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
cyber@uabs.sumdu.edu.ua

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

(остаточний)

Керівник НДР
д-р. екон. наук, професор О.В. Кузьменко

2020

Рукопис закінчений 23 грудня 2020 р.

Результати цієї роботи розглянуті науковою радою СумДУ, протокол від 23 грудня 2020 р. № 6

СПИСОК АВТОРІВ

Зав. кафедри економічної кібернетики, д-р екон. наук, професор (керівник)	23.12.2020	О.В. Кузьменко (вступ, підрозділи 1.3.1, 1.3.2, 1.4.1, 2.1.3, 2.2.3, 3.2, 3.4.1, 3.4.2, висновки)
Доцент кафедри економічної кібернетики, канд. екон. наук, доцент (відповідальний виконавець)	23.12.2020	Г.М. Яровенко (підрозділи 1.2.1, 1.2.2, 1.2.3, 1.4.1, 1.4.2, 1.4.3, 2.2.3, 2.3.1, 2.3.2, 3.1.1, 3.1.2, 3.1.3)
Професор кафедри економічної кібернетики, д-р екон. наук, професор	23.12.2020	С.В. Лєонов (підрозділи 1.1.1, 1.1.2, 1.4.2, 2.3.2)
Доцент кафедри банківської справи, фінансів та страхування, канд. екон. наук, доцент	23.12.2020	О.А. Криклій (підрозділ 1.3.3, 2.1.1, 3.3.2)
Доцент кафедри економічної кібернетики, канд. техн. наук, доцент	23.12.2020	К.Г. Гриценко (підрозділи 2.1.2, 2.2.2, 3.3.1)
Доцент кафедри економічної кібернетики, канд. екон. наук	23.12.2020	А.О. Бойко (підрозділи 2.2.3, 2.3.2)
Ст.викл. кафедри економічної кібернетики, канд. екон. наук	23.12.2020	О.О. Пушко (підрозділ 1.1.2, 1.1.3, 2.2.1)
Аспірант кафедри економічної кібернетики	23.12.2020	Т.В. Доценко (підрозділи 1.3.1, 1.3.2, 1.4.2, 2.1.3, 2.2.3, 2.3.2, 3.2, 3.4.1, 3.4.2)
Аспірант кафедри економічної кібернетики	23.12.2020	О.С. Кушнєрьов (підрозділ 3.4.1)

Аспірант кафедри економічної кібернетики	23.12.2020	В.О. Ковач (підрозділ 1.2.2)
Магістр-випускник кафедри економічної кібернетики	23.12.2020	М.М. Бояджян (підрозділи 1.2.1, 1.4.1)
Магістр-випускник кафедри економічної кібернетики	23.12.2020	С.В. Клімов (підрозділ 1.4.3)
Бакалавр-випускник кафедри економічної кібернетики	23.12.2020	Ю.Д. Онопко (підрозділ 2.3.1)

РЕФЕРАТ

Звіт про НДР: 498 с., 145 рис., 72 табл., 120 формул, 330 джерел, 7 додатків.

БАНК, КІБЕРБЕЗПЕКА, КІБЕРЗАГРОЗА, КІБЕРШАХРАЙСТВО, ІНТЕЛЕКТУАЛЬНИЙ АНАЛІЗ, КОМП'ЮТЕРНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ, МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ, МОНІТОРИНГ.

Об'єкт дослідження – система інформаційних зв'язків та фінансово-економічних відносин між економічними суб'єктами в процесі руху грошових коштів через банківську систему, що супроводжується застосуванням сучасних інформаційних технологій.

Мета роботи – розвиток методології та міждисциплінарного методичного інструментарію боротьби з кіберзлочинами в банківській сфері, обґрунтування та розробка організаційно-інституційних засад забезпечення стійкості фінансового кіберпростору на внутрішньобанківському та державному рівнях для забезпечення економічної безпеки держави та захисту прав споживачів фінансових послуг.

Методи дослідження – системний підхід, діалектичний метод наукового пізнання, фундаментальні положення банківської справи, сучасні математичні методи, моделі та інформаційні технології в банківській сфері, сучасні концепції кібербезпеки, законодавчі та нормативні документи Національного банку України, інструкції банків, наукові праці вітчизняних та зарубіжних фахівців.

Досліджено види кіберзагроз, шахрайств, причин їх виникнення; розроблено математичні моделі ймовірності виникнення шахрайських операцій в банках; здійснено оцінку рівня втрат банків від шахрайських операцій; розроблено комплекс превентивних заходів для попередження кібер-загроз та шахрайств; проведено моделювання бізнес-процесів служби аудиту банку; розроблено алгоритми виявлення та попередження шахрайств в банках, які здійснюються із зовнішніх джерел; розроблено алгоритми виявлення та попередження шахрайств в банках, що здійснюються персоналом банку; визначено напрям розвитку кіберпростору як складової інформаційної безпеки на загальнодержавному рівні; визначено кількісний та якісний рівні ефективності роботи внутрішньобанківської системи кібербезпеки; розроблено методологічне підґрунтя підвищення ефективності організації системи кіберзахисту в банках та концепції реформування фінансового кіберпростору.

ЗМІСТ

ВСТУП

В сучасних умовах цифровізації економіки, стійкого розвитку комп'ютерних та інформаційних технологій, банкоцентричності фінансового ринку, великої концентрації грошей, різноманітності on-line послуг банківська діяльність не лише робить банки привабливими для кіберзлочинців та призводить до «інтелектуалізації» банківських шахрайств, але й виступає об'єктом тих фінансових шахрайств, які здійснюються як зовнішніми по відношенню до банку шахраями, так і внутрішніми, в якості яких виступає керівництво та персонал банку. Все це значно знижує довіру до фінансових інституцій, зменшує обсяги ресурсів в економіці, негативно впливає на фінансово-економічну безпеку України та її імідж надійного фінансового партнера в євроінтеграційних процесах. Поєднання в межах даного проекту наукового потенціалу дослідників з різних сфер (ІТ-аналітика, кібернетика, економіко-математичне моделювання, фінанси, банківська справа) відкриває нові можливості для її міждисциплінарного вирішення на системному рівні.

Світовою та вітчизняною науковою спільнотою напрацьовано значний інструментарій по застосуванню методів кібербезпеки для постфактум-реагування на виникнення шахрайств в банках. Даний проект враховує існуючі напрацювання, але спрямований на вирішення проблеми ранньої діагностики потенційних джерел кібершахрайських операцій, оцінки їх ймовірності, організації незалежного моніторингу дій банківського персоналу та формування організаційно-інституційного забезпечення стійкості фінансового кіберпростору на загальнодержавному рівні, що сприятиме підвищенню рівня захисту споживачів та зменшенню втрат національної економіки.

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.

Враховуючи останні тенденції, банки зобов'язані інвестувати значною мірою в модернізацію системи кіберзахисту шляхом придбання або створення сучасних систем виявлення та попередження шахрайств, які врешті-решт також можуть виявитися неефективними. Тому для боротьби із шахрайствами банки повинні підходити послідовно та системно. По-перше, необхідна чітка регламентація дій персоналу щодо доступу до даних, що дозволить уникнути фактів його доступу до персональної інформації клієнтів та відповідно викрадення її. По-друге, вводити стратегії, які включають проведення тренінгів з обізнаності про шахрайство, роз’яснення серед населення через засоби масової

інформації та Інтернет, оцінку ризиків шахрