певну циклічність. Це пов’язано з тим, що створюються певні інструменти протидії існуючим шахрайським атакам. Однак, минаючи інструменти, що виникають, створюються нові типи

атак. Таким чином, зменшення кількості фішинг-атак через використання протидіючих інструментів замінюється різким збільшенням їх кількості.

Отже, фішинг виділяється як найпоширеніший вид кібератаки в електронному банкінгу. Таким чином, надалі буде запропонована математична модель протидії подібним шахрайським атакам банків.

Моделювання процесу протидії кібершахрайствам в сфері електронного банкінгу є складним питанням з точки зору збору реальних даних. Відповідна статистика закрита. Крім того, величезна кількість шахрайських схем не виходить на рівень правоохоронних органів. Тому це питання можна дослідити лише в теоретичній формі. У цьому дослідженні пропонується моделювати процес протидії шахрайству в банку за допомогою моделі економічної динаміки. Отже, використання інструментів для боротьби з кібератаками та появу нових атак можна порівняти з класичною моделлю «хижак-жертва» [88].

$$\begin{cases} x` = (a - c \cdot y)x \\ y` = -(b + d \cdot x)y \end{cases} \tag{2.1}$$

де x - кількість жертв;

y - кількість хижаків;

a,b,c,d - коефіцієнти, що відображають взаємодію між видами.

Припустимо, що для нашої предметної області x - кількість шахрайських атак, y - кількість інструментів для боротьби з шахрайськими атаками у сфері електронного банкінгу.

Використання моделі Лотки-Вольтерра з логістичним зростанням [92] і моделі Холлінга-Таннера [93] дозволяє запропонувати модель протидії банківським кібератакам:

$$\begin{cases} x` = (a - d \cdot x - b \cdot y)x \\ y` = -c \cdot y + \dfrac{1}{b} - y \end{cases} \tag{2.2}$$

де x - кількість кібератак на момент часу t;

y - кількість доступних інструментів для боротьби з шахрайськими атаками на момент часу *t;*

a - коефіцієнт природного збільшення кількості шахрайських атак;

b - коефіцієнт ефективності одного інструменту протидії шахрайським атакам;

c - коефіцієнт природного зменшення кількості інструментів протидії шахрайським атакам за одиницю часу;

d - коефіцієнт міжвидової конкуренції для шахраїв. *d*=1/*D*, де *D* - максимально можлива кількість атак.

Наступним кроком є пошук особливих точок системи.

На основі символьних розрахунків отримуємо дві особливі точки.

$$(x_1; y_1) = (0; \frac{1}{(1+c)b}) \tag{2.3}$$

$$(x_2; y_2) = (\frac{(1+c)a-1}{(1+c)d}; \frac{1}{(1+c)b}) \tag{2.4}$$

Дослідження першої особливої точки є недоцільним з практичної точки зору, оскільки передбачається, що кількість шахрайських атак дорівнює 0. Тому ми дослідимо другу особливу точку. Лінеаризуємо модель за допомогою матриці Якобі.

$$J(x,y) = \begin{pmatrix} a - b \cdot y - 2 \cdot d \cdot x & -b \cdot x \\ 0 & -c - 1 \end{pmatrix} \tag{2.5}$$

Замінюємо *x* і *y* в якобіані значенням другої особливої точки і обчислюємо слід і детермінант для отриманої матриці Якобі.

$$tr = a - c - \frac{2 \cdot a + 2 \cdot a \cdot c - 2}{c+1} - \frac{b}{b + b \cdot c} - 1 \tag{2.6}$$

$$\Delta = a + a \cdot c - 1 \tag{2.7}$$

На основі аналізу характеристичного рівняння, отримаємо наступний вираз для дискримінанта:

$$D = \left(c - a + \frac{b}{b + b \cdot c} + \frac{2 \cdot d(a + a \cdot c - 1)}{(1 + c)d} + 1\right)^2 - \\ -4 \cdot a - 4 \cdot a \cdot c + 4 \tag{2.8}$$

З огляду на економічний зміст вхідних параметрів запропонованої моделі, дискримінант не може бути негативним. Отже, корені характерного рівняння не можуть бути комплексними числами. Більше того, враховуючи, що другий корінь характерного рівняння завжди буде від'ємним числом, можна зробити висновок, що корені характерного рівняння можуть приймати такі значення:

– дійсні, від'ємні, різні - особлива точка типу стійкий вузол;

– дійсні, від'ємні, співпадаючі - особлива точка типу стійкий вироджений вузол;

– дійсні, різні, різних знаків - особлива точка типу сідло;

– перший корінь 0, другий від'ємний - особлива точка типу пряма стійких точок рівноваги.

Для досягнення цих типів особливих точок сформуємо обмеження, які повинні бути накладені на співвідношення вхідних параметрів (табл. 2.1).

Таблиця 2.1 – Типи особливої точки залежно від співвідношення вхідних параметрів моделі

Тип особливої точки	Співвідношення вхідних параметрів
Стійкий вузол	$a + a \cdot c - 1 > 0$ $\frac{\sqrt{D}}{2} \neq 0$
Стійкий вироджений вузол	$a + a \cdot c - 1 > 0$ $\frac{\sqrt{D}}{2} = 0$
Сідло	$a + a \cdot c - 1 < 0$
Пряма стійких точок рівноваги	$a + a \cdot c - 1 = 0$

Для проведення чисельних експериментів та вивчення поведінки запропонованої моделі ми побудуємо імітаційну модель процесу протидії

кібератаками в електронному банкінгу, використовуючи інструменти системної динаміки (рис. 2.5).

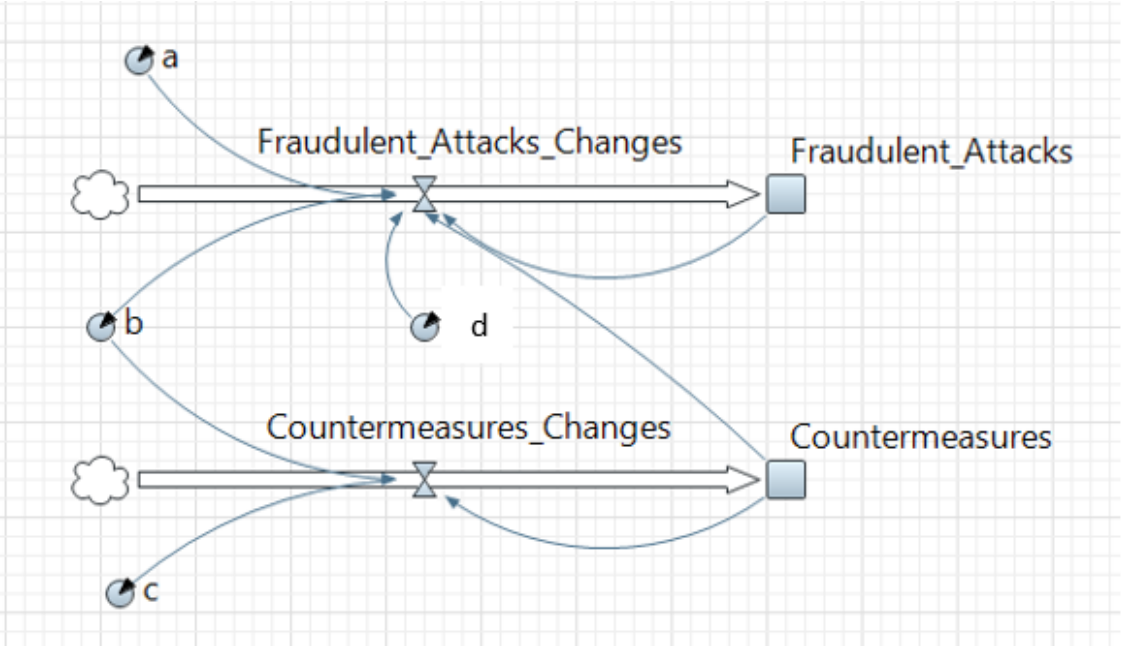

Рисунок 2.5 – Діаграма «потік-дані» для моделі процесу протидії кібершахрайствам в електронному банкінгу

Структура побудованої моделі представлена в табл. 2.2.

Таблиця 2.2 – Опис елементів діаграми

Назва елементу на діаграмі	**Тип елементу**
Fraudulent_Attacks (кібератаки)	Накопичувач
Countermeasures (інструменти протидії)	Накопичувач
Fraudulent_Attacks_Changes (зміна кількості кібератак)	Потік
Countermeasures_Changes (зміна кількості інструментів протидії)	Потік
a	Параметр
b	Параметр
c	Параметр
d	Параметр

Побудована схема дозволяє проводити імітаційні експерименти, що враховують різні співвідношення вхідних параметрів запропонованої моделі процесу протидії кібершахрайству а електронному банкінгу для отримання особливих точок зазначених типів.

Проведені імітаційні експерименти для випадку сідла показали, що кількість шахрайських атак з часом виходить на нуль, а кількість інструментів для боротьби з ними наближається до деякого стаціонарного значення.

Симуляційні експерименти для прямої стійких точок рівноваги показали випадок, подібний до сідла.

Побудова часових графіків та фазових портретів запропонованої моделі для випадку стійкого виродженого вузла спричинила необхідність вибору параметрів таким чином, щоб дискримінант характеристичного рівняння приймав нульове значення. Така ситуація можлива лише в тому випадку, коли параметр c=0. Це означає, що інструменти протидії шахрайським атакам є успішними і немає їх «вимирання». Але ця ситуація не дуже приваблива з практичної точки зору. X та y, як у випадку зі стійким вузлом, переходять в якийсь стаціонарний стан. Але значення x доволі високе. І воно буде збільшуватись зі збільшенням значення параметра a, отже тим більше нових шахрайських атак породжують атаки, які закінчились успішно.

Підсумовуючи результати комп'ютерного моделювання, можна зробити висновок, що з практичної точки зору випадок сідла та прямої стійких точок рівноваги є найбільш бажаними, оскільки в цих випадках значення x (кількість шахрайських атак) наближується до 0, незалежно від початкових значень x та y (координати початкового стану системи). Таким чином, значення параметра a має бути $a \leq \frac{1}{1+c}$. За своїм економічним змістом, параметр c може приймати значення від 0 до 1. Таким чином, параметр a має змінюватись у меах від 0.5 до 1. Це означає, що у відповідь на кожну успішний кібератаку має виникнути хоча б одна нова атака, що навряд чи може бути в реальному житті. Як правило, їх виникає набагато більше.

Відповідно, на практиці найбільш ймовірними випадками є стійкий вузол і стійкий вироджений вузол, так як вони направлені на зменшення значення *x*. Таким чином, нам слід прагнути зменшити значення $x = \frac{(1+c)a-1}{(1+c)d}$. З цього виразу ми бачимо, що найбільш впливовими є параметри *a* та *d*. Більш того, для *a* зв'язок є прямим, а для *d* - зворотнім.

Підсумовуючи, можна стверджувати, що для отримання більш сприятливої ситуації з практичної точки зору необхідно зменшити значення параметрів *a* і *c* та збільшити параметр *d*.

Таким чином, дана модель дозволяє провести теоретичне дослідження питання моделювання процесу боротьби з кібератаками у сфері електронного банкінгу. Побудова імітаційної моделі, також, дозволяє проводити і числові експерименти на умовно встановлених значень. Проте, дана модель може бути використана банківськими установами на реальній статистиці, яка збирається для внутрішньої звітності банку та є закритою для зовнішніх користувачів.

2.2 Нечітко-множинна модель оцінки рівня ризику шахрайства банківського персоналу

Банківські втрати через шахрайства становлять приблизно 70 млрд. доларів шорічно, 70 % яких реалізуються за участі банківського персоналу [96], що свідчить про глобальний характер шахрайств банківського персоналу. Основна відповідальність за встановлення та моніторинг усіх аспектів ризиків шахрайства в банку і за діяльність щодо запобігання шахрайству лежить на керівниках банку. Небезпечність шахрайства персоналу у банківській діяльності обумовлює необхідність активної протидії їм, одним із інструментів якої є незалежний аудит, який в тому числі оцінює рівень ризику шахрайства банківського персоналу.

В роботі [97] виділено два види шахрайства персоналу, ризик виникнення яких оцінюється окремо: викривлення фінансової звітності та незаконне заволодіння активами. Для кожного виду шахрайства виділено пов'язані з ним

умови: спонукання до шахрайства, сприятливі можливості для шахрайства, схильність співробітника до шахрайства. Кожна комбінація виду шахрайства та умови його виникнення пов’язана зі специфічними факторами ризику шахрайства, які, в свою чергу, характеризуються певними індикаторами ризику шахрайства. Ключовою відмінністю між фактором ризику шахрайства та індикатором ризику шахрайства є той факт, що індикатор ризику шахрайства спостерігається аудитором безпосередньо, в той час як фактор ризику шахрайства спостерігається аудитором лише опосередковано через присутність пов’язаних з ним індикаторів ризику шахрайства. Аудитор використовує індикатори ризику шахрайства та власні міркування для прийняття рішення щодо існування специфічного фактору ризику шахрайства персоналу.

Незважаючи на існування значної кількості наукових публікацій з досліджуваної проблематики, питання оцінювання рівня ризику шахрайства банківського персоналу з урахуванням нечітких оцінок індикаторів ризику шахрайства, наразі висвітлені недостатньо. На основі опрацювання [98] в роботі [97] запропоновано інноваційний підхід до оцінки ризику шахрайства персоналу, зокрема, вводиться бінарне та нечітке оцінювання аудиторами індикаторів ризику шахрайства персоналу, а також пропонується система оцінювання ризику шахрайства персоналу, побудована на засадах теорії нечіткої логіки. В той же час запропонована в роботі [97] система нечіткого логічного висновку вимагає побудови та відповідного обґрунтування експертної бази нечітких правил. Ми вважаємо, що більш раціональною є побудова узагальнюючої оцінки ризику шахрайства персоналу на основі агрегування нечітких оцінок індикаторів ризику шахрайства з використанням ієрархічного дерева. Агрегований опис містить порівняно з початковим менше інформації, при цьому корисна інформація залишається, а надмірна звужується [99, с. 223].

Модель оцінювання рівня ризику шахрайства банківського персоналу пропонується представити у вигляді представленого на рис. 2.6 деревоподібного графа з двома рівнями ієрархії, побудованого на основі опрацювання [100].

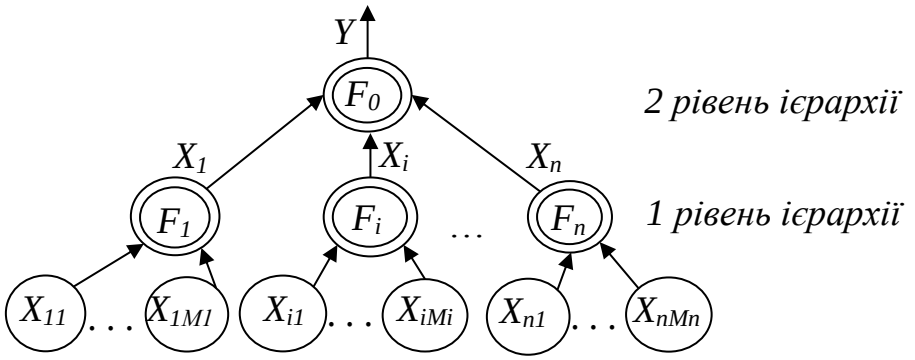

Рисунок 2.6 – Ієрархічна структура моделі оцінювання рівня ризику шахрайства банківського персоналу

На першому рівні ієрархії фактори ризику шахрайства банківського персоналу характеризуються наборами своїх складових – індикаторів ризику шахрайства банківського персоналу (вхідними змінними X_{ij}), що групуються за відповідними факторами ризику X_i, рівні яких визначаються в результаті агрегування вхідних змінних X_{ij}. На другому рівні ієрархії рівень ризику шахрайства банківського персоналу в цілому Y визначається в результаті агрегування отриманих на попередньому етапі оцінювання рівнів факторів ризику X_i.

Елементи деревоподібного графа (рис. 2.6) інтерпретуються таким чином:

– кінцеві вершини X_{ij} – оцінки індикаторів ризику, пов'язаних з i-тим фактором ризику, $i=\overline{1,n}; j=\overline{1,M_i}$, де n – кількість факторів ризику, M_i – кількість індикаторів ризику, що пов'язані з i-тим фактором ризику через некінцеву вершину F_i;

– некінцеві вершини F_i - функції згорток за факторами ризику X_i, $i=\overline{1,n}$;

– дуги, що виходять із нетермінальних вершин (X_i), – рівні відповідних факторів ризику шахрайства банківського персоналу.

– некінцева вершина F_0 – функція згортки факторів ризику X_i, $i=\overline{1,n}$.

– дуга *Y*, що виходить з кореня дерева, – рівень ризику шахрайства банківського персоналу в цілому.

Кількісне оцінювання індикаторів ризику шахрайства X_{ij} передбачає використання анкет, у яких аудитор зазначає рівень присутності відповідного індикатора ризику в діапазоні від 0 до 1. Якщо аудитор використовує іншу кількісну шкалу, то можна виконати перехід від цієї шкали до 01-носія на основі простого лінійного перетворення. Ми пропонуємо виконати агрегування анкетних оцінок індикаторів ризику шахрайства персоналу за рівнями ієрархії графа, представленого на рис. 2.6, із пересуванням від нижніх рівнів ієрархії до верхніх. Рівень ризику шахрайства банківського персоналу в цілому опишемо наступною нечіткою ієрархічною моделлю:

$$Y=<G, L, S, F>, \qquad (2.9)$$

де *G* – ієрархічний граф, показаний на рис. 1;

L – терм-множина можливих значень лінгвістичних змінних;

S – система відношень пріоритетів індикаторів ризику та факторів ризику;

F – функція згортки нечітких оцінок у відповідних вершинах графа *G*. Ваги дуг графа відповідають ступеню впливу відповідних індикаторів ризику та факторів ризику на результуючу оцінку.

Оцінки рівнів індикаторів ризику X_{ij}, оцінки рівнів факторів ризику X_i, а також оцінку рівня ризику шахрайства банківського персоналу в цілому *Y* представимо у вигляді лінгвістичних змінних L_{ij}, L_i та L_Y відповідно. З метою спрощення моделі сформуємо одну терм-множину можливих значень для всіх лінгвістичних змінних L_{ij}, L_i та L_Y з п'яти якісних термів T_{ij}^k, T_i^k, T_Y^k, відповідно: "дуже низький" (*k=1*), "низький" (*k=2*), "середній" (*k=3*), "високий" (*k=4*), "дуже високий" (*k=5*). Кожному нечіткому терму T_{ij}^k лінгвістичної змінної L_{ij}

поставимо у відповідність трапецієподібну функцію належності $\mu_k\left(X_{ij}\right)$ з параметрами $\underline{t_{ij}^k};\overline{t_{ij}^k};a_{ij}^k;b_{ij}^k$ $(k=\overline{1,5})$, наведену на рис. 2.7.

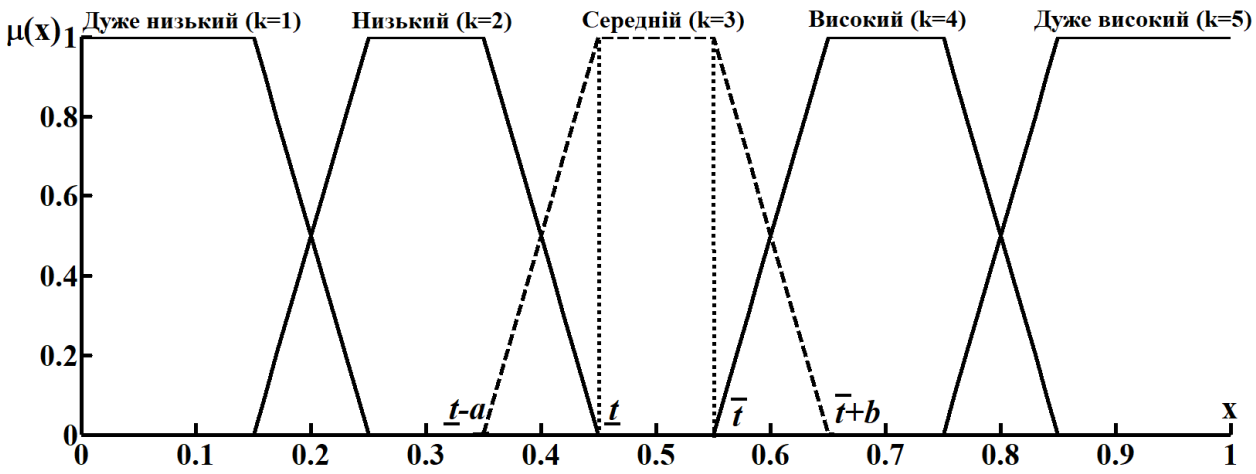

Рисунок 2.7 – Нечітка терм-множина

$$\mu_k\left(X_{ij}\right)=\begin{cases} 0, \text{ якщо } X_{ij}\le \underline{t_{ij}^k}-a_{ij}^k \text{ або } X_{ij}\ge \overline{t_{ij}^k}+b_{ij}^k \\ \dfrac{X_{ij}-\left(\underline{t_{ij}^k}-a_{ij}^k\right)}{a_{ij}^k}, \quad \text{якщо} \quad \underline{t_{ij}^k}-a_{ij}^k<X_{ij}<\underline{t_{ij}^k} \\ 1, \quad \text{якщо} \quad \underline{t_{ij}^k}\le X_{ij}\le \overline{t_{ij}^k} \\ \dfrac{\left(\overline{t_{ij}^k}+b_{ij}^k\right)-X_{ij}}{b_{ij}^k}, \text{ якщо} \quad \overline{t_{ij}^k}<X_{ij}<\overline{t_{ij}^k}+b_{ij}^k \end{cases} \tag{2.10}$$

Аналогічно поступимо і з нечіткими термами T_i^k, T_Y^k $(k=\overline{1,5})$ лінгвістичних змінних L_i і L_Y.

В якості множини функцій належності (2.10) пропонується обрати стандартний нечіткий п’ятирівневий 01-класифікатор з трапецієвидними функціями належності [100]:

$$\mu_1(X_{ij})=\begin{cases}0, \quad якщо \quad X_{ij}\geq 0,25\\ 10\cdot(0,25-X_{ij}), \quad якщо \quad 0,15<X_{ij}<0,25\\ 1, якщо\ 0\leq X_{ij}\leq 0,15\end{cases} \tag{2.11}$$

$$\mu_2(X_{ij})=\begin{cases}0, якщо\ X_{ij}\leq 0,15\ або\ X_{ij}\geq 0,45\\ 10\cdot(X_{ij}-0,15), \quad якщо \quad 0,15<X_{ij}<0,25\\ 1, \quad якщо \quad 0,25\leq X_{ij}\leq 0,35\\ 10\cdot(0,45-X_{ij}), \quad якщо \quad 0,35<X_{ij}<0,45\end{cases} \tag{2.12}$$

$$\mu_3(X_{ij})=\begin{cases}0, якщо\ X_{ij}\leq 0,35\ або\ X_{ij}\geq 0,65\\ 10\cdot(X_{ij}-0,35), \quad якщо \quad 0,35<X_{ij}<0,45\\ 1, \quad якщо \quad 0,45\leq X_{ij}\leq 0,55\\ 10\cdot(0,65-X_{ij}), \quad якщо \quad 0,45<X_{ij}<0,65\end{cases} \tag{2.13}$$

$$\mu_4(X_{ij})=\begin{cases}0, якщо\ X_{ij}\leq 0,55\ або\ X_{ij}\geq 0,85\\ 10\cdot(X_{ij}-0,55), \quad якщо \quad 0,55<X_{ij}<0,65\\ 1, \quad якщо \quad 0,65\leq X_{ij}\leq 0,75\\ 10\cdot(0,85-X_{ij}), \quad якщо \quad 0,75<X_{ij}<0,85\end{cases} \tag{2.14}$$

$$\mu_5(X_{ij})=\begin{cases}0, \quad якщо \quad X_{ij}\leq 0,75\\ 10\cdot(0,85-X_{ij}), \quad якщо \quad 0,75<X_{ij}<0,85\\ 1, якщо\ 0,85\leq X_{ij}\leq 1\end{cases} \tag{2.15}$$

Стандартний нечіткий п’ятирівневий 01-класифікатор робить проекцію лінгвістичного опису на 01-носій (відрізок [0,1] дійсної вісі), розташовуючи симетрично вузли класифікації (0.1, 0.3, 0.5, 0.7, 0.9), в яких значення відповідної функції належності дорівнює одиниці, а всіх інших – нулю (рис. 2.7). Невпевненість аудитора в класифікації лінійно убуває (зростає) при видаленні

від вузла (з наближенням до вузла, відповідно). Сума значень функцій належності нечітких термів в усіх точках 01-носія дорівнює одиниці [100].

Агрегування нечітких оцінок лінгвістичних змінних здійснюється за рівнями ієрархії з пересуванням від нижніх рівнів графа *G* (рис. 2.6) до верхніх. Попередньо аудитор кількісно оцінює рівні вхідних змінних X_{ij} (від 0 до 1) для кінцевих вершин графа.

Для агрегування нечітких оцінок використаємо матричну схему, наведену в [100, с. 79]. Якщо по рядках матриці відкладені лінгвістичні змінні L_{ij} індикаторів ризику, а по стовпцях – їх нечіткі терми T_{ij}^{k} $(k=\overline{1,5})$, виражені відповідним набором функцій належності $\mu_k\left(X_{ij}\right)$, то кількісна оцінка фактору ризику X_i в діапазоні від 0 до 1 розраховується за формулою подвійного згортання:

$$X_i=\sum_{j=1}^{M_i}\omega_{ij}\sum_{k=1}^{5}\left(\alpha_k\cdot\mu_k(X_{ij})\right) \tag{2.16}$$

$$\sum_{k=1}^{5}\mu_k(X_{ij})=1 \tag{2.17}$$

$$\sum_{j=1}^{M_i}\omega_{ij}=1 \tag{2.18}$$

де ω_{ij} – вага індикатора ризику X_{ij} в оцінюванні фактора ризику X_i;

M_i – кількість індикаторів ризику, що пов'язані з фактором ризику X_i;

$\alpha_k=0{,}2\cdot k-0{,}1$ – ваги нечітких термів (так звані вузлові точки стандартного нечіткого п'ятирівневого класифікатора: 0,1; 0,3; 0,5; 0,7; 0;9).

Вагові коефіцієнти ω_{ij} можуть бути отримані на основі побудови системи ваг Фішберна [100, с. 37] або матриці парних порівнянь [101]. Можна також

оцінити вагу відповідних індикаторів ризику X_{ij} з використанням певної бальної шкали, а потім нормалізувати одержані результати.

Розраховане за формулами (2.11)-(2.18) значення фактору ризику X_i знаходиться в діапазоні від 0 до 1, тому його можна лінгвістично розпізнати за формулами (2.11)-(2.15). Пройшовши послідовно знизу вгору по всіх рівнях ієрархії G і застосовуючи формули (2.11)-(2.18) ми одержуємо лінгвістичну інтерпретацію оцінки рівня ризику шахрайства банківського персоналу в цілому.

Розглянемо приклад оцінювання ризику шахрайства персоналу щодо викривлення фінансової звітності, використовуючи дані, наведені в роботі [97]. Всі фактори ризику шахрайства персоналу класифіковані за такими категоріями:

1. Спонукання до викривлення фінансової звітності.

2. Сприятливі можливості для викривлення фінансової звітності.

3. Обґрунтування викривлення фінансової звітності.

Значущість всіх категорій і факторів ризику вважаємо однаковою. Нормалізовані ваги індикаторів факторів ризику та оцінки аудитором рівнів присутності відповідних індикаторів у об’єкта аудиту наведені в табл. 2.3-2.5.

Таблиця 2.3 – Спонукання до викривлення фінансової звітності

	Індикатор фактору ризику	**Нормалізована вага індикатора**	**Рівень присутності індикатора ризику**
Фактор 1.1. Прибутковість знаходиться під загрозою економічних умов діяльності			
1.1.1	Високий ступінь конкуренції або насичення ринку супроводжується зниженням прибутковості	0,128	0,9
1.1.2	Висока чутливість до швидких змін, таких як зміни в технології або зміни процентних ставок	0,128	0,3
1.1.3	Значне зниження споживчого попиту та зростання банкрутств як у галузі, так і в економіці в цілому	0,128	0,1
1.1.4	Операційні збитки, які становлять загрозу банкрутства або недружнього поглинання	0,179	
1.1.5	Повторювані негативні грошові потоки від операцій або неможливість генерувати грошові потоки від	0,205	

Продовження таблиці 2.3

	Індикатор фактору ризику	Нормалізована вага індикатора	Рівень присутності індикатора ризику
	операцій при одночасному звітуванні про прибутки та зростання доходів		
1.1.6	Швидке зростання або незвичайна прибутковість, особливо в порівнянні з іншими установами тієї ж галузі	0,179	0,3
1.1.7	Нові бухгалтерські або нормативні вимоги.	0,052	
Фактор 1.2. Надмірний тиск на керівництво з метою виконання очікувань третіх сторін			
1.2.1	Очікування інвестиційних аналітиків, інституційних інвесторів, великих кредиторів або інших зовнішніх сторін, що стосуються прибутковості, включаючи очікування, створені керівництвом у занадто оптимістичних прес-релізах і щорічних звітах	0,267	0,8
1.2.2	Необхідність отримання додаткового фінансування для забезпечення конкурентоспроможності	0,233	0,2
1.2.3	Гранична здатність погашати борги	0,25	
1.2.4	Негативні наслідки звітування про погані фінансові результати важливих зупинених операцій, таких як злиття або заключення контрактів	0,25	0,2
Фактор 1.3. Отримана інформація свідчить про те, що особистий фінансовий стан керівництва залежить від фінансового стану об'єкта аудиту			
1.3.1	Значні фінансові інтереси в об'єкті аудиту	0,313	0,9
1.3.2	Значна винагорода (наприклад, бонуси, акції), що залежить від досягнення агресивних цілей щодо ціни акцій, операційних результатів, фінансового становища або грошового потоку	0,374	0,9
1.3.3	Особисті гарантії по заборгованості об'єкта аудиту	0,313	
Фактор 1.4. Надмірний тиск на персонал з метою досягнення фінансових цілей, встановлених керівництвом, включаючи цілі стимулювання збуту			
1.4.1	Присутній надмірний тиск на персонал з метою досягнення фінансових цілей, встановлених керівництвом, включаючи цілі стимулювання збуту	1	0,8

Таблиця 2.4 – Сприятливі можливості для викривлення фінансової звітності

	Індикатор фактору ризику	Нормалізована вага індикатора	Рівень присутності індикатора ризику
Фактор 2.1. Характер діяльності об'єкта аудиту надає можливості для викривлення фінансової звітності			
2.1.1	Важливі операції з пов'язаними сторонами здійснюються не за правилами звичайного бізнесу або операції з пов'язаними суб'єктами господарювання не перевірені або перевірені іншою організацією	0,188	
2.1.2	Сильна фінансова присутність або здатність домінувати в певному секторі економіки, яка дозволяє об'єкту аудиту диктувати умови клієнтам, що може призвести до шахрайських операцій	0,141	
2.1.3	Активи, зобов'язання, доходи або витрати базуються на оцінках, що включають суб'єктивні судження або невизначеності, які важко підтвердити	0,165	
2.1.4	Важливі, незвичайні або надзвичайно складні операції, особливо ті, що здійснюються в кінці періоду, які створюють питання "пріоритету змісту над формою"	0,188	
2.1.5	Важливі операції, проведені через міжнародні кордони в юрисдикціях, де існують різні бізнес-середовища та культури	0,141	
2.1.6	Значні банківські рахунки або допоміжні операції в юрисдикціях офшорів, для яких немає чіткого ділового обґрунтування	0,176	
Фактор 2.2. Неефективний моніторинг з боку керівництва			
2.2.1	Домінування в управлінні однієї особи без компенсаційних елементів управління	0,548	0,6
2.2.2	Неефективний нагляд з боку правління або комітету з питань аудиту за процесом фінансової звітності та внутрішнього контролю	0,452	
Фактор 2.3. Складна організаційна структура			
2.3.1	Труднощі у визначенні організації або окремих осіб, які мають контрольний пакет акцій в об'єкті аудиту	0,304	
2.3.2	Надмірна організаційна структура, що включає незвичайні юридичні особи або управлінські гілки	0,348	
2.3.3	Висока плинність вищого керівництва та юрисконсультів	0,348	

Продовження таблиці 2.4

	Індикатор фактору ризику	Нормалізована вага індикатора	Рівень присутності індикатора ризику
Фактор 2.4. Недостатні компоненти внутрішнього контролю			
2.4.1	Неадекватний моніторинг, включаючи автоматизований контроль та контроль за проміжною фінансовою звітністю (там, де потрібна зовнішня звітність)	0,333	0,8
2.4.2	Високий коефіцієнт плинності кадрів або використання неефективного обліку, внутрішнього аудиту або IT-персоналу	0,333	
2.4.3	Неефективний облік і інформаційні системи, включаючи ситуації, які стосуються умов, що підлягають звітуванню	0,333	

Таблиця 2.5 – Обґрунтування викривлення фінансової звітності

	Індикатор фактору ризику	Нормалізована вага індикатора	Рівень присутності індикатора ризику
Фактор 3.1. Наявність у керівництва або співробітників поглядів, що дозволяють їм брати участь або обґрунтовувати викривлення фінансової звітності			
3.1.1	Неефективне впровадження, підтримка або дотримання цінностей або етичних норм об’єкта аудиту керівництвом	0,058	0,8
3.1.2	Надмірна участь нефінансового менеджменту у виборі принципів бухгалтерського обліку або визначенні важливих оцінок	0,079	
3.1.3	Відома історія порушень законів і нормативних актів або претензій до об’єкту аудиту, його вищого керівництва, які стверджують про шахрайство або порушення законів і правил	0,092	
3.1.4	Надмірна зацікавленість керівництва в збільшенні цін акцій або доходів суб’єкта аудиту	0,089	0,8
3.1.5	Практика керівництва щодо надавання аналітикам, кредиторам та іншим третім сторонам агресивних або нереальних прогнозів	0,089	0,8
3.1.6	Неспроможність керівництва своєчасно виправити ситуацію, що підлягає звітуванню	0,079	
3.1.7	Інтерес керівництва до використання невідповідних засобів для мінімізації податків	0,089	
3.1.8	Повторні спроби керівництва виправдати невідповідний облік на об’єкті аудиту	0,079	

Продовження таблиці 2.5

	Індикатор фактору ризику	**Нормалізована вага індикатора**	**Рівень присутності індикатора ризику**
3.1.9	Часті суперечки з поточним або попереднім аудитором з питань бухгалтерського обліку, аудиту або звітності	0,074	
3.1.10	Невиправдані вимоги до аудитора, такі як необгрунтовані часові обмеження щодо завершення аудиту або видачі аудиторського звіту	0,088	
3.1.11	Формальні або неформальні обмеження аудитора, які неналежним чином обмежують його доступ до людей або інформації або здатність аудитора ефективно спілкуватися з керівництвом або комітетом з аудиту	0,092	
3.1.12	Домінуюча поведінка керівництва в роботі з аудитором, особливо в тому, що стосується спроб вплинути на масштаб роботи аудитора або на вибір персоналу, призначеного для аудиту	0,092	

Розрахунок кількісних оцінок факторів ризику шахрайства персоналу здійснено за формулами (2.12)-(2.18) з використанням інформації, наведеної в таблицях 2.3-2.5. Інтерпретація рівнів кількісних оцінок факторів ризику шахрайства персоналу здійснена за формулами (2.12)-(2.16). Результати наведені в табл. 2.6.

Таблиця 2.6 – Розпізнавання рівнів факторів ризику шахрайства персоналу

i	Фактор ризику шахрайства персоналу	Кількісна оцінка	Функції належності для рівнів *i*-го фактору ризику шахрайства персоналу				
			Дуже низький $\mu_1(X_i)$	Низький $\mu_2(X_i)$	Середній $\mu_3(X_i)$	Високий $\mu_4(X_i)$	Дуже високий $\mu_5(X_i)$
1	Фактор 1.1	0,22	0,3	0,7			
2	Фактор 1.2	0,31		1			
3	Фактор 1.3	0,618			0,32	0,68	
4	Фактор 1.4	0,8				0,5	0,5
5	Фактор 2.2	0,329		1			
6	Фактор 2.4	0,266		1			
7	Фактор 3.1	0,189	0,61	0,39			

Розрахунок кількісної оцінки ризику шахрайства персоналу по категоріях здійснено за формулами (2.11)-(2.18) з використанням інформації, наведеної в таблиці 2.6. Інтерпретація рівнів кількісної оцінки ризику шахрайства персоналу по категоріях здійснена за формулами (2.11)-(2.15). Результати наведені в табл. 2.7.

Таблиця 2.7 – Розпізнавання рівнів ризику шахрайства персоналу по категоріях

Категорія ризику шахрайства	Кількісна оцінка	Функції належності для рівнів категорій ризику шахрайства				
		Дуже низький $\mu_1(X_i)$	Низький $\mu_2(X_i)$	Середній $\mu_3(X_i)$	Високий $\mu_4(X_i)$	Дуже високий $\mu_5(X_i)$
Категорія 1	0,5			1		
Категорія 2	0,3		1			
Категорія 3	0,178	0,72	0,28			

Розрахунок кількісної оцінки ризику шахрайства персоналу в цілому здійснено за формулами (2.11)-(2.18) з використанням інформації, наведеної в таблиці 2.6. Інтерпретація рівнів кількісної оцінки ризику шахрайства персоналу в цілому здійснена за формулами (2.11)-(2.15). Результати наведені в табл. 2.8.

Таблиця 2.8 – Розпізнавання рівня ризику шахрайства персоналу в цілому

Кількісна оцінка	Функції належності для рівнів ризику шахрайства персоналу в цілому				
	Дуже низький $\mu_1(X_i)$	Низький $\mu_2(X_i)$	Середній $\mu_3(X_i)$	Високий $\mu_4(X_i)$	Дуже високий $\mu_5(X_i)$
0,4		0,5	0,5		

Згідно з наведеними в таблицях 2.6-2.8 результатами рівень ризику шахрайства персоналу в цілому – проміжний між лінгвістичними оцінками «Середній» і «Низький», але об’єкт аудиту характеризується високим рівнем фактору ризику 1.3 (особистий фінансовий стан керівництва залежить від фінансового стану об’єкта аудиту) та високим рівнем фактору ризику 1.4

(надмірний тиск на персонал з метою досягнення фінансових цілей, встановлених керівництвом, включаючи цілі стимулювання збуту). Це означає, що існує високий рівень ризику викривлення фінансової звітності через спонукання до викривлення фінансової звітності, бо саме до цієї категорії належать фактори ризику 1.3 і 1.4. Тому аудитор повинен ретельно дослідити саме цю сферу.

Оцінювання ризику шахрайства персоналу є складовою частиною аудиторської діяльності та представляє собою дуже складний і трудомісткий процес. Розроблена нечітко-множинна модель надає аудитору можливість оцінити ризик шахрайства банківського персоналу та визначити основні сфери, що найбільше сприяють шахрайству. Це дозволяє підвищити загальну ефективність аудиту та сприяє попередженню шахрайств.

2.3 Оцінювання ризику використання фінансових посередників з метою легалізації кримінальних доходів на основі інтелектуального аналізу даних

Для дослідження ризику використання фінансових посередників з метою легалізації кримінальних доходів було обрано найбільш релевантні показники його характеристики та сформовано певну послідовність його розрахунку. Отже, розглянемо більш детально кроки запропонованого науково-методичного підходу.

1 етап. Формування статистичної бази дослідження. Для проведення дослідження було сформовано набір даних по 215 країнам світу за 2017 рік. Дані показники представляє собою статистичну інформацію, яку було отримано з офіційних сайтів світових організацій. Так, авторами було обрано 1 індикатор регресанд - рівень ризику використання фінансових посередників з метою легалізації кримінальних доходів з результатів попередньо проведених досліджень [104] та 7 індикаторів регресорів: з офіційного сайту Світового банку – валовий внутрішній продукт на душу населення (ВВП); позови до

центрального уряду; внутрішньо переміщені особи, нові переміщення, пов'язані з конфліктом та насильством (кількість випадків) [105]; по даним Організації економічного співробітництва та розвитку - банківська таємниця [106]; з сайту організації Transparency International – індекс сприйняття корупції [107]; з матеріалів досліджень Інституту економіки та миру – глобальний індекс тероризму [108]; з розрахунків Happy Planet Index – світовий індекс щастя [109].

Обґрунтування доцільності включення зазначеного набору індикаторів обумовлене результатами дослідження колінеарності шляхом застосування сигма-обмеженої параметризації (рисунок 2.8) та кореляційного аналізу залежності як регресанда від кожного із індикаторів регресорів, так і факторів між собою (рисунок 2.9). З метою проведення такого методу інтелектуального аналізу даних як виявлення ключових факторів запропоновано застосовувати програму Statistica, пакет Аналіз, вкладка Поглиблені методи, вкладка Загальні лінійні моделі GLM.

	Статистики колінеарності для членів в рівнянні Сигма-обмежена параметризація							
Ефект	Допуск	Дисперс. Infl fac	R квадр.	Risk of money laundering Бета	Risk of money laundering Частк.	Risk of money laundering Напівчас.	Risk of money laundering t	Risk of money laundering p
GDP per capita (current LCU)	0,9156	1,0921	0,0844	-0,0329	-0,0441	-0,0315	-0,4322	0,6665
Bank Secrece	0,5000	1,9999	0,5000	0,0992	0,0977	0,0702	0,9621	0,3384
Claims on central government, et	0,8784	1,1384	0,1216	-0,1513	-0,1946	-0,1418	-1,9443	0,0548
Internally displaced persons, new	0,7193	1,3903	0,2807	-0,2218	-0,2546	-0,1881	-2,5795	0,0114
Corruption Perceptions Index	0,3991	2,5058	0,6009	-0,5877	-0,4611	-0,3713	-5,0918	0,0000
Global Terrorism Index	0,7220	1,3850	0,2780	0,0870	0,1030	0,0740	1,0142	0,3130
Happy Planet Index	0,4504	2,2203	0,5496	-0,1861	-0,1722	-0,1249	-1,7129	0,0900

Рисунок 2.8 – Статистика колінеарності індикаторів статистичної бази дослідження

Аналіз рисунку 1 (коефіцієнтів бета - графа Risk of money laundering) свідчить про доцільність ранжування предикторів за ступенем їх впливу на відгук наступним чином: 1) індекс сприйняття корупції; 2) внутрішньо переміщені особи, нові переміщення, пов'язані з конфліктом та насильством (кількість випадків); 3) світовий індекс щастя; 4) позови до центрального уряду;

5) банківська таємниця; 6) глобальний індекс тероризму; 7) валовий внутрішній продукт на душу населення, причому лише два перших здійснюють сильний вплив, в той час як інші - помірний.

	Кореляції векторів в матриці плану X Кореляц. матриця для векторів в матриці плану X							
Ефект	GDP pe capita (current LCU)	Bank Secrece	Claims on central governmen etc. (% GDP)	Internally displaced persons, new displacement associate with conflict and violenc (number of cases)	Corrupti on Percepti ons Index	Global Terroris m Index	Happy Planet Index	Risk of money launderi ng
GDP per capita (current LCU)	1,000(	0,1107	-0,117(	0,032(	-0,090(	0,086(	-0,014(	0,052(
Bank Secrece	0,1107	1,000(	0,291(	-0,255(	0,611(	-0,100(	0,583(	-0,368(
Claims on central government, etc	-0,117(	0,291(	1,000(	-0,113(	0,134(	-0,008(	0,177(	-0,206(
Internally displaced persons, new	0,032(	-0,255(	-0,113(	1,000(	-0,242(	0,484(	-0,215(	-0,006(
Corruption Perceptions Index	-0,090(	0,611(	0,134(	-0,242(	1,000(	-0,259(	0,716(	-0,646(
Global Terrorism Index	0,086(	-0,100(	-0,008(	0,484(	-0,259(	1,000(	-0,200(	0,158(
Happy Planet Index	-0,014(	0,583(	0,177(	-0,215(	0,716(	-0,200(	1,000(	-0,545(
Risk of money laundering	0,052(	-0,368(	-0,206(	-0,006(	-0,646(	0,158(	-0,545(	1,000(

Рисунок 2.9 – Матриця кореляції індикаторів статистичної бази дослідження

Крім того, часткові коефіцієнти кореляції (графа Risk of money laundering рисунку 1) демонструють ступінь впливу одного предиктора на відгук за умови припущення, що інші предиктори закріплені на постійному рівні. Розрахункові значення даного показника підтверджують описаний вище висновок про значний ступніть впливу на ризик використання фінансових посередників з метою легалізації кримінальних доходів, лише індексу сприйняття корупції та показнику - внутрішньо переміщені особи, нові переміщення, пов'язані з конфліктом та насильством (кількість випадків), а також помірному впливу усіх інших.

Переходячи до аналізу коефіцієнта детермінації (графа R квадрат рисунку 1), тобто квадрата коефіцієнта множинної кореляції між даною змінною та всіма іншими, зазначимо помірність усіх показників, але зв’язок між трьома предикторами (банківська таємниця, індекс сприйняття корупції, світовий індекс щастя) та всіма іншими значно більший, ніж для чотирьох незазначених предикторів.

В той же час, дослідження кореляційної матриці (рисунок 2.8) дозволяє стверджувати про наявність оберненого зв’язку середнього ступеня між рівнем досліджуваного ризику та індексом сприйняття корупції і світовим індексом щастя, про що свідчать відповідні коефіцієнти кореляції -0,6466 та -0,5454. Крім того, між результативною ознакою та факторною банківська таємниця спостерігається слабкий обернений зв’язок. В розрізі інших регресорів, а саме: валовий внутрішній продукт на душу населення (ВВП), позови до центрального уряду, внутрішньо переміщені особи, нові переміщення, пов'язані з конфліктом та насильством (кількість випадків), глобальний індекс тероризму, світовий індекс щастя, зв’язок не є підтвердженим на рівні 95% значущості.

Переходячи до аналізу мультиколінеарності регресорів, спостерігаємо лише один випадок високого ступеня залежності між індексом сприйняття корупції і світовим індексом щастя, оскільки відповідний коефіцієнт кореляції приймає значення 0,71. Незважаючи на необхідність вилучення одного із зазначених факторів із моделі з метою нівелювання проблеми колінеарності відповідних векторів, пропонуємо залишити обидва показники, оскільки з економічної точки зору обидва індикатори представляють значний інтерес в розрізі дослідження ризику використання фінансових посередників з метою легалізації кримінальних доходів.

2 етап. Формування методології дослідження. Обґрунтування методів математичної формалізації поставленої проблеми. Оцінювання ризику фінансових посередників з метою легалізації кримінальних доходів з використанням засад інтелектуального аналізу даних пропонується здійснити шляхом побудови нейронної мережі. Економіко-математичні моделі нейронної мережі залежності ризику використання фінансових посередників з метою легалізації кримінальних доходів від факторних ознак запропоновано представити у вигляді багатошарового персептрону та мережі на основі радіальних базисних функцій.

Так, економіко-математична модель нейронної мережі досліджуваного ризику набуває вигляду [110]:

$$f(x) = F\left(\sum_{i_N} w_{i_N j_N N} \dots \sum_{i_2} w_{i_2 j_2 2} F\left(\sum_{i_1} w_{i_1 j_1 1} x_{i_1 j_1 1} - \theta_{j_1 1}\right) - \theta_{j_2 2} \dots - \theta_{j_N N}\right), \quad (2.19)$$

де $F\left(\sum_{i_1} w_{i_1 j_1 1} x_{i_1 j_1 1} - \theta_{j_1 1}\right)$ – шар 1;

$\sum_{i_2} w_{i_2 j_2 2} F\left(\sum_{i_1} w_{i_1 j_1 1} x_{i_1 j_1 1} - \theta_{j_1 1}\right) - \theta_{j_2 2}$ – шар 2;

$F\left(\sum_{i_N} w_{i_N j_N N} \dots \sum_{i_2} w_{i_2 j_2 2} F\left(\sum_{i_1} w_{i_1 j_1 1} x_{i_1 j_1 1} - \theta_{j_1 1}\right) - \theta_{j_2 2} \dots - \theta_{j_N N}\right)$ – шар N;

i – номер входу;

j – номер нейрону у шарі;

$x_{i_1 j_1 1}$ – і-ий вхідний сигнал j-го нейрону у шарі 1;

$w_{i_N j_N N}$ – ваговий коефіцієнт і-ого вхідного сигналу j-го нейрону у шарі N;

$\theta_{j_N N}$ – пороговий рівень j-го нейрону у шарі N.

В свою чергу, економіко-математична модель нейронної мережі ризику використання фінансових посередників з метою легалізації кримінальних доходів у вигляді мережі на основі радіальних базисних функцій набуває вигляду [111, 112]:

$$f(x) = \sum_{i=1}^{N} w_i \varphi(\|x - x_i\|), \quad (2.20)$$

де w_i – ваговий коефіцієнт і-ого вхідного сигналу;

x_i – центри радіальних базисних функцій.

Для побудови нейронної мережі типу багатошарового персептрону MLP використовується алгоритм Бройдена - Флетчера - Гольдфарба – Шанно (Broyden–Fletcher–Goldfarb–Shanno (BFGS)) – один із нарозповсюдженіших квазіньютонівських методів, сутність якого полягає у здійсненні ітеративної процедури числової оптимізації з метою пошуку локального екстремуму нелінійної функції без обмежень. Алгоритм BFGS передбачає реалізацію наступною послідовності кроків [113]:

1) визначення вагових коефіцієнтів випадковими малими величинами та початкового значення наближення зворотнього гессіана V – матриці розміру nxn, де n – довжина вектор градієнта g.

2) розрахунок градієнту g.

3) обчислення кореляції вагових коефіцієнтів $\Delta W = g \cdot \tau, W_{k+1} = W_k - \Delta W$, де τ параметр швидкості навчання.

4) визначення нового значення градієнту $g = g(W)$, враховуючи попереднє значення g_p, а також обчислення зміну градієнту $\Delta g = g - g_p$.

5) розрахунок зворотного гессіана (r зміна градієнта, s зміна ваг):

$$V_{k+1} = V_k - \frac{V_k \cdot s \cdot s^T \cdot V_k}{s^T \cdot V_k \cdot s} + \frac{r \cdot r^T}{s^T \cdot s}, \quad (2.21)$$

$$r = \Delta g_k = g_k - g_{k-1}$$

$$s = \Delta W_k = W_k - W_{k-1}$$

6) розрахунок зміни вагових коефіцієнтів $\Delta W = W \cdot g$ та відповідне коригування параметрів $W = W - \Delta W$.

7) визначимо значення похибки. У випадку перевищення похибки значення заданої точності, необхідно повторити алгоритм, починаючи з 4 етапу. В іншому випадку, алгоритм зупиняється.

Для побудови нейронної мережі на основі радіальних базисних функцій RBF використовується алгоритм RBFT.

Для реалізації даного етапу пропонується використати можливості програми Statistica, пакет Аналіз, вкладка Нейронні мережі, складка Регресія. Визначення вагових коефіцієнтів здійснимо за допомогою методу найменших квадратів.

3 етап. Практична апробація методики проектувальних розрахунків. Проведемо економіко-математичне моделювання двох типів нейронних мереж (багатошарового персептрону MLP та мережі на основі радіальних базисних функцій RBF) регресійної залежності ризик використання фінансових

посередників з метою легалізації кримінальних доходів від релевантних регресорів і систематизуємо отримані результати в табличному вигляді (рисунок 2.10).

Підсумки моделей (Таблиця нейронні мережі.sta)

N	Архітектура	Продуктивність навч.	Контр. продуктивність	Тест. продуктивність	Помилка навчання	Контрольна помилка	Тестова помилка	Алгоритм навчання	Функція помилки	Ф-я актив. прихованих нейр.	Ф-я актив. вихідних нейр.
1	MLP 7-4-1	0,866524	0,768185	0,809887	0,006050	0,011037	0,011871	BFGS 26	Сум. квадр	Гіперболічна	Гіперболічна
2	MLP 7-7-1	0,788958	0,840554	0,819724	0,009235	0,007807	0,011506	BFGS 13	Сум. квадр	Логістична	Синус
3	MLP 7-6-1	0,868518	0,732577	0,841998	0,005977	0,012816	0,010205	BFGS 21	Сум. квадр	Логістична	Гіперболічна
4	MLP 7-6-1	0,808654	0,850489	0,838236	0,008409	0,007230	0,010283	BFGS 13	Сум. квадр	Логістична	Синус
5	MLP 7-4-1	0,845428	0,728619	0,819179	0,006942	0,012588	0,011430	BFGS 12	Сум. квадр	Логістична	Експонента
6	MLP 7-10-1	0,795541	0,795391	0,813813	0,008899	0,010099	0,011420	BFGS 9	Сум. квадр	Експонента	Тотожна
7	MLP 7-8-1	0,828275	0,826108	0,848803	0,007645	0,008299	0,009922	BFGS 19	Сум. квадр	Логістична	Гіперболічна
8	RBF 7-20-1	0,827427	0,691915	0,808933	0,007637	0,014047	0,012504	RBFT	Сум. квадр	Гауссіан	Тотожна
9	RBF 7-20-1	0,855934	0,716948	0,804731	0,006475	0,012829	0,012420	RBFT	Сум. квадр	Гауссіан	Тотожна
10	MLP 7-9-1	0,790786	0,837738	0,846213	0,009130	0,007997	0,009753	BFGS 12	Сум. квадр	Логістична	Тотожна

Рисунок 2.10 – Результати побудови моделей нейронних мереж регресійної залежності ризик використання фінансових посередників з метою легалізації кримінальних доходів від регресорів

Аналіз рисунку 2.10 свідчить про значно більший спектр побудованих нейронних мереж у вигляді багатошарового персептрону MLP (80% моделей), ніж мереж на основі радіальних базисних функцій RBF (20% моделей). Усі представлені моделі характеризуються високим рівнем адекватності, про що свідчать наведені у графах «Продуктиваність навчання», «Контр продуктивність», «Тест продуктивність» критерії. В той же час, продуктивність моделей MLP має значно більший діапазон варіації коефіцієнтів кореляції – від 0,7890 до 0,8685 (навчальна вибірка), від 0,7286 до 0,8505 (контрольна вибірка), від 0,8099 до 0,8448 (тестова вибірка), ніж RBF моделей – відповідно, від 0,8274 до 0,8559 (навчальна вибірка), від 0,6919 до 0,7169 (контрольна вибірка), від 0,8047 до 0,8089 (тестова вибірка). Достовірність 10 побудованих моделей нейронних мереж підтверджується також показником помилки в межах навчальної, контрольної та тестової вибірки, яка приймає близькі до нульового рівня значення.

З метою подальшого використання побудованих моделей для прогнозування рівня ризику використання фінансових посередників з метою легалізації кримінальних доходів виберемо по дві моделі багатошарового персептрону MLP та мережі на основі радіальних базисних функцій RBF з найкращими характеристиками адекватності, а саме: першу модель з архітектурою MLP 7-4-1 (загальна кількість шарів 7, кількість прихованих шарів 4), третю модель з архітектурою MLP 7-6-1 (загальна кількість шарів 7, кількість прихованих шарів 6, рисунок 2.11), восьму модель з архітектурою RBF 7-20-1 (загальна кількість шарів 7, кількість прихованих шарів 20), дев’яту модель з архітектурою RBF 7-20-1 (загальна кількість шарів 7, кількість прихованих шарів 20). Для побудови нейронної мережі типу багатошарового персептрону MLP 7-4-1 та MLP 7-6-1 використовується алгоритм BFGS, відповідно, нейронної мережі на основі радіальних базисних функцій RBF 7-20-1 використовується алгоритм RBFT.

	Ваги	
Ваги ID	З'єднання 1.MLP 7-6-1	Значення ваг 1.MLP 7-6-1
1	GDP per capita (current LCU) --> прихований нейро	0,24229
2	Bank Secrece –> прихований нейрон	-3,56386
3	Claims on central government, etc. (% GDP) --> прихований нейр	-0,35591
4	Internally displaced persons, new displacement associated with conflict and violence (number of cases) --> прих нейрон 1	0,76272
5	Corruption Perceptions Index --> прихований нейро	-3,36003
6	Global Terrorism Index –> прихований нейро	2,85833
7	Happy Planet Index --> прихований нейрон	-1,90713
8	GDP per capita (current LCU) --> прихований нейро	0,09608
9	Bank Secrece –> прихований нейрон	-1,74837
10	Claims on central government, etc. (% GDP) --> прихований нейр	0,01076
11	Internally displaced persons, new displacement associated with conflict and violence (number of cases) --> прих нейрон 2	-0,26839
12	Corruption Perceptions Index --> прихований нейро	-3,03234
13	Global Terrorism Index –> прихований нейро	0,88732
14	Happy Planet Index --> прихований нейрон	-2,69782
15	GDP per capita (current LCU) -->прихований нейро	0,14886
16	Bank Secrece –> прихований нейрон	-1,73532
17	Claims on central government, etc. (% GDP) --> прихований нейр	-0,10462
18	Internally displaced persons, new displacement associated with conflict and violence (number of cases) --> прих нейрон 3	-0,58360

Рисунок 2.11 – Фрагмент архітектури нейронної мережі семишарового персептрону із 6 прихованими шарами MLP 7-6-1

Діаграму розсіювання теоретичних (отриманих шляхом використання побудованих обраних чотирьох нейронних мереж) та фактичних значень ризик використання фінансових посередників з метою легалізації кримінальних доходів наведемо на рисунку 2.12. На основі візуального співвідношення нейронних мереж, побудованих для прогнозування досліджуваного ризику необхідно відмітити високу достовірність обраних модель, про що свідчить достатньо щільне розташування фактичних значень у порівнянні із теоретичними (прогнозними, знайденими на основі використання моделей).

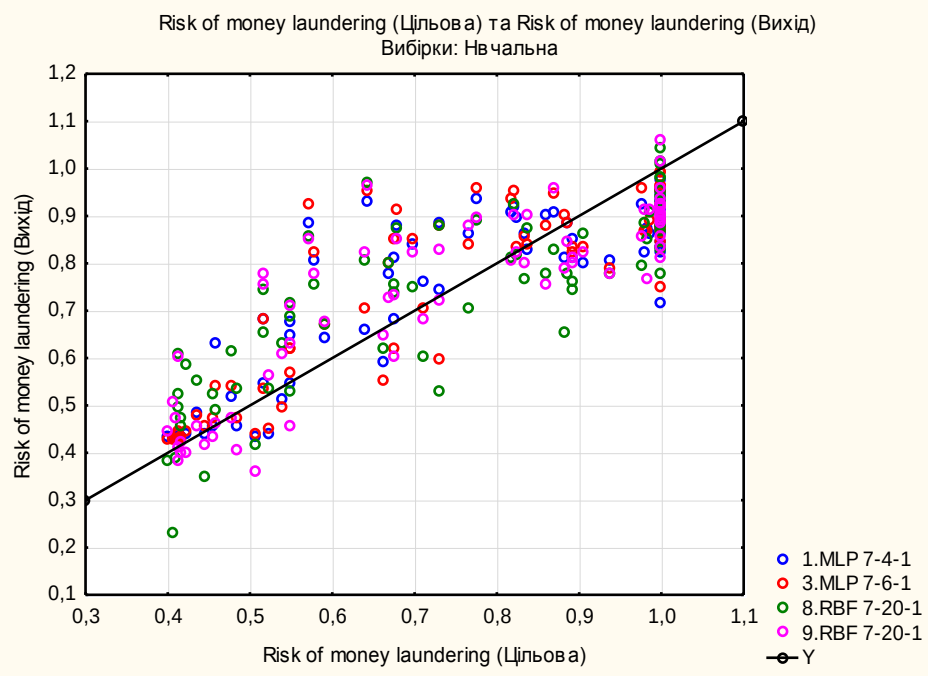

Рисунок 2.12 – Співвідношення фактичних та прогнозних рівнів ризику використання фінансових посередників з метою легалізації кримінальних доходів

Важливого значення в межах формалізації ризику використання фінансових посередників з метою легалізації кримінальних доходів за допомогою нейронної мережі набуває ґрунтовний аналіз вхідних предикторів. Так побудуємо відповідні діаграми розсіювання (рисунок 2.13 – 2.16).

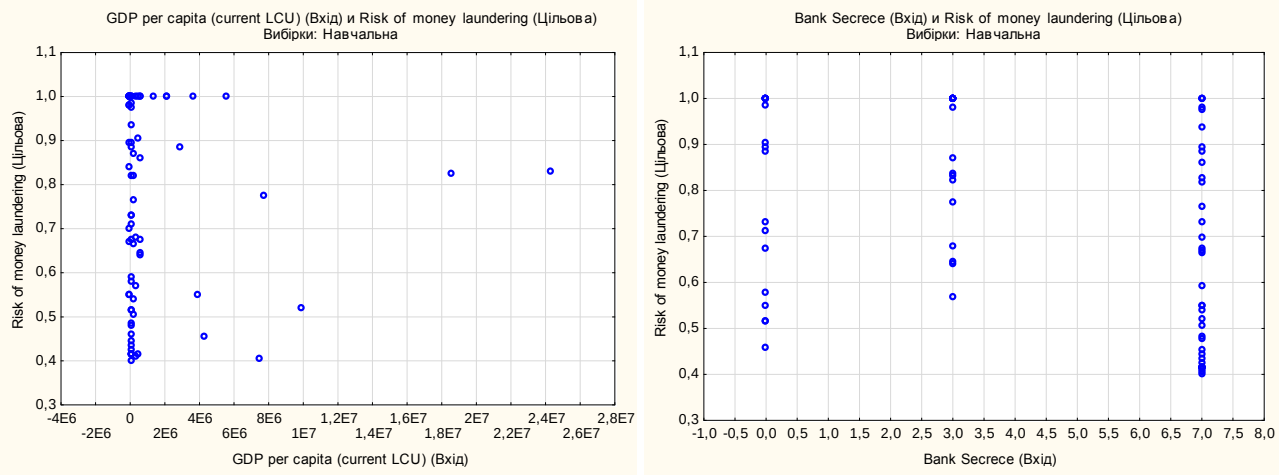

Рисунок 2.13 – Діаграми розсіювання факторів ризику використання фінансових посередників з метою легалізації кримінальних доходів: валовий внутрішній продукт на душу населення, банківська таємниця

Аналіз попарної залежності результативної ознаки від валового внутрішнього продукту на душу населення та банківської таємниці свідчить про (рисунок 2.13): відсутність чіткої залежності ризику використання фінансових посередників з метою легалізації кримінальних доходів від валового внутрішнього продукту на душу населення, оскільки не зважаючи на відсутність значної варіації факторної ознаки, спостерігаємо зміну результативної від 0,4 до 1,0 частки одинці; значення показника банківська таємниця мають чітке групування на 3 кластери, при чому третій кластер є найбільшим за обсягом, тобто зі збільшенням значення даного регресора, досліджуваний рівень ризику буде зростати.

Переходячи до дослідження залежності ризик використання фінансових посередників з метою легалізації кримінальних доходів від позовів до центрального уряду (рисунок 2.14) спостерігаємо наявність хаотичного розподілу, тобто відсутність чіткої взаємозалежності між досліджуваними предикатами. В розрізі показника внутрішньо переміщені особи, нові переміщення, пов'язані з конфліктом та насильством (кількість випадків), аналогічно як для випадку ВВП на душу населення, спостерігається відсутність

чіткої залежності досліджуваного ризику від даного факторного показника, оскільки не зважаючи на відсутність значної варіації факторної ознаки, спостерігаємо зміну результативної від 0,4 до 1,0 частки одинці.

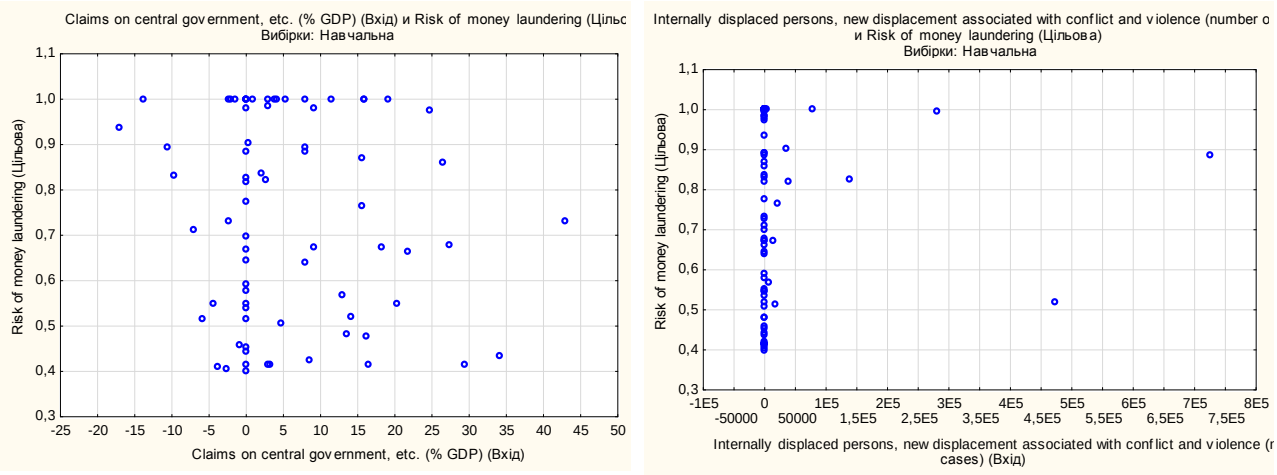

Рисунок 2.14 - Діаграми розсіювання ризику використання фінансових посередників з метою легалізації кримінальних доходів: позови до центрального уряду, внутрішньо переміщені особи, нові переміщення, пов'язані з конфліктом та насильством (кількість випадків)

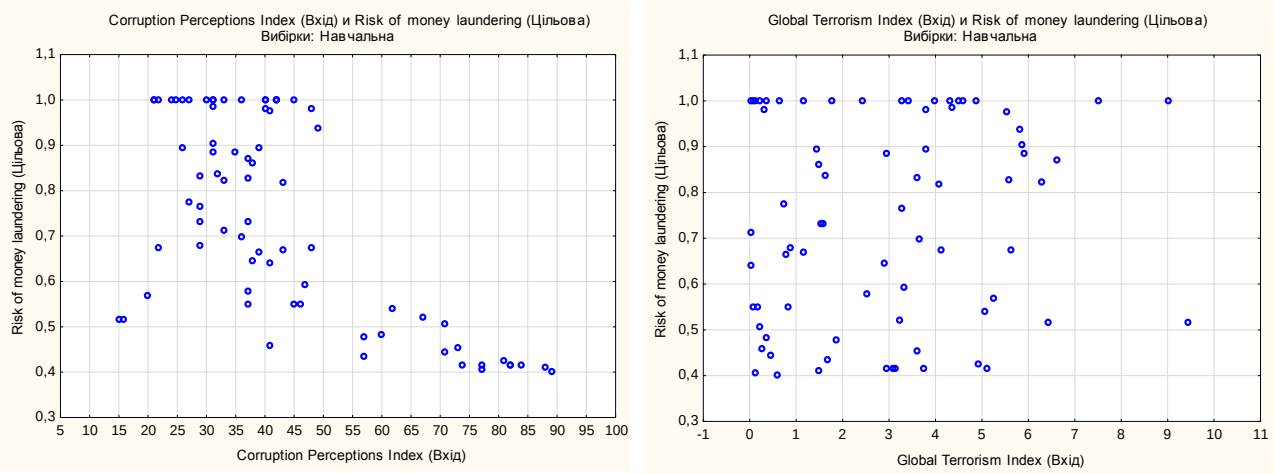

Рисунок 2.15 - Діаграми розсіювання факторів ризику використання фінансових посередників з метою легалізації кримінальних доходів: індекс сприйняття корупції, глобальний індекс тероризму

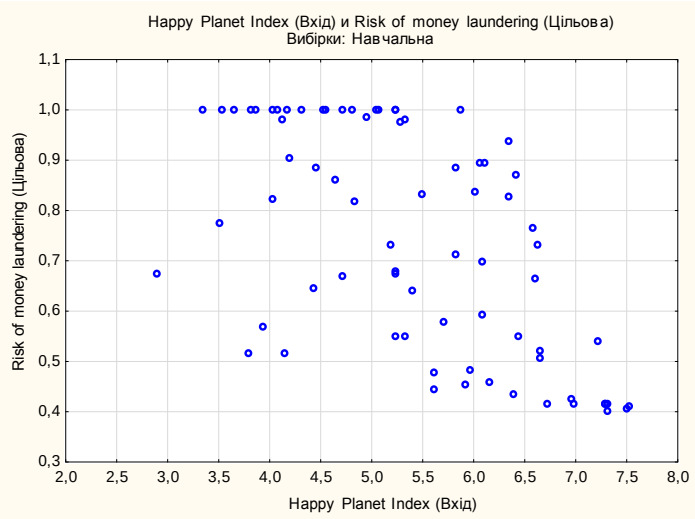

Рисунок 2.16 - Діаграми розсіювання факторів ризику використання фінансових посередників з метою легалізації кримінальних доходів: світовий індекс щастя

Переходячи до дослідження впливу індексу сприйняття корупції (рисунок 2.15) та світового індексу щастя (рисунок 2.16) на ризик використання фінансових посередників з метою легалізації кримінальних доходів спостерігаємо в середньому обернено пропорційну залежність, тобто зі збільшенням факторної ознаки, значення результативної зменшується і навпаки. В розрізі дослідження впливу глобального індексу тероризму спостерігаємо наявність хаотичного розподілу.

Переходячи до останнього, але одного із найважливіших етапів представленої методики – прогнозування майбутніх рівнів досліджуваного рівня ризику, виникає необхідність попереднього детального аналізу якості чотирьох побудованих і описаних вище нейронних мереж: багатошарового персептрону MLP 7-4-1, MLP 7-6-1, мережі на базі радіальних базисних функцій RBF 7-20-1, RBF 7-20-1. Для цього розглянемо статистики передбачених значень (рисунок 2.17) та чутливість моделей обраних нейронних мереж в розрізі вхідних предикторів (рисунок 2.18).

Статистики	Статистики передбачених значень Цільова: Risk of money laundering			
	1.MLP 7-4-1	3.MLP 7-6-1	8.RBF 7-20-1	9.RBF 7-20-1
Мінімум передбачених знач. (Навчальна)	0,43035	0,42597	0,22755	0,36046
Максимум передбачених знач. (Навчальна)	0,97322	0,99047	1,04531	1,05707
Мінімум передбачених знач. (Контрольна)	0,43214	0,42667	0,37610	0,45000
Максимум передбачених знач. (Контрольна)	0,96293	0,99084	0,92952	0,90805
Мінімум передбачених знач. (Тестова)	0,42897	0,42666	0,42732	0,33787
Maximum prediction (Тестова)	0,92754	0,96464	0,96360	0,94910

Рисунок 2.17 – Статистики передбачених значень

Мережі	Чутливість Вибірки: Навчальна						
	Corruption Perceptions Index	Bank Secrece	Happy Planet Index	Global Terrorism Index	GDP per capita (current LCU)	Internally displaced persons, new displacement associated with conflict and violence (number of cases)	Claims on central government, etc. (% GDP)
1.MLP 7-4-1	2,083688	1,206860	1,499772	1,507157	1,022270	0,999329	1,037536
3.MLP 7-6-1	2,144036	1,459289	1,652610	1,628276	1,028311	1,000281	0,998251
8.RBF 7-20-1	1,712405	1,758827	1,459724	1,395042	0,980984	0,953876	0,913740
9.RBF 7-20-1	2,444216	2,132763	1,583271	1,480569	1,033622	0,971278	0,973889
Среднее	2,096087	1,639435	1,548844	1,502761	1,016297	0,981191	0,980854

Рисунок 2.18 – Чутливість моделей обраних нейронних мереж в розрізі вхідних предикторів

Аналіз статистичних характеристик моделей нейронних мереж, представлених на рисунках 2.17 і 2.18, свідчить про високу якість моделей (незначну варіацію мінімальних та максимальних рівнів як в межах навчальної, так і контрольної та тестової вибірок) та незначний рівень чутливості моделей до зміни масштабу вхідних даних.

Переходячи до прогнозування ризику використання фінансових посередників з метою легалізації кримінальних доходів на період 2019 – 2023 рр, сформуємо (на основі експертного підходу) перспективні напрямки розвитку 7 індикаторів регресорів: валовий внутрішній продукт на душу населення (ВВП), позови до центрального уряду, внутрішньо переміщені особи, нові переміщення, пов'язані з конфліктом та насильством (кількість випадків); банківська таємниця;

індекс сприйняття корупції; глобальний індекс тероризму; світовий індекс щастя, представлені в таблиці 2.9.

Таблиця 2.9 – Прогнозні значення вхідних статистичних даних оцінювання ризику використання фінансових посередників з метою легалізації кримінальних доходів

Series Name	2017	2018	2019	2020	2021	2022	2023
GDP per capita (current LCU)	70233,0	84190,3	105238	136809	177852	222315	277894
	26%	20%	25%	30%	30%	25%	25%
Bank Secrece	3	3,0	3	3	3,0	3	3
Claims on central government, etc. (% GDP)	24,2	20,0	19	17	15	13	11
	-12%	-18%	-5%	-10%	-10%	-15%	-15%
Internally displaced persons, new displacement associated with conflict and violence (number of cases)	21000,0	12000,0	9600	8640	8208	7962	7882
	-81%	-43%	-20%	-10%	-5%	-3%	-1%
Corruption Perceptions Index	30	32	28	22	17	13	10
	3%	7%	-13%	-21%	-23%	-24%	-23%
Global Terrorism Index	6,54	6,05	5,5	4,5	3,5	2,5	1,8
	-8%	-7%	-9%	-18%	-22%	-29%	-28%
Happy Planet Index	4,25	4,41	4,65	4,71	5,95	5,11	5,25

Аналіз прогнозних значень ризику використання фінансових посередників з метою легалізації кримінальних доходів (рисунок 2.19, графи 2 – 5) на період 2019 -2023 рр. свідчить про досить близькі рівні значень показників (отримані на основі використання чотирьох нейронних мереж): багатошарового персептрону MLP 7-4-1, MLP 7-6-1, мережі на базі радіальних базисних функцій RBF 7-20-1, RBF 7-20-1. Отже, справедливо зазначити, що прогнозні значення ризику використання фінансових посередників з метою легалізації кримінальних доходів, незалежно від досить низького прогнозного рівня 2019 року, мають тенденцію до стрімкого зростання в найближчій перспективі.

	Таблиця значень користувача										
Спостереження	1.Risk of money laundering_(t)	3.Risk of money laundering_(t)	8.Risk of money laundering_(t)	9.Risk of money launderi ing_(t)	GDP per capita (current LCU)	Bank Secrece	Claims or central governme nt, etc. (% GDP)	Internally displaced persons, new displacement associated with conflict and violence (number of cases)	Corrupti on Percepti ons Index	Global Terroris m Index	Happy Planet Index
1	0,44668	0,31916	0,60453	,77699	105238,(	3,00000(	19,00000	9600,00(	28,00000	28,00000	4,65000(
2	0,91701	0,96150	0,88942(	,90166	105237,8	3,00000(	18,98612	9600,00(	28,00000	5,50000	4,65000(
3	0,91891	0,96077	0,90367	,90930	136809,2	3,00000(	17,08751	8640,00(	22,00000	4,50000	4,71000(
4	0,93335	0,96384	0,91051	,95819	177851,9	3,00000(	15,37876	8208,00(	17,00000	3,50000	5,95000(
5	0,93036	0,96543	0,94262	,91891	222314,9	3,00000(	13,07194	7961,76(	13,00000	2,50000	5,11000(

Рисунок 2.19 – Альтернативні прогнозні значення вхідних та вихідного предикторів оцінювання ризику використання фінансових посередників з метою легалізації кримінальних доходів

Таким чином, справедливо зазначити, що оцінювання ризику використання фінансових посередників з метою легалізації кримінальних доходів на основі нейронних мереж є досить актуальним є потужним і гнучким інструментом забезпечення ефективної системи державного контролю, враховуючи необхідність обробки великого об’єму даних. Цей метод дозволяє автоматично виявляти складні залежності економічних процесів, прогнозувати можливі результати і мати можливість їх використовувати при прийнятті ефективних рішень у сфері державного управління. Впровадження такої методики дозволить ефективно передбачати та боротися зі злочинами пов’язаними з легалізацією доходів, одержаних злочинним шляхом і фінансуванням тероризму, що сприятиме позитивному економічному, фінансовому, соціальному, політичному, культурному розвитку країни, а також підвищить рейтинг країни в світовому просторі.

3 МОДЕЛЮВАННЯ БІЗНЕС-ПРОЦЕСІВ, ПОВЯЗАНИХ ІЗ ПЕРЕВІРКОЮ ОПЕРАЦІЙ НА ПРЕДМЕТ ШАХРАЙСТВА

3.1 Розробка моделей бізнес-процесів перевірок операцій на предмет шахрайств, які здійснюються персоналом банку

Сьогодні банківська діяльність приваблює різного роду шахраїв, які намагаються незаконним шляхом привласнювати кошти, що акумулюються на рахунках у банках або є об'єктом банківських транзакцій. Шахрайство може здійснюватися не тільки зовнішніми по відношенню до банківської установи особами, наприклад, хакерами, але й самими банківськими працівниками. Так, близько 85% шахрайств з банківськими ресурсами здійснюється саме співробітниками банків, які мають доступ до бази даних, паролів, інформаційних ресурсів. Особливо це актуально для невеличких банків та філій, де один працівник має високий рівень відповідальності за велику кількість бізнес-процесів, що може викликати бажання шахраювати з коштами, вилучати інформацію та продавати її стороннім особам, організовувати змови або схеми, через які відбуватиметься легалізація незаконних доходів, тощо.

Дана проблема вимагає кардинальних методів боротьби. Одним з можливих інструментів може бути створення інтегрованої системи, яка включає в себе службу внутрішнього аудиту банку та службу кіберзахисту. Така комплексна інтеграція необхідна для поєднання інструментарію аудиту та служби безпеки. Оскільки служба внутрішнього аудиту є самостійною та підпорядковується тільки керівництву банку, то її статус дозволяє здійснювати перевірки неупереджено. Але здійснення аудиту відбувається, як правило, один раз на рік, то за часту аудитори виявляють порушення працівниками, які було здійснено досить давно. Як результат, дії працівника вже нанесли шкоду банку та його клієнтам. Якщо підходи аудиту інтегрувати в службу кіберзахисту, то це сприятиме створенню потужного інструменту для виявлення шахрайств.

Обов’язковою умовою такої системи повинна бути автоматизація, яка дозволить здійснювати перевірки аудиторами оперативно, щодня та охоплювати значні обсяги інформаційних потоків. Саме тому, пропонуємо впровадити наступні автоматизовані бізнес-процеси аудиту діяльності персоналу з метою виявлення ними шахрайств.

Загалом шахрайства у банках можна поділити на три категорії: шахрайства при розрахунково-касовому обслуговуванні яке в свою чергу включає несанкціоноване списання сум з рахунку, підміну купюр фальшивими, та витягування банкнот з перерахованої пачки; шахрайства з кредитами - зарахування сум, призначених для погашення боргу на інші рахунки, оформлення кредитів на неіснуючих позичальників, оформлення кредитів без відома клієнтів; шахрайства з депозитами - вилучення внесених коштів, применшення сум в документах, списання коштів без відома клієнта.

Але, такий тип шахрайства, як наприклад, підміну купюр фальшивими поки що автоматизувати майже неможливо, на відміну від переказу коштів з рахунків клієнта без його відома, який є найбільш «популярним» способом шахраювання з боку персоналу.

Проведемо моделювання процесу виявлення шахрайств, які здійснюються працівниками банків щодо клієнтських рахунків за допомогою програмного продукту Bizagi Studio у нотації BPMN 2.0 (рисунок 3.1). Моделювання здійснюємо з позиції автоматизації даного процесу, який повинен охоплювати наступні види перевірок, як:

- перевірка активності рахунку клієнтів, чи він не є «сплячим»;
- встановлених лімітів на рахунках, що здійснюються у відповідності із вимогами НБУ, політикою банку, посадовими інструкціями тощо;
- перевірка власника рахунку щодо наявності його у «чорному списку» або він є іноземцем, померлим тощо;
- його геолокація, провайдер, домен, адже різка зміна цих даних може сигналізувати про шахрайство;

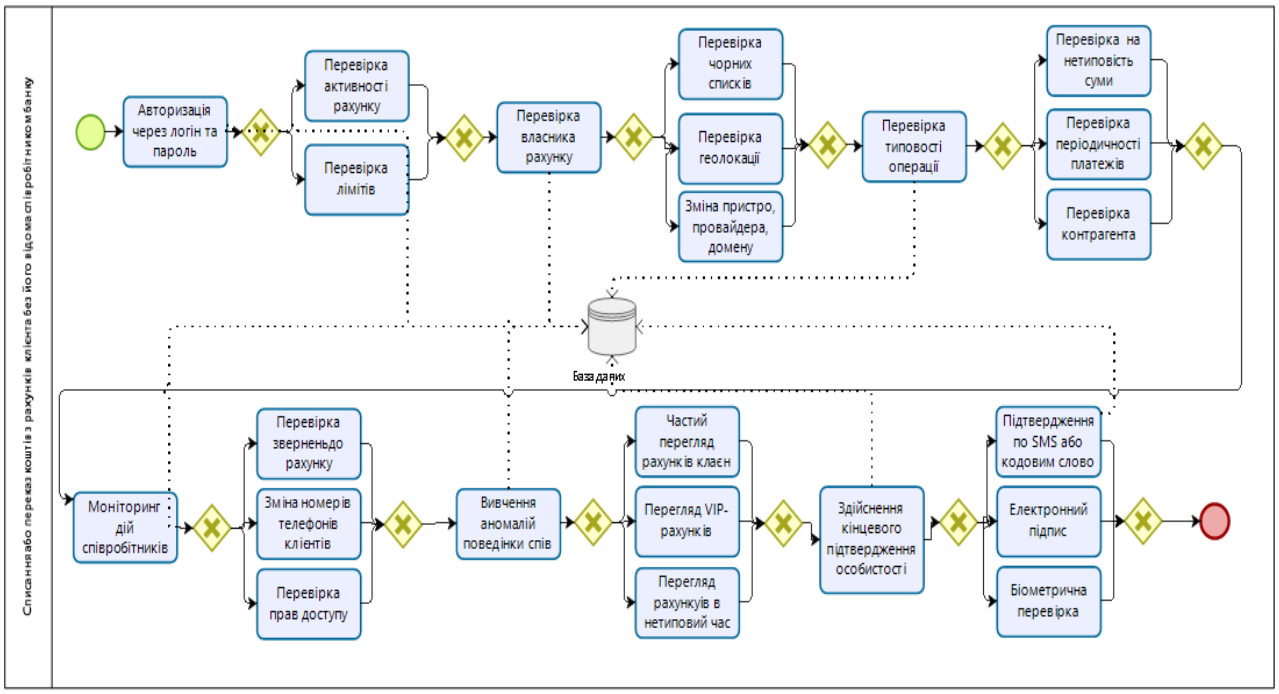

Рисунок 3.1 – Модель бізнес-процесу перевірки операцій працівників щодо здійснення ними шахрайств стосовно клієнтських рахунків

- перевірка типовості операції, а саме нетиповості її суми (нетипово великі або нетипово дрібні операції по розрахунковому рахунку) , періодичності платежів, подвійні оплати , контрагентів (чи були перекази на його рахунок раніше, отримуємо інформацію про одержувача платежу, банку одержувача, призначення та суму платежу, часу і періодичності платежів даному контрагенту);
- перевірка дій співробітників щодо їх звернень до клієнтських рахунків, зміни телефонів (без відома клієнта), прав доступу та відповідності політиці безпеці банку (це можуть бути випадки копіювання бази даних, користування некорпоративною поштою);
- перевірки аномалій, які полягають у частоті перегляду клієнтських рахунків (наприклад, співробітник раніше розглядав в день близько 100 заявок на отримання кредиту, але в якийсь день йому вдалося обробити 250 заявок - таке різке підвищення кількості перевірених заявок говорить про зміну якихось обставин), рахунків VIP-клієнтів (якщо це не входить в його посадові обов'язки), їх перевірка у нетиповий час (необхідно отримати інформацію про те, в який час

доби співробітник найбільш інтенсивно проводить будь-які операції, якщо він робить це особливо часто рано вранці або пізно ввечері, то це досить підозріло, якщо типовий профіль працівника є іншим - це відхилення від профілю і привід встановити за співробітником додатковий контроль);

- здійснення підтвердження особистості за SMS, кодовим словом, електронним підписом, біометрикою («біометричний» портрет клієнта, ідентифікує і верифікує його, порівнюючи спочатку з фотографією в паспорті (або фото, зроблене співробітником банку при оформлення картки), а після з мільйонами ідентичних портретів і з базами лояльних клієнтів і боржників. Також деякі банки застосовують іншу біометричну перевірку клієнтів. Особливо популярним способом є перевірка відбитків пальців. Вона використовується в 48% банківських біометричних проектах. На другому місці - розпізнавання по малюнку вен пальця і голосу).

Наступним способом здійснення незаконних дій з боку персоналу є шахрайство зі «сплячими рахунками». Рахунок вважається «сплячим», якщо за тривалий проміжок часу по ньому не було жодної операції. Такий рахунок є найбільш привабливим для зловмисника, оскільки клієнт з великою ймовірністю не помітить витік грошових коштів, а потім буде вже пізно. У такого виду шахрайства є різновид: іноді злочинець не просто веде кошти на свій рахунок, а виробляє з ними якісь операції, а потім через певний проміжок часу повертає гроші на місце. У зловмисника може бути «гаманець», куди стікаються гроші з інших сплячих рахунків. Якщо один з рахунків раптово перестає бути «сплячим», то зловмисник, замітаючи сліди, перераховує кошти на цей рахунок з «гаманця», або з іншого скомпрометованого «сплячого» рахунка, і для клієнта банку операція виявляється «непомітною». А власники інших рахунків, полеглих «жертвами» зловмисника, просто не в курсі подій, що відбуваються з їхніми коштами.

Проведемо моделювання процесу виявлення шахрайств, які здійснюються працівниками банків по відношенню до «сплячих рахунків» (рисунок 3.2).

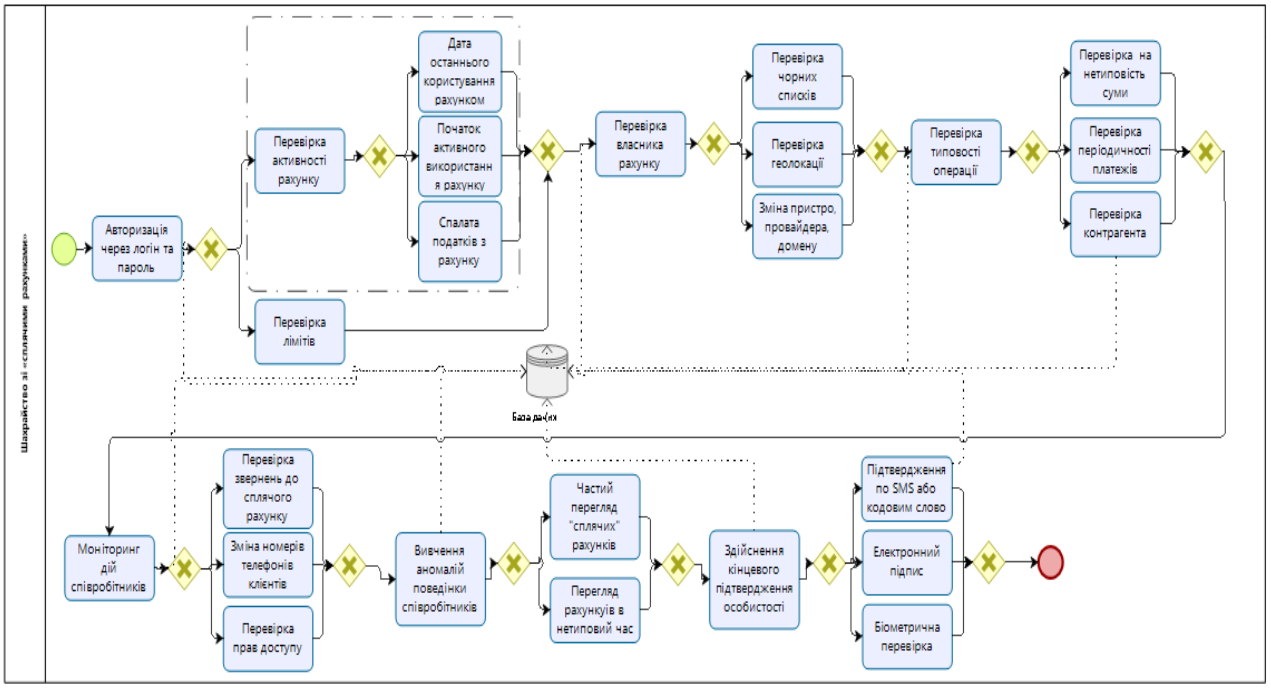

Рисунок 3.2 – Модель бізнес-процесу перевірки операцій працівників щодо здійснення ними шахрайств по відношенню до «сплячих рахунків»

Бізнес-процес автоматизованої перевірки працівників, щодо виявлення такого виду шахрайств, повинен включати: перевірку активності рахунку – дати користування, дати початку активності, сплати податків по рахунку; перевірку власників рахунку на предмет їх наявності у «чорному списку», геолокації, зміни провайдерів, доменів; перевірка типовості операцій, які здійснюються по такому рахунку; перевірка дій та аномалій працівників банку щодо «сплячих рахунків».

Оформлення онлайн-кредитів на неіснуючих позичальників є також розповсюдженим видом шахрайства, яке здійснюють банківські працівники, оскільки вони мають доступ до індивідуальної інформації клієнтів: паспортних даних, індивідуального податкового номеру, тощо. Тому бізнес-процес автоматизованої перевірки співробітника повинен включати дії, характерні для бізнес-процесів перевірки, описаних вище, а також: перевірку кредитної історії позичальника – наявності заборгованості, статусу заборгованості, зміни простроченої заборгованості; перевірку середнього розміру кредитів, наданих по відділенням у динаміці (наприклад, середній розмір кредиту у всіх відділеннях рівний 5700 грн., а в одному - 19999 грн, що є аномалією).

Проведемо моделювання процесу виявлення шахрайств, які здійснюються працівниками банків стосовно оформлення онлайн-кредитів на неіснуючих позичальників (рисунок 3.3).

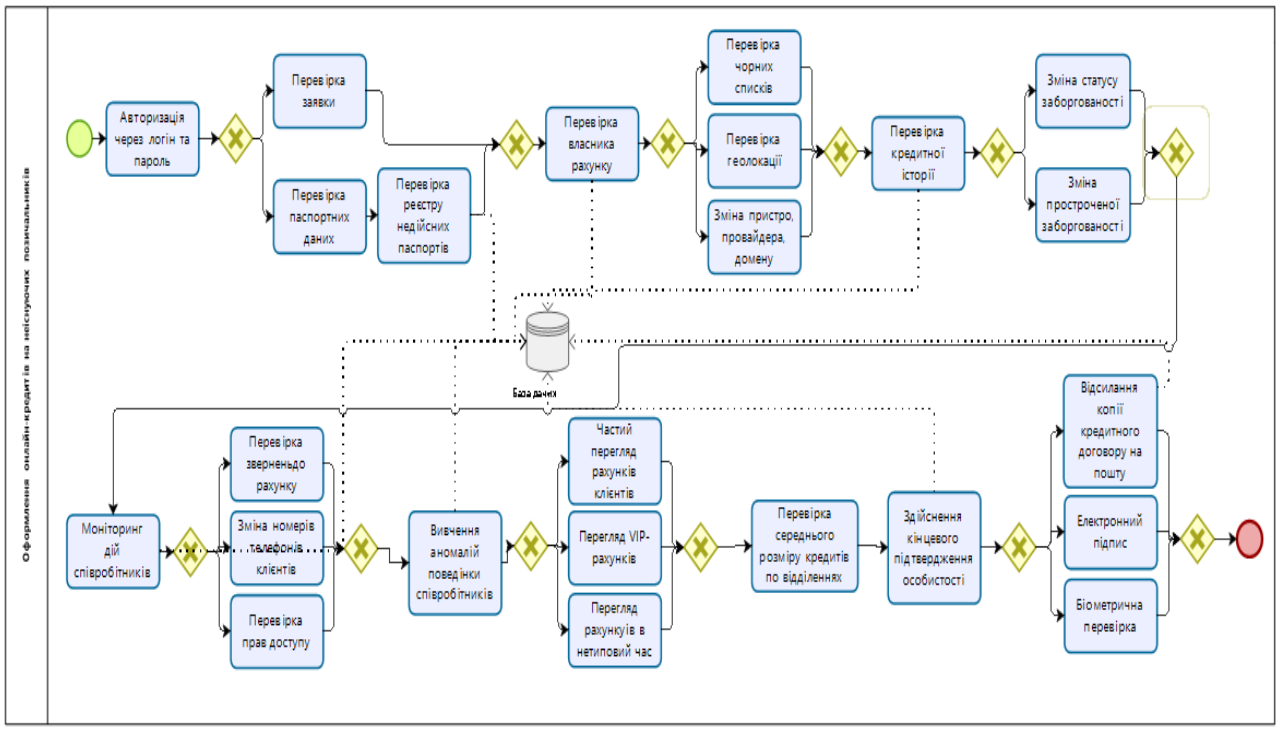

Рисунок 3.3 – Модель бізнес-процесу перевірки операцій працівників щодо здійснення ними шахрайств стосовно оформлення онлайн-кредитів на неіснуючих позичальників

Після здійснення перевірки за вказаними параметрами система повинна надати висновок щодо ймовірності здійснення шахрайства працівником. Або система повинна заздалегідь блокувати такі дії користувача, якщо є ймовірність шахрайства. Але проблема полягає в тому, що задля здійснення працівниками поточних операцій необхідні права доступу до інформаційної системи банку. Якщо це керівник філії, який має значні повноваження, то в такому випадку система не буде його блокувати, якщо він намагається шахраювати. Тому процес блокування можливий для працівників нижньої ланки управління, а відносно керівництва система повинна збирати інформацію щодо його перевірки, та

автоматично надсилати до системи безпеки банку. Тільки тоді знизиться вірогідність шахрайства серед персоналу банку.

Тема боротьби із шахрайствами у банках є досить актуальною, тому для її вирішення необхідні сучасні та прогресивні методи, які передбачають комбінацію методів з різних сфер. Такий підхід дозволить виявляти шахрайства більш ефективно та з меншими наслідками для банку та його клієнтів.

3.2 Розробка моделі бізнес-процесу автоматизованої перевірки операцій на предмет ризику легалізації коштів у банку

Зважаючи на той факт, що фінансова система України орієнтована на банки, основними учасниками відмивання коштів є банки. Так, за даними Державної служби фінансового моніторингу України, кількість повідомлень про підозрілі фінансові операції, зафіксовані у 2017 році, становила 8 013 500 (на 26,8% більше, ніж у 2016 році), і 99% цих звітів формували банки. Водночас зазначимо, що понад 90% фінансових операцій записів, які приймаються Державною службою фінансового моніторингу, належать до обов'язкового фінансового моніторингу [116]. Таким чином, вимоги державних регуляторів призводять до виявлення підозрілих операцій, а система внутрішнього фінансового моніторингу банків є неефективною.

Таким чином, актуальним стає формування автономної, швидкої та багатофункціональної внутрішньобанківської системи фінансового моніторингу. Рішення цього завдання пропонується реалізувати шляхом прототипування інформаційної системи моніторингу транзакцій, пов'язаних з відмиванням грошей через банки.

Вивчаючи особливості прототипування інформаційної системи внутрішньобанківського фінансового моніторингу, зазначимо, що процес виявлення операцій, пов'язаних з відмиванням коштів, є досить важким, періодичним за своєю суттю, значно залежить від кадрових рішень, але добре формалізований. Тому проаналізуємо існуючу систему внутрішньобанківського

фінансового моніторингу, розроблену за допомогою нотації BPMN 2.0 [117] та програмного забезпечення Bizagi Studio [118] (рис. 3.4.).

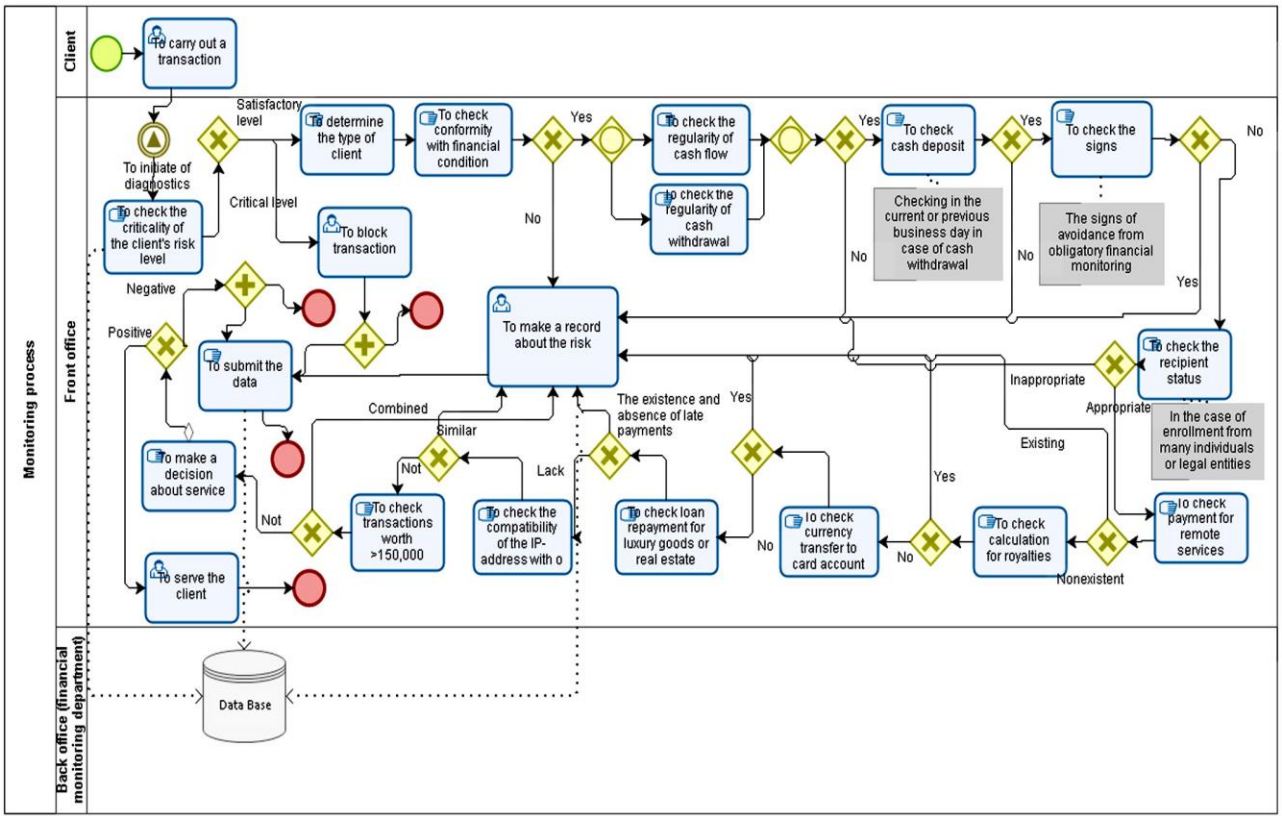

Рисунок 3.4 – Діаграма існуючого бізнес-процесу внутрішньобанківського моніторингу

Таким чином, ідентифікація ризику, пов’язаного з використанням банківських послуг для відмивання грошей, полягає в оцінці джерел доходу, отриманих суб'єктом господарювання або фізичною особою. Таким чином, ми перевіряємо:

– відповідність коштів, перерахованих на банківський рахунок, фінансовому стану клієнта;

– регулярність надходження коштів та подальше зняття грошових коштів;

– ознаки ухилення від обов'язкової процедури фінансового моніторингу з боку клієнта;

– статус бенефіціара у випадку кредитування коштів багатьох фізичних чи юридичних осіб;

– оплата клієнтом за віддалені послуги;

– сплата роялті, зарахування іноземної валюти на картковий рахунок клієнта;

– погашення кредиту клієнта на елітні товари чи нерухомість;

– подібні IP-адреси клієнтських транзакцій з іншими транзакціями;

– операції, що перевищують 150 000 грн.

Після кожної перевірки запис про ризик транзакцій вводиться до бази даних.

Виходячи з зазначеного, існують такі недоліки існуючої системи фінансового моніторингу ризиків, пов'язаних із використанням банківських послуг для відмивання грошей:

– відсутність єдиної системи обов’язкових операцій, які в залежності від рівня їх регулювання певними нормативно-правовими актами є обов'язковими або рекомендованими;

– всі операції здійснюються працівником банку вручну, вимагаючи відповідної компетенції та значної кількості часу;

– введення транзакції в базу ризикових операцій відбувається на розсуд банківського спеціаліста, що робить неможливим високий рівень неупередженості оцінки;

– оцінки ризику відмивання грошей працівниками банку не проводяться під час кожної операції. Визначення підозрілих угод проводиться періодично, залежно від рівня ризику клієнта, від підозри фахівця, відповідно до трансакцій клієнта або відповідно до запитів працівників бек-офісу.

Таким чином, ефективним рішенням проблем низької ефективності внутрішньобанківської системи фінансового моніторингу ризиків, пов'язаних з відмиванням грошей, є використання інформаційних технологій. У вітчизняних банків таких систем немає через специфіку предметної області. Тому ми пропонуємо створити прототип автоматизованої системи фінансового

моніторингу банківських операцій. З цією метою вдосконалено існуючий процес моніторингу банку, враховуючи можливість його автоматизації. На малюнку 2 представлена схема вдосконаленого бізнес-процесу фінансового моніторингу, яка була розроблена за допомогою нотації BPMN 2.0 [117] та програмного забезпечення Bizagi Studio [118].

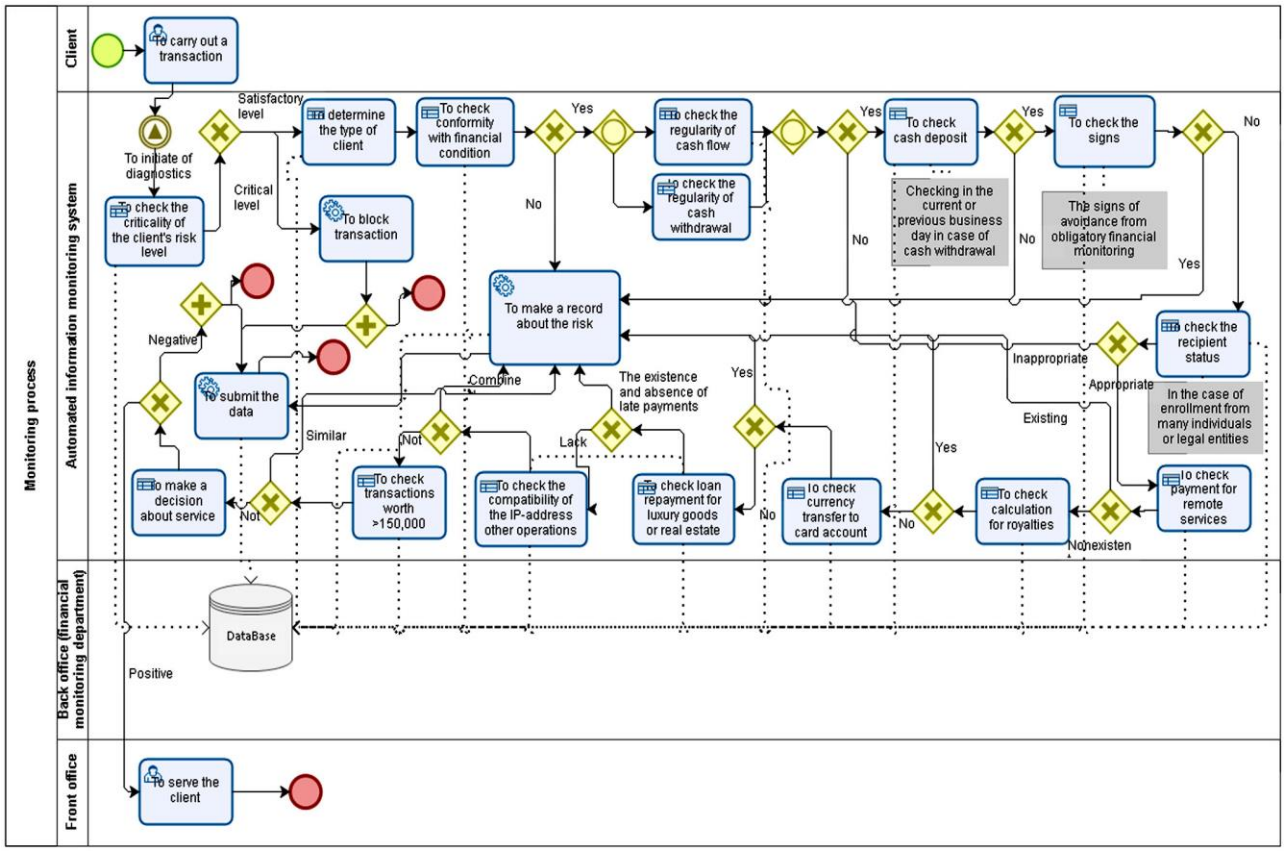

Рисунок 3.5 – Модель бізнес-процесу моніторингу в автоматизованому системному середовищі

Розглядаючи дані, представлені на рисунку 3.5, можна стверджувати, що автоматизована система замість працівників фронтового офісу банку повинна мати справу з основними діями, пов’язаними з перевіркою підозрілих угод. Це дозволить розвантажити керівників фронт-офісів щодо перевірки потенційних операцій, пов'язаних з відмиванням грошей. Їх автоматизація допоможе підвищити ефективність роботи персоналу банку під час здійснення фінансового моніторингу. А саме, по-перше, це дозволить здійснювати постійну онлайн-перевірку. По-друге, ситуація впливу працівника на процес перевірки та

приховування чи спотворення його результатів більше не буде можливою. Це відбудеться тому, що система передбачає застосування логіки бізнес-правил, яка сприятиме автоматичному вибору тих операцій, які не відповідають заданим умовам. Адміністратор несе відповідальність за їх налаштування, а інші банківські працівники не зможуть цілеспрямовано впливати на процес верифікації. По-третє, така система дозволяє перевірити більший обсяг операцій щодо їх участі у відмиванні грошей та фінансуванні тероризму. Оскільки моніторинг обов'язково застосовується до операцій, наприклад, сума яких перевищує 150 000 гривень, відповідно операції з меншими сумами, які також можуть мати кримінальні джерела походження, залишаються поза увагою.

Використання автоматизованої системи полегшить перевірку всіх транзакцій незалежно від їх суми. По-четверте, перевагою запропонованого рішення є гнучкість налагодження цієї системи у разі зміни законодавства чи положень Національного банку України та інструкцій банку щодо перевірки таких операцій. Це можливо завдяки змінам параметрів бізнес-правил, що використовуються для перевірки транзакцій.

При розробці внутрішньобанківської системи фінансового моніторингу важливо побудувати інформаційну модель, яка забезпечує розуміння взаємозв'язків між об'єктами системи та їх структурою. Для цього на основі запропонованого бізнес-процесу (рис. 3.5) автори розробили інформаційну модель, засновану на техніці структурованого аналізу та проектування (SADT) у нотації DFD (Diagram Flow Diagrams). Автори обрали цю методологію завдяки її можливостям опису потоків даних з урахуванням їх взаємодії в процесі ручної та автоматизованої обробки інформації. Таким чином, на рисунку 3.6 показаний результат цього моделювання - модель DFD фінансового моніторингу банківських операцій, що виконується в програмному середовищі All Fusion Process Modeller [119].

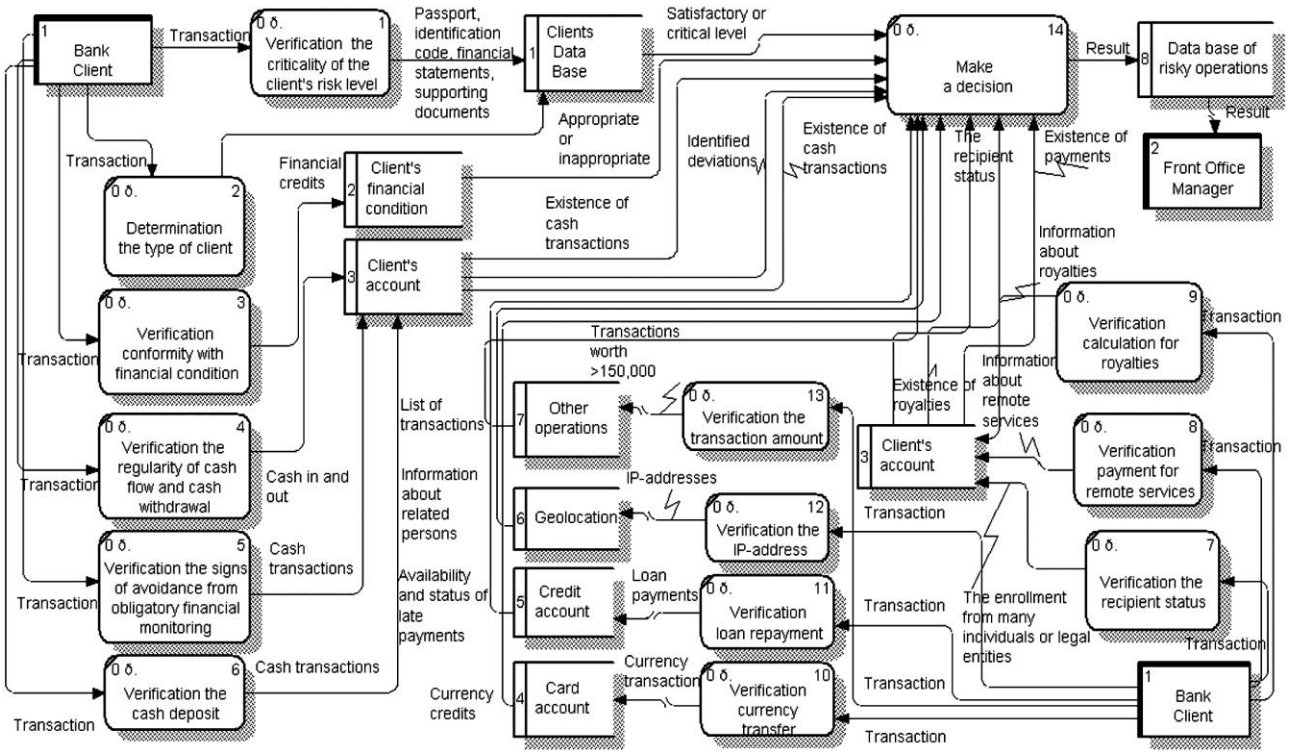

Рисунок 3.6 – DFD-модель автоматизованого моніторингу банківських транзакцій

Запропонована модель включає такі основні суб'єкти, як "Клієнт банку" та "Менеджер фронт-офісу", 14 основних функцій, пов'язаних з верифікацією банківських операцій щодо їх використання у відмиванні грошей чи фінансуванні тероризму, та 8 основних структур для зберігання інформації. Вхідні та вихідні потоки інформації визначаються між представленими об'єктами.

Функції 1-13 на рисунку 3.6 показують основні сфери моніторингу: перша перевірка критичності рівня ризику клієнта, друга верифікація типу клієнта, третя перевірка відповідності фінансовому стану, четверта перевірка регулярності грошових потоків та зняття готівки, п'ята перевірка ознак уникнення обов'язкового фінансового моніторингу, шоста перевірка депозиту готівкою тощо. У цих сферах є операції, визначені так, ніби є ризик відмивання грошей. Результати перевірок акумулюються у блоці «Прийняти рішення», де приймається рішення про те, чи існує ризик для транзакції чи немає ризику.

Розуміння інформації про вхідні та вихідні потоки є дуже важливим. Оскільки основним предметом моніторингу є клієнтська транзакція, вона перевіряється шляхом порівняння з критеріями. В якості критеріїв банк може використовувати фінансову документацію клієнта, кредитні платежі, інформацію про платежі за дорогі покупки, операції, які не відповідають виду діяльності клієнта, інформацію про виплату авторських гонорарів, IP-адресу операції тощо. Ця інформація зазвичай міститься в автоматизованій банківській системі, куди буде інтегрований автоматизований модуль фінансового моніторингу.

Розроблена модель DFD лягла в основу створення логічної схеми даних, реалізація якої дозволила сформувати внутрішню інформаційну систему прототипу системи. Для цього були створені сутності, встановлені відносини, обрані типи відносин та вказані атрибути. Таким чином, була створена повна структура даних для розробки бази даних автоматизованої системи моніторингу, яка була розроблена за допомогою програмного продукту Bizagi Studio [118] (рис. 3.7).

Запропонована модель (рис. 3.7) визначає структуровану модель бази даних на базі SQL Server, яка визначає, як дані доступні, зберігаються та використовуються в системі. Цінність моделі полягає в тому, що вона враховує основну специфіку моніторингу транзакцій у банку.

Наступним кроком у розробці системного прототипу є розробка інтерфейсів та визначення основних бізнес-правил. Таким чином, були розроблені форми інтерфейсу користувача, які дозволяють побачити, як користувач взаємодіє із системою. Оскільки запропонована система здійснює весь процес верифікації без участі працівника, була створена форма результатів верифікації (рис. 3.8).

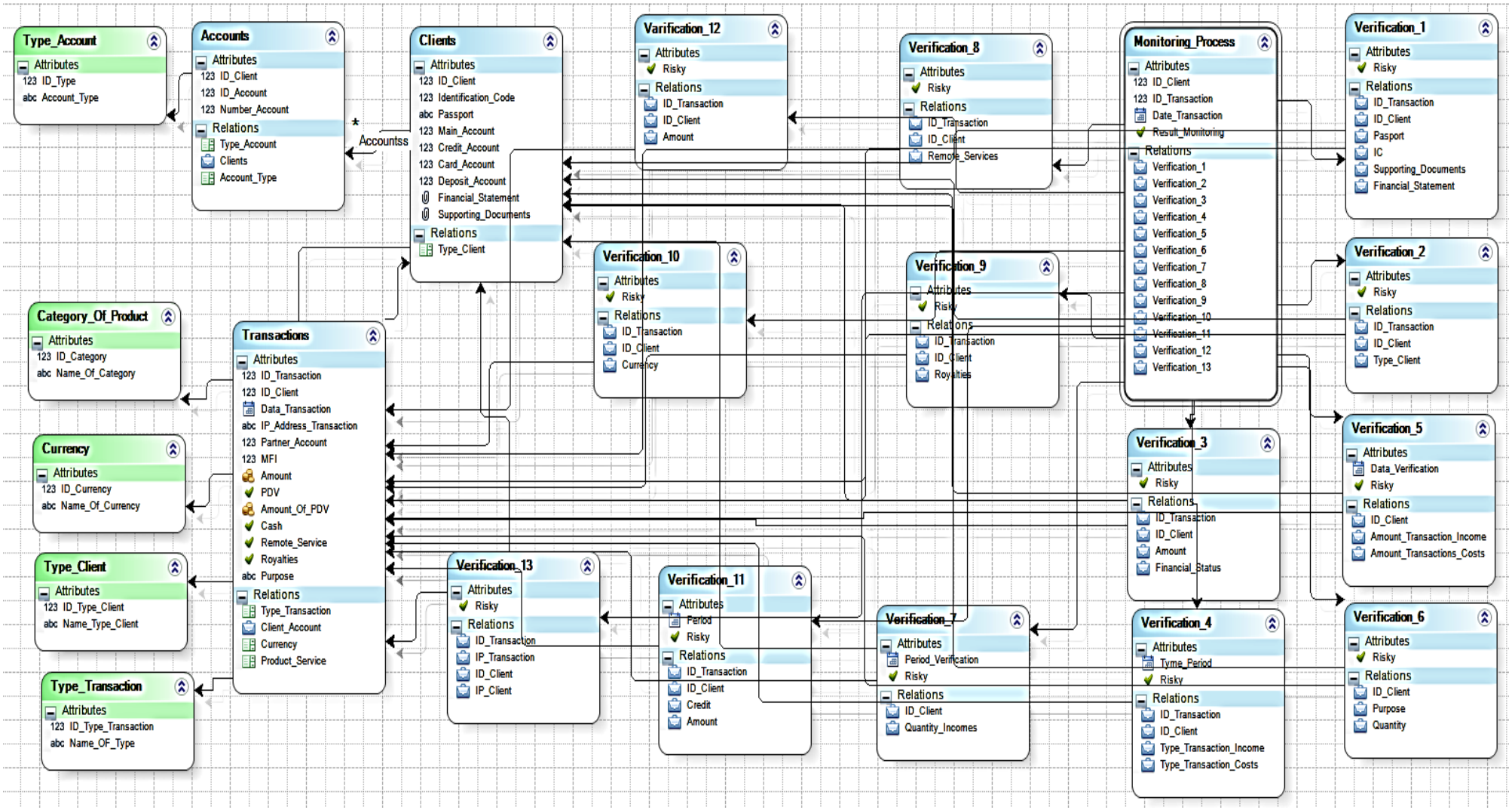

Рисунок 3.7 – Структурна модель бази даних автоматизованої системи моніторингу

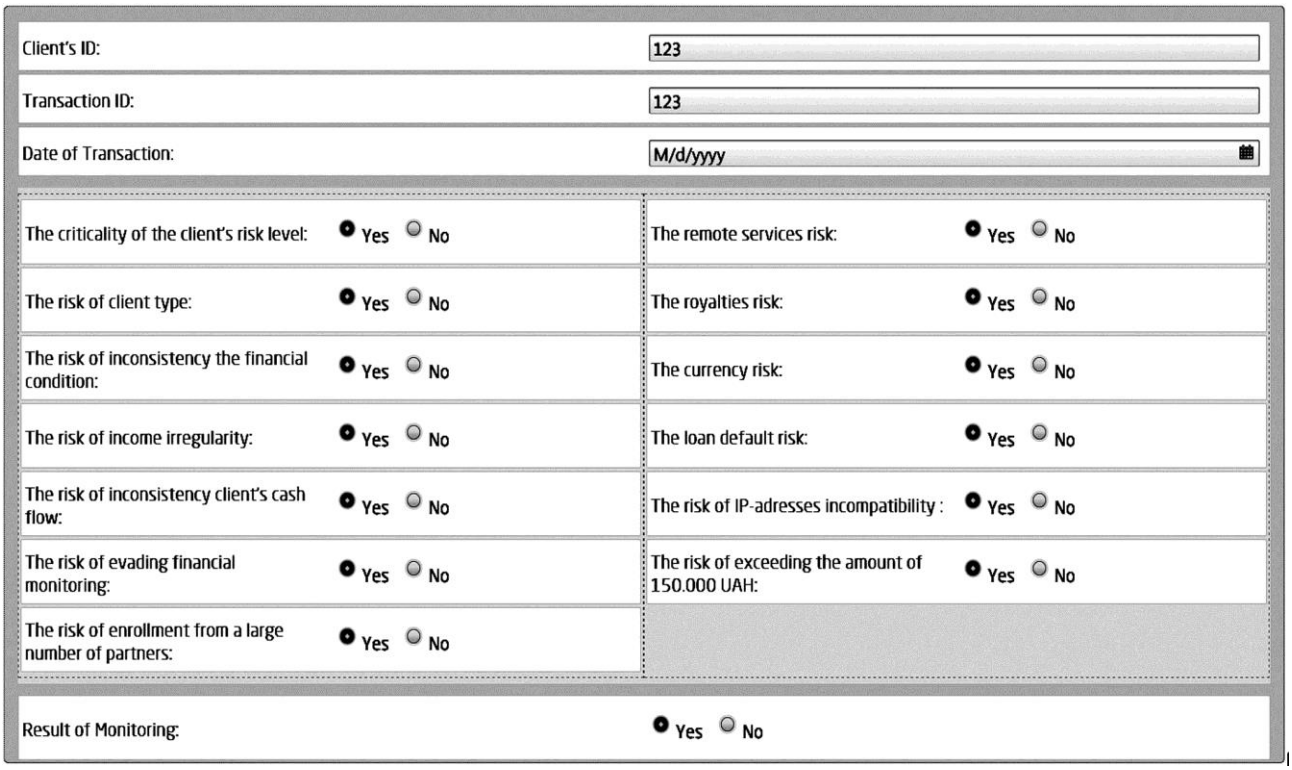

Рисунок 3.8 – Форма інтерфейсу користувача, яка містить результати перевірки

Розроблена форма дозволяє отримувати інформацію про клієнта, транзакцію та результати моніторингу за тринадцятьма правилами. Для кожної позиції ризику було запропоновано лише два варіанти. Система надає опцію "ТАК", якщо є ризик здійснення транзакції. Система видає "НІ" за відсутності ризику. Інформаційна система також дозволяє отримати загальний результат моніторингу. Відповідь "ТАК" вказуватиме на наявність ризику на будь-якому рівні перевірки, і транзакція буде відхилена. Якщо на всіх рівнях моніторингу немає ризику, система дасть відповідь "НІ" і транзакція буде прийнята.

Для автоматичного виконання дій системою розроблено основні правила. Вони важливі для подальшого розвитку автоматизованої системи. Розробка правил здійснювалася за такою логікою, представленою формулами 3.1-3.2.

Для проведення моніторингу – (формула 3.1):

$$\begin{gathered} IF\ [Condition\ of\ Verification\_1 \neq Criteria\ of\ Verification\_1]\ THEN\ [Risk = \\ 1]\ ELSE\ [Risk = 0] \\ \dots \\ IF\ [Condition\ of\ Verification\_N \neq Criteria\ of\ Verification\_N]\ THEN\ [Risk \\ = 1]\ ELSE\ [Risk = 0], \end{gathered} \tag{3.1}$$

де: *Condition of Verification_1* – умова перевірки операції на відповідність критерію 1;

Condition of Verification_N – умова перевірки операції на відповідність критерію N;

N – номер критерію перевірки від 1 до 13;

Criteria of Verification_1 – перший критерій, обраний для перевірки операції на предмет існування ризику відмивання грошей;

Criteria of Verification_N – критерій N, обраний для перевірки операції на предмет існування ризику відмивання грошей;

Risk = 1 – наявність ризику відмивання грошей;

Risk =0 – відсутність ризику відмивання грошей.

Для отримання загального результату моніторингу встановлюється наступне правило (формула 3.2):

$$\begin{gathered} IF\ [Verification\_1 = 1\ OR\ Verification\_2 = 1\ OR\ Verification\_3 = 1\ OR \\ Verification\_4 = 1\ OR\ Verification\_5 = 1\ OR\ Verification\_6 = 1\ OR \\ Verification\_7 = 1\ OR\ Verification\_8 = 1\ OR\ Verification\_9 = 1\ OR \\ Verification\_10 = 1\ OR\ Verification\_11 = 1\ OR\ Verification\_12 = 1\ OR \\ Verification\_13 = 1]\ THEN\ [\text{“YES” } Risk\ AND\ Reject\ operation]\ ELSE \\ [\text{“NO” } Risk\ AND\ Accept\ Operation], \end{gathered} \tag{3.2}$$

де: *Verification_1,2,…,13* – результат кожної перевірки на відповідність або невідповідність критерію перевірки;

“YES” Risk AND Reject operation – рішення, коли існує ризик відмивання грошей та відхилення угоди;

“NO” Risk AND Accept Operation – рішення, коли немає ризику відмивання грошей і операція здійснюється.

Розроблені правила складають групу «Визначте вирази», що визначає поведінку системи за певних умов. Таким чином, правила враховують умови розгалуження, які відповідають позитивному результату верифікації, коли транзакція не загрожує ризиком відмивання грошей або негативною, коли транзакція вводиться до бази ризикових операцій та блокується системою.

Справедливо зазначити, що незважаючи на те, що проблема оцінки ризику, пов’язаного із використанням банків для відмивання грошей чи фінансування тероризму, не є пріоритетним, але його вирішення є надзвичайно важливим як для банків, так і для держави в цілому. Таким чином, за останні п’ять років темпи відмивання грошей через банківські операції значно перевищують темпи економічного зростання в Україні. У свою чергу, для банків ризики проявляються у посиленні нагляду з боку Національного банку України, посиленні мотивації банківського персоналу до шахрайства та майбутньої втрати фінансової стабільності.

Банки, як суб'єкти первинного фінансового моніторингу, повинні аналізувати транзакції клієнта, щоб виявити особливості, характерні для відмивання грошей, отриманих незаконним шляхом. У рамках цієї діяльності вони можуть виявляти ці операції лише після факту. Практичний досвід банків України показує, що фінансовий моніторинг є періодичним, несистематичним, проводиться вручну, на його результати може впливати "людський фактор", що є проявом корумпованої складової. Але головне завдання моніторингу - не допустити транзакцій, з якими існує ризик відмивання грошей. Тому прототипування інформаційної системи моніторингу банківських операцій, пов'язаних з відмиванням коштів, є дуже актуальною проблемою.

Таким чином, було отримано прототип автоматизованої системи фінансового моніторингу транзакцій для пошуку їх зв'язку з відмиванням грошей. Прототип складається з моніторингової моделі бізнес-процесів в автоматизованому системному середовищі, автоматизованої моделі моніторингу банківської діяльності DFD, структурної моделі бази даних, форм інтерфейсу користувача та логіки бізнес-правил перевірки.

Застосування запропонованої інформаційної системи дозволяє перевірити транзакції клієнта за тринадцятьма правилами ризику. Такий підхід дозволяє оцінити ризик відмивання грошей за кожною транзакцією. Якщо операція не відповідає хоча б одному правилу, її відхиляють. Система робить висновок про підвищений ризик цієї транзакції. Через автоматичний процес вплив банківських працівників на операції з ризиком виключається. Крім того, фронт-офіс може приймати рішення на основі інформації, отриманої з інформаційної системи.

Впровадження запропонованої системи дозволить автоматизувати процес моніторингу, знизити його трудомісткість, підвищити ефективність перевірки шляхом опрацювання більшої кількості транзакцій та перенести фокус з працівника на автоматизовану систему, щоб зменшити вплив на результати перевірки.

Надалі запропонований прототип планується впровадити у практичну діяльність банків на рівні суб'єктів первинного фінансового моніторингу. Оскільки ця реалізація передбачає необхідність оптимізації моніторингового бізнес-процесу в банку, це вимагає значної кількості часу. В сучасних умовах посилення боротьби з проблемою відмивання грошей інтерес банків до цього рішення є безумовним. Під впливом регулювання цієї проблеми Національним банком України впровадження банками автоматизованої системи моніторингу сприятиме створенню єдиної інформаційної бази моніторингу та інтеграції інформації на рівні суб'єктів державного моніторингу.

ВИСНОВКИ

Отримані наукові результати створюють передумови формування ефективної комплексної системи кібербезпеки банків, інтегрованої із внутрішнім аудитом та моніторингом, спрямованої на боротьбу із банківськими шахрайствами. Серед основних результатів, що мають наукову новизну і практичну значущість, слід зазначити такі:

– визначено, що для попередження кіберзагроз ключову роль відіграє система внутрішнього аудиту, яка виявляє слабкі місця в системі забезпечення кібербезпеки та управління кібер-ризиками, надає об'єктивну оцінку поточному рівню кібербезпеки в банку, виробляє рекомендації щодо усунення слабких місць. Внутрішній аудит визначено як періодичну систему збору та оцінки інформації для визначення того, чи забезпечують всі системи банку належний стан захищеності інформаційних активів та інформаційної інфраструктури, збереження властивостей інформаційних активів (доступності, цілісності чи конфіденційності) на цільовому рівні відповідно до встановлених критеріїв в умовах постійного впливу зовнішніх та або / внутрішніх загроз з дотриманням вимог національного та міжнародного законодавства. Було розроблено механізм внутрішнього аудиту, як сукупності взаємопов'язаних елементів (цілі та завдання, об'єкт, суб'єкт), що функціонують на основі загальних та спеціальних принципів та дозволяють об'єктивно оцінити рівень захищеності та збереження властивостей інформаційних активів та інформаційної інфраструктури банку в умовах постійного впливу зовнішніх та або / внутрішніх загроз, а також дотримання вимог національного та міжнародного законодавства;

– встановлено, що в системі аудиту доцільно використовувати сучасні методи виявлення та попередження шахрайства персоналу: стандарт ISO/IEC 27001 «Управління інформаційною безпекою», метод аналізу розривів, метод оцінки ризиків, система фрод-моніторингу, якісні методи, кількісні методи, методи машинного навчання. Доведено, що найбільш оптимальними для врахування невизначеності та виявлення шахрайств у банках є гібридні методи,

що використовують сильні сторони різних підходів, застосування яких дозволяє знизити рівень шахрайства та підвищити відповідальність банківського персоналу;

– визначено доцільність застосування заходів впливу у сфері фінансового моніторингу для забезпечення банківської безпеки, а саме: скорочення кількості фінансових злочинів і відповідних втрат від них; зниження об'єму тіньової економіки; посилення надійності банків; посилення контрою за міждержавними переказами; контроль за діяльністю конвертаційних центрів; збільшення сум сплачених податків від викритих нелегальних доходів; покращення ефективного застосування бюджетних ресурсів; скорочення корупційного рівня; зростання показника конкурентоспроможності країни; боротьба з кіберзлочинністю; контроль операцій з цінними паперами; зосередження уваги на можливих шахрайствах у банківській сфері; посилення протидії фінансуванню тероризму, військових дій;

– розроблено динамічну модель у вигляді класичної моделі «хижак-жертва», яка дозволяє провести дослідження питання моделювання процесу боротьби з кібератаками у сфері електронного банкінгу. Побудова імітаційної моделі дозволила провести числові експерименти на умовно встановлених значеннях;

– розроблено нечітко-множинну модель, як надає аудитору можливість оцінити ризик шахрайства банківського персоналу та визначити основні сфери, що найбільше сприяють шахрайству. Модель було розроблено для оцінювання ризику шахрайства персоналу щодо викривлення фінансової звітності. З цією метою виділено три групи індикаторів ризику: спонукання до викривлення фінансової звітності; сприятливі можливості для викривлення фінансової звітності; обґрунтування викривлення фінансової звітності. Використання даної моделі на практиці дозволить підвищити загальну ефективність аудиту та сприятиме попередженню шахрайств;

– проведено оцінку ризику використання фінансових посередників з метою легалізації кримінальних доходів на основі нейронних мереж з метою

забезпечення ефективної системи контролю з боку Національного банку України. Метод дозволяє автоматично виявляти складні залежності економічних процесів, прогнозувати можливі результати і мати можливість їх використовувати при прийнятті ефективних рішень у сфері державного управління. Застосування запропонованої методики дозволить ефективно передбачати та боротися зі злочинами пов'язаними з легалізацією доходів, одержаних злочинним шляхом і фінансуванням тероризму;

– розроблено моделі бізнес-процесів перевірок операцій на предмет шахрайств, які здійснюються персоналом банку, з урахуванням потенційної можливості їх автоматизації та інтегрування в систему кібербезпеки банку. Моделі було розроблено для трьох ймовірних ситуацій шахрайства банківськими працівниками, а саме: списання або переказ коштів з рахунків клієнта без його відома; шахрайство зі «сплячими рахунками»; оформлення онлайн-кредитів на неіснуючих позичальників;

– розроблено модель бізнес-процесу моніторингу банківських транзакцій на предмет можливості відмивання грошей з урахуванням створення автоматизованої інформаційної системи внутрішнього банківського моніторингу, інтегрованої в автоматизовану інформаційну систему банку. Запропоновано прототип інтегрованої бази даних, інтерфейсу результатної форми моніторингу та інформаційної моделі пропонованої системи. Реалізація розробленої системи сприятиме комплексної системи протидії банківським шахрайствам, яка об'єднає систему кіберзахисту, аудиту та моніторингу банку.

Подальші дослідження повинні бути спрямовані на розробку внутрішньобанківської системи кібербезпеки та організаційно-інституційних засад забезпечення стійкості фінансового кіберпростору на загальнодержавному рівні, а саме: визначення кількісного та якісного рівня ефективності роботи внутрішньобанківської системи кібербезпеки; рівня стійкості фінансового кіберпростору на загальнодержавному рівні; розробку проектів нормативно-правових актів та внутрішньобанківських інструкцій щодо організації системи кіберзахисту в банках.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Boer M., Vazquez J. Cyber Security & Financial Stability: How cyber-attacks could materially impact the global financial system. URL: https://www.iif.com/Portals/0/Files/IIF%20Cyber%20Financial%20Stability%20Paper%20Final%2009%2007%202017.pdf?ver=2019-02-19-150125-767 (дата звернення: 01.05.2019).

2. The impact of cybersecurity incidents on financial institutions. URL: https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_Generali_The-Impact-of-Cybersecurity-Incidents-on-Financial-Institutions-2018.pdf (дата звернення: 01.05.2019).

3. Restore, rationalize and reinvent. A fundamental shift in the way banks manage risk: Eighth annual global EY/IIF bank risk management survey. URL: https://www.ey.com/Publication/vwLUAssets/ey-eighth-annual-global-eyiif-bank-risk-management-survey/$FILE/ey-eighth-annual-global-eyiif-bank-risk-management-survey.pdf (дата звернення: 01.05.2019).

4. Посилення цифрового середовища проти кібер-загроз. Дослідження глобальних тенденцій інформаційної безпеки за 2018 рік: основні висновки. *PwC Україна. Міжнародне рейтингове агенство*: URL: https://www.pwc.com/ua/uk/survey/2018/pwc-2018-gsiss-strengthening-digital-society-against-cyber-shocks-ukr.pdf (дата звернення: 01.05.2019).

5. Облік і аудит у банках: підручник / А. М. Герасимович, Л. М. Кіндрацька, Т. В. Кривов’яз та ін. / За заг. ред. А. М. Герасимовича. К.: КНЕУ, 2004. 536 с.

6. Кірєєв О. І. Внутрішній аудит у банку : навчальний посібник для студентів вищих навчальних закладів. К: Центр навчальної літератури, 2006. 220 с.

7. Костырко Л. А. Банковский аудит : учебное пособие. Луганск: [б.в.], 1998. 220 с.

8. Маркевич М. А. Організація і методика внутрішнього аудиту в банку: дис. ... канд. екон. наук : 08.00.09; Університет банківської справи Національного банку України. К., 2011. 301 с.

9. Письменна М.С. Внутрішній аудит в банківській системі : дис. ... канд. екон. наук : 08.00.09; Одеський державний економічний університет. Одеса, 2011. 265 с.

10. Аудит у банках: навчальний посібник / За заг. ред. О. М. Сарахман. - К.: УБС НБУ, 2007. 334 с.

11. Внутрішній аудит у банку: навчальний посібник / О. М. Сарахман та ін. – К.: УБС НБУ, 2015. 239 с.

12. Арсланбеков-Федоров А. А. Система внутреннего контроля коммерческого банка: монография / Под ред. А. М. Тавасиева. М.: Юнити-Дана, 2004. 191 с.

13. Банк С. В. Аудит в коммерческих банках: учебное пособие. М.: Экономистъ, 2007. 156 с.

14. Аудит банков: учебное пособие / Г. Н. Белоглазова, Л. П. Кроливецкая, Е. А. Лебедев [и др.]. / Под ред. Г. Н. Белоглазовой, Л. П. Кроливецкой. Изд. 2-е, перераб. и доп. М.: Финансы и статистика, 2005. 413 с.

15. Соколинская Н.Э. Банковский аудит. М.: Перспектива, 1994. 118 с.

16. Barakat A. Banks Basel II norms requirement regarding internal control. *Delhi Business Review*. 2009. № 10 (2). P. 35-49.

17. Rossiter C. Top 10 priorities for internal audit in a changing environment: new realities lead to a larger, more central and more visible role for internal audit. *Bank Accounting & Finance.* Aug.-Sept. 2007. P.34-40.

18. Akinyomi O. J. Examination of fraud in the Nigerian banking sector and its prevention. *Asian Journal of Management Research.* 2012. № 3 (1), P. 182-194. URL: https://mtu.edu.ng/mtu/oer/journals/31-EIJMRS3015.pdf (дата звернення: 01.05.2019).

19. Boateng A. A., Boateng G. O., Acquah H. A literature review of fraud risk management in micro finance institutions in Ghana. *Research Journal of Finance and Accounting*. 2014. №5 (11). URL:https://ssrn.com/abstract=2537768 (дата звернення: 01.05.2019).

20. Palfi C., Muresan M. Survey on Weaknesses of Banks Internal Control Systems. *Journal of International Finance and Economics.* 2009. № 9 (1). P. 106-116.

21. Petraşcu D., Tieanu A. The role of internal audit in fraud prevention and detection. *Procedia Economics and Finance.* 2014. № 16. P. 489-497. URL: https://www.sciencedirect.com/science/article/pii/S2212567114008296 (дата звернення: 01.05.2019).

22. Salameh R., Al-Weshah G., Al-Nsour M., Al-Hiyari A. Alternative Internal Audit Structures and Perceived Effectiveness of Internal Audit in Fraud Prevention: Evidence from Jordanian Banking Industry. *Canadian Social Science.* 2011. № 7 (3). P. 40-50. URL: http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=79201535&site=ehost-live (дата звернення: 01.05.2019).

23. Ula M., Ismail Z., Sidek Z. M. A Framework for the governance of information security in banking system. *Journal of Information Assurance & Cyber Security*. 2011. 1-12. URL: https://ibimapublishing.com/articles/JIACS/2011/726196/726196.pdf (дата звернення: 01.05.2019).

24. Usman A. K., Shah, M. H. Critical success factors for preventing e-banking fraud. *The Journal of Internet Banking and Commerce.* 2013. № 18 (2). URL: http://www.icommercecentral.com/open-access/critical-success-factors-for-preventing-ebanking-fraud-1-14.php?aid=38196 (дата звернення: 01.05.2019).

25. Мельниченко О. В. Аудит систем електронних грошей на основі інтегрованої звітності банків. *Бізнес Інформ.* 2013. № 12. С. 301-305.

26. Мельниченко О. В. Аудит договірної роботи та методологічного забезпечення банків з організації обігу електронних грошей. *Вісник*

Житомирського державного технологічного університету. Серія : Економічні науки. 2014. № 2. С. 68-74.

27. Мельниченко О. В. Аудит інформаційної безпеки банку при роботі з електронними грошима. *Проблеми економіки.* 2013. №4. С. 341-347.

28. Мельниченко О. В. Теорія, методологія та практика обліку, аналізу і аудиту електронних грошей в банках: монографія. Житомир ЖДТУ, 2015. 383 с.

29. Мельниченко О.В. Аудит електронних грошей у банках України. *Вісник Національного банку України.* 2013. №3. С. 41-45.

30. Попович О. В., Войновська К.О. Особливості аудиту інформаційної безпеки банку при роботі з електронними грошима. *Формування ринкових відносин в Україні*. 2014. № 12. С. 127-130.

31. Кібальник Л. О., Напора І. Ю. Впровадження політики інформаційної безпеки банківських установ. *Причорноморські економічні студії*. 2016. Вип. 12(2). С. 119-122. URL: http://nbuv.gov.ua/UJRN/bses_2016_12(2)__23 (дата звернення: 01.05.2019).

32. Король О. Г. Аналіз загроз і механізмів забезпечення безпеки інформації в системі електронних платежів комерційного банку України. *Системи обробки інформації*. 2015. Вип. 9. С. 88-95. URL: http://nbuv.gov.ua/UJRN/soi_2015_9_21

33. Щодо організації та функціонування систем ризик-менеджменту в банках України: методичні рекомендації, схвалені Постановою Правління НБУ від 02.08.2004 № 361 [Електронний ресурс]. URL: http://zakon.nau.ua/doc/?uid=1045.5945.1&nobreak=1.

34. Рой Я. В., Мазур Н. П., Складанний П. М. Аудит інформаційної безпеки – основа ефективного захисту підприємства. *Кібербезпека: освіта, наука, техніка*. 2018. № 1. С. 86-93.

35. Practice Guide for Security Risk Assessment & Audit [ISPG-SM01] / Office of the Government Chief Information Officer. URL: https://www.ogcio.gov.hk/en/our_work/information_cyber_security/government/doc/ISPG-SM01.pdf (дата звернення: 01.05.2019).

36. Внутрішній аудит: навчальний посібник / за ред. Ю. Б. Слободяник. Суми :ТОВ «ВПП «Фабрика друку», 2018. 248 с.

37. Хох В. Д., Мелешко Є. В., Смірнов О. А. Дослідження методів аудиту систем управління інформаційною безпекою. *Системи управління, навігації та звязку*. 2017. Вип. 1. С. 38-42.

38. Conteh N.Y., Schmick P.J. Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks. *International Journal of Advanced Computer Research*. 2016. №6. P. 31-38.

39. Scarfone K., A. Souppaya, A.Cody, M. Orebaugh Technical Guide to Information Security Testing and Assessment: Recommendations of the National Institute of Standards and Technology (NIST Special Publication 800-115). Gaithensburg: NIST, 2008. 80 p.

40. Криклій О.А., Павленко Л.Д. Система внутрішнього аудиту як превентивна складова в системі кібербезпеки банку. Облік і фінанси. 2019. № 2 (84). с. 124-133

41. 2018 Report to the nations on occupational fraud and abuse, Association of Certified Fraud Examiners (ACFE). URL: https://s3-us-west-2.amazonaws.com/acfepublic/2018-report-to-the-nations.pdf (дата звернення: 29.11.2019)

42. Спритність рук: топ-схеми шахрайства в банках. *Financial club*. URL: https://finclub.net/ua/priama-mova/sprytnist-ruk-topskhemy-shakhraistva-v-bankakh.html (дата звернення: 29.11.2019)

43. KPMG. Global banking fraud survey. URL: https://assets.kpmg/content/dam/kpmg/xx/pdf/2019/05/global-banking-fraud-survey.pdf (дата звернення: 30.08.2019).

44. Мельник С.С. Сутність фінансового шахрайства в комерційному банку. *Науковий вісник Ужгородського національного університету. Серія «Міжнародні економічні відносини та світове господарство»*. 2016. Випуск 6, частина 2. С. 91-95.

45. Рац О.М. Дослідження особливостей організації фрод-моніторингу в системі управління економічною безпекою банку. *Комунальне господарство міст*. 2016. Випуск 127. С. 33-37.

46. Д'яконова І.І., Павленко Л.Д., Криклій О.А. Сучасний стан та перспективи колаборації банків та FinTech. *Проблеми і перспективи економіки та управління.* 2019. № 1 (17). с.190-200

47. Стандарт ISO/IEC 27001:2013. URL: https://intercert.com.ua/articles/posts/292-standart-iso-iec-27001-2013 (дата звернення: 29.11.2019)

48. Monique Magalhaes. Cybersecurity assessments and audits: everything you need to know. URL: http://techgenix.com/cybersecurity-assessments-and-audits/ (дата звернення: 29.11.2019)

49. Усач Б.Ф., Маркевич М.А. Виявлення фактів шахрайства у контексті аудиту фінансових звітів банків. *Вісник Житомирського державного технологічного університету. Серія «Економічні науки»*. 2010. № 3 (53). С. 253-255.

50. Міжнародні стандарти професійної практики внутрішнього аудиту. URL: https://na.theiia.org/translations/PublicDocuments/IPPF-Standards-2017-Ukrainian.pdf (дата звернення: 29.11.2019)

51. Болгар Т.М. Удосконалення моніторингу банківського кредитного процесу. *Академічний огляд*. 2013. № 2 (39). С. 36-42.

52. Яровенко Г.М. Розробка інформаційної моделі виявлення ознак шахрайства у банках. *Інвестиції: практика та досвід*. 2018. № 14. С. 23-28.

53. Гриценко К.Г. Нечітко-множинний метод оцінки рівня ризику шахрайства банківського персоналу. *Приазовський економічний вісник*. 2019. № 3 (14). С. 451-456. URL: http://pev.kpu.zp.ua/vypusk-14 (дата звернення: 29.11.2019)

54. Мовчан О., Вольська М. Шахрайство, як один з найбільших ризиків, або як не проґавити головну проблему під час проведення внутрішнього аудиту.

URL: https://www.iia.org.ua/wp-content/uploads/2017/04/Fraud-as-one-of-biggest-rist.pdf (дата звернення: 29.11.2019)

55. Гутцайт Е.М. Аудит: концепция, проблемы, эффективность, стандарты. Москва: ЭЛИТ 2000; ЮНИТИ ДАНА. 2002.

56. Jarrod West, Maumita Bhattacharya, Rafigul Islam (2014) Intelligent financial fraud detection practices: an investigation. *Proceedings of the international conference on security and privacy in communication networks*. Volume 153. P. 186-203. DOI: 10.1007/978-3-319-23802-9_16

57. Rinky D. Patel, Dheeraj Kumar Singh (2013) Credit card fraud detection & prevention of fraud using genetic algorithm. *International journal of soft computing and engineering (IJSCE)*. Volume 2, issue 6. P. 292-294.

58. MohdAvesh Zubair Khan, JabirDaud Pathan, Ali Haider Ekbal Ahmed (2014) Credit card fraud detection system using hidden Markov model and k-clustering. *International journal of advanced research in computer and communication engineering*. Volume 3, issue 2. P. 5458-5461.

59. Balamurugan M., Mathiazhagan P. (2015) Credit card transaction fraud detection system using fuzzy logic and k-means algorithm. *International Journal of Innovative Research in Technology*. Volume 2, issue 3. P. 171-176.

61. Гриценко К.Г. (2019) Дослідження особливостей незалежного аудиту для попередження шахрайства банківського персоналу. *Інфраструктура ринку*, Випуск 37. – Режим доступу до ресурсу: http://www.market-infr.od.ua/uk/37-2019

62. Економічна безпека підприємства : навчальний посібник / Небава М. І., Міронова Ю.В. Вінниця : ВНТУ, 2017. 73 с. URL: https://web.posibnyky.vntu.edu.ua/fmib/33nebava_ekonomichna_bezpeka_pidpriyemstva/ekon_bezp_Nebava.pdf (accessed 05 July 2019).

63. Корелин В.В., Габуниа Н.Г. Инструменты обеспечения экономической безопасности промышленного предприятия. *Известия Санкт-Петербургского государственного экономического университета*, *CyberLeninka*;Федеральное государственное бюджетное образовательное

учреждение высшего образования «Санкт-Петербургский государственный экономический университет (СПбГЭУ)» №4 (100). 2016. С.114-116.

64. Лук'янова В.В., Головач Т.В. Економічний ризик: Навч. посіб. Київ: Академвидав, 2007. 464 с.

65. Мандзіновська Х.О. Економічна безпека держави: сутність, складові елементи та проблеми забезпечення: наукові записки. 2(53). 2016. С.159-166.

66. Підхомний О. Фінансова безпека України: інструменти і стратегії формування : монографія. Львів : ЛНУ імені Івана Франка, 2014. 320 с.

67. Іващенко Г. А. Ідентифікація дефініції «економічна безпека підприємства»/ Г. А. Іващенко, О. Ф. Ярошенко. *Науковий журнал «Бізнес Інформ»*.№9, Харків, 2011. С. 129 – 131.

68. Кавун С.В. Економічна та інформаційна безпека підприємств у системі консолідації інформації. Навчальний посібник / С.В. Кавун, А.А.Пилипенко, Д.О. Репко. Харків: Вид. ХНЕУ, 2013. 264 с.

69. Прокопішина О. В. Управління економічною безпекою зовнішньоекономічної діяльності підприємства: автореф. дис. на здобуття наук, ступеня канд. екон. наук : спец. 08.00.04 «Економіка та управління підприємствами». Харківський національний економічний ун-т . Харків, 2009. 20 с

70. Василишин Т.С. Фінансова безпека: сутність і місце в системі економічної безпеки держави. *Соціально-економічний розвиток і безпека України: стан та перспективи:* матеріали міжвузівської науково-практичної конференції здобувачів вищої освіти і молодих вчених, м. Львів, 19 квітня 2018 р. / за заг. ред. Я.Я. Пушака. Львів: Ліга-Прес, 2018. С.53-55.

71. Куришко О.О. Національна система фінансового моніторингу в Україні : дис. ... канд. екон. наук : 08.00.08 / Куришко Олександр ISSN 1994-1749. 2015. Вип. 2 (32). *Проблеми теорії таметодології бухгалтерського обліку, контролю і аналізу*. Національний банк України, Державний вищий навчальний заклад «Українська академія банківської справи Національного банку України» ; наук. кер. Леонов С.В. Суми, 2013. 256 с.

72. Новак О.С., Дідківська Н.І. Роль фінансового моніторингу у забезпеченні фінансової безпеки держави. *Ефективна економіка* № 12. 2016. URL: http://www.economy.nayka.com.ua/?op=1&z=5511 (accessed 29 July 2019).

73. Петрук О.М. Зарубіжний досвід організації фінансового моніторингу та перспективи його впровадження в Україні / О.М. Петрук, О.В. Смагло. *European cooperation scientific approaches and applied technologies.* 2015. № 2 (2). P. 89–99.

74. Практичне застосування Байєсівського аналізу при здійсненні фінансового моніторингу в банках: монографія/ О.В. Кузьменко, Т.А. Медвідь, Л.Г. Левченко та ін.; за заг. ред. С.О. Дмитрова. Суми: ДВНЗ УАБС НБУ, 2011. 46 с.

75. Зеленецький В. С. Боротьба з легалізацією (відмиванням) доходів, одержаних злочинним шляхом, та фінансуванням тероризму (економікоправовий аналіз) : наук.-практ . посібник / В. С. Зеленецький, В. Л. Кротюк, Д. А. Файєр. Х. : Вид-во «Кросроуд», 2007. 668 с.

76. Schneider F. The (Hidden) Financial Flows of Terrorist and Organized Crime Organizations: A Literature Review and Some Preliminary Empirical Results. 2010. №4860. URL: http://ftp.iza.org/dp4860.pdf (accessed 29 July 2019).

77. Протидія легалізації злочинних доходів і фінансуванню тероризму /С. Г. Гуржій, С. М. Клюшке, В. М. Кірсанов та ін. *Держ. ком. фін.моніторингу України*. Київ : Такі справи, 2008. 560 с.

78. Небава М. І. Інституціоналізація тіньової економічної діяльності як загроза економічній безпеці України. *Тіньова економіка: генезис,джерела розвитку, перспективи подолання та цивілізаційної інтеграції*:Матеріали І Міжнародної науково-практичної конференції. (Вінниця, 23-24травня 2013 р.). Вінниця: НВЦ «Генеза», 2013. С. 139-143.

79. Кузьменко О.В., Доценко Т.В., Скринька Л.О. Роль фінансового моніторингу в сучасній системі забезпечення економічної безпеки національної економіки. *Науковий погляд: економіка та управління*. 2019. №3(65). с. 98 - 108.

80. Гриценко К.Г. Аналіз методів виявлення шахрайств у банках, що здійснюються персоналом банку. *Інфраструктура ринку*. 2019. Випуск 34. С. 333-337. – Режим доступу до ресурсу: http://www.market-infr.od.ua/uk/34-2019.

81. OECD science, technology, and industry scoreboard: Towards a knowledge-based economy. Organisation for Economic Cooperation and Development. http://www.oecd.org/(2001). Режим доступу 13 березня 2019

82. Babenko, V., Syniavska, O.: Analysis of the current state of development of electronic commerce market in Ukraine. Tech. Aud. and Prod. Res. 5, 40-45 (2018). doi: 10.15587/2312-8372.2018.146341

83. Mia, A., Rahman, M., Uddin, M.: E-Banking: Evolution, Status and Prospects. Cost & Manag. 1(35), 36-48 (2007)

84. The Statistical Portal. https://www.statista.com/ (2019). Accessed 13 Mar 2019

85. Lastdrager, E.: Achieving a consensual definition of phishing based on a systematic review of the literature. Cr. Sc. 3, 9 (2014). doi: 10.1186/s40163-014-0009-y

86. Jakobsson, M., Myers, S. (ed.) Phishing and countermeasures: understanding the increasing problem of electronic identity theft. John Wiley & Sons, Inc. (2007)

87. J. Shi, S. Saleem.: Phishing: Final Report. https://www2.cs.arizona.edu/~collberg/Teaching/466-566/2014/Resources/presentations/2012/topic5-final/report.pdf (2012). Accessed 9 Mar 2019

88. Swanink, R.: Persistent effects of manin-the-middle attacks. Bachelor Thesis, Radboud University (2016)

89. Damodaram, R.: Study on phishing attacks and antiphishing tools. IRJET, 3(1), 700-705 (2016)

90. Alsayed, A., Bilgrami, A.: E-banking security: Internet hacking, phishing attacks, analysis and prevention of fraudulent activities. Int. J. Of Emerg. Techn. and Adv. Activ. 7(1), 109-115 (2017)

91. Delgado, O., Fuster-Sabater, A., Sierra, J.: Analysis of new threats to online banking authentication schemes. https://core.ac.uk/download/pdf/36021441.pdf (2008). Accessed 10 Mar 2019

92. Oliinyk, V., Wiebe, I., Syniavska O., Yatsenko, V.: Optimization model of Bass. JAES, 8(62), 2168 – 2183 (2018)

93. Gupta, R.: Dynamics of a Holling-Tanner Model. AJER, 6(4), 132-140 (2017)

94. Syniavska, O., Dekhtyar, N., Deyneka, O., Zhukova, T., Syniavska O.: Security of e-banking systems: modelling the process of counteracting e-banking fraud. SHS Web of Conf. 65 (2019). DOI: https://doi.org/10.1051/shsconf/20196503004

95. Kuznetsov, A., Shapoval, O., Chernov, K., Yeromin, Y., Popova, M., Syniavska, O. (2019). Automated Software Vulnerability Testing Using In-Depth Training Methods. CEUR Workshop Proceedings, Vol. 2353: 227-240.

96. A-Z of internal banking fraud. URL: https://netguardians.ch/internal-banking-fraud/ (дата звернення: 07.06.2019).

97. Christie L. Comunale, Rebecca L. Rosner, Thomas R. Sexton. The Auditor's Assessment of Fraud Risk: A Fuzzy Logic Approach. Journal of Forensic & Investigative Accounting. Vol. 2, Issue 3, Special Issue, 2010. P.95-140.

98. Statement on Auditing Standards No. 99: Consideration of Fraud in a Financial Statement Audit. URL: https://www.aicpa.org/research/standards/auditattest/downloadabledocuments/au-00316.pdf (дата звернення: 07.06.2019)

99. Пономаренко В.С., Малярець Л.М. Багатовимірний аналіз соціально-економічних систем: [навчальний посібник]. Харків: ХНЕУ, 2009. 384 с.

100. Недосекин А.О. Оценка риска бизнеса на основе нечетких данных: [монография]. Санкт-Петербург, 2004. 100 с.

101. Вітлінський В.В., Великоіваненко Г.І. Ризикологія в економіці та підприємництві: [монографія]. Київ: КНЕУ, 2004. 480 с.

102. Гриценко К.Г. Використання теорії нечітких множин для оцінювання рівня захищеності банківської установи від кібершахрайств. *Приазовський*

економічний вісник. 2019. №1(12). С. 214-219. URL: http://pev.kpu.zp.ua/vypusk-12.

103. Гриценко К.Г. Нечітко-множинна ієрархічна модель оцінювання рівня ризику шахрайства банківського персоналу // Проблеми та перспективи розвитку фінансово-кредитної системи України: збірник матеріалів IV Всеукраїнської науково-практичної on-line конференції (21-22 листопада 2019 року) / Навчально-науковий інститут бізнес-технологій «УАБС» Сумського державного університету. – Суми : ННІ БТ «УАБС» СумДУ, 2019.

104. Lyeonov, S., Kuzmenko, O., Yarovenko, H. & Dotsenko, T. (2019). The Innovative Approach to Increasing Cybersecurity of Transactions Through Counteraction to Money Laundering. Marketing and Management of Innovations, 3, 308-326. http://doi.org/10.21272/mmi.2019.3-24

105. World Bank Open Data. Available online: https://data.worldbank.org (accessed on 30 December 2018).

106. Organisation for Economic Co-operation and Development. Available online: https://data.oecd.org/?_ga=2.69359696.157983792.1546455347-1152323357.1544691649 (accessed on 30 December 2018).

107. Transparency International. Available online: https://www.transparency.org/news/feature/corruption_perceptions_index_2017?gclid=EAIaIQobChMIusejy-PP3wIVVIuyCh0NdwBEEAAYASAAEgIyc_D_BwE (accessed on 30 December 2018).

108. Institute for economics & peace. Available online: http://visionofhumanity.org/app/uploads/2017/11/Global-Terrorism-Index-2017.pdf (accessed on 30 December 2018).

109. Happy Planet Index. Available online: http://happyplanetindex.org (accessed on 30 December 2018).

110. Pham D.T., Packianather M.S., Afify A.A. (2007) Artificial Neural Networks. In: Andina D., Pham D.T. (eds) Computational Intelligence. Springer, Boston, MA DOIhttps://doi.org/10.1007/0-387-37452-3_3

111. Michael J. D. Powell; Michael J. D. Powell. Restart procedures for the conjugate gradient method (англ.) // Mathematical Programming (англ.)русск. : journal. — Springer, 1977. — Vol. 12. — P. 241—254. — DOI:10.1007/bf01593790.

112. Broomhead, David H.; Lowe, David. Multivariable Functional Interpolation and Adaptive Networks (англ.) // Complex Systems : journal. — 1988. — Vol. 2. — P. 321—355.

113. Метод Бройдена–Флетчера–Гольдфарба–Шанно https://math.semestr.ru/optim/broyden.php

114. Kuzmenko O., Boiko A., Yarovenko H., Dotsenko T. (2019) Data mining-based assesselement of the risk of using financial intermediaries for money laundering. *Ефективна економіка*. 10. DOI: 10.32702/2307-2105.2019.1

115. Яровенко Г.М., Онопко Ю.Д. Моделювання бізнес-процесів автоматизованого внутрішнього аудиту діяльності працівників банку. Proceedings of the 1st International Scientific and Practical Conference «Scientific Research in XXI Century» (December 16-18, 2019). Ottawa, Canada: Methuen Publishing House, 2019. pp. 73-75

116. The State Financial Monitoring Service. URL: http://www.sdfm.gov.ua/index.php?lang=en. (дата звернення: 03.12.2019).

117. About the business process model and notation specification version 2.0 // Object Management Group Business Process Model and Notation. 2011. URL: https://www.omg.org/spec/BPMN/2.0/ (дата звернення: 03.12.2019).

118. Bizagi Studio – the most business-friendly and flexible process automation software // Bizagi. URL: https://www.bizagi.com/en/products/bpm-suite/studio. (дата звернення: 03.12.2019).

119. BPM Microsystems company. URL: https://bpmmicro.com/support/software/downloads/. (дата звернення: 03.12.2019).

120. Leonov S., Yarovenko H., Boiko A., Dotsenko T. Information system for monitoring banking transactions related to money laundering. *CEUR Workshop Proceedings*. 2019. Vol. 2422. P. 297-307.

121. Leonov S., Yarovenko H., Boiko A., Dotsenko T. Prototyping of information system for monitoring banking transactions related to money laundering. *The 8th International Conference on Monitoring, Modeling & Management of Emergent Economy (M3E2 2019). - SHS Web Conf.* 2019. Vol. 65. DOI: https://doi.org/10.1051/shsconf/20196504013

122. Bilan Y., Vasylieva T., Lyeonov S., Tiutiunyk I. Shadow economy and its impact on demand at the investment market of the country. *Entrepreneurial Business and Economics Review*. 2019. Volume 7. Issue 2. Pages 27-43.

123. Яровенко Г.М., Бойко А.О., Доценко Т.В. Розробка інформаційної системи моніторингу банківських операцій, пов'язаних із легалізацією незаконних коштів. *Економіка, фінанси, облік та право: стратегічні пріоритети розвитку в умовах глобалізації : збірник тез доповідей міжнародної науково-практичної конференції (Полтава, 20.04.19).* Полтава: ЦФЕНД, 2019. С. 55-57

124. Кузьменко, О. В., Овчаренко В. О. Тенденції розвитку сучасних банківських технологій. *Науковий вісник Ужгородського національного університету : серія: Міжнародні економічні відносини та світове господарство.* 2019. Вип. 24, №Ч.2. С. 98–103.

125. Кузьменко О. В., Касаєва Ю. В. Дослідження ролі інформаційних технологій у забезпеченні інвестиційної привабливості та соціально-економічного розвитку країни. *Інвестиції: практика та досвід.* 2019. № 16. С. 5–15. DOI: 10.32702/2306-6814.2019.16.5

126. Кузьменко О.В., Бойко А.О., Яровенко Г.М., Доценко Т.В. Інтелектуальний аналіз як механізм виявлення схемних операцій в Україні. *Scientific discoveries: projects, strategies and development: Collection of scientific papers «ΛΌГОΣ» with Proceedings of the International Scientific and Practical Conference (Vol. 1), October 25, 2019.* Edinburgh, UK: European Scientific Platform. P. 29-31. DOI: https://doi.org/10.36074/25.10.2019.v1.04

127. Яровенко Г.М., Нечепоренко І.Д. Сучасні технології кіберзахисту щодо виявлення шахрайств, які здійснюються персоналом банку. *Проблеми та*

перспективи розвитку фінансово-кредитної системи України : збірник матеріалів IV Всеукраїнської науково-практичної on-line конференції : у 2 ч. (м. Суми, 21–22 листопада 2019 року) / Навчально-науковий інститут бізнес-технологій «УАБС» Сумського державного університету. Суми : Сумський державний університет, 2019. Ч. 2. С. 149-153.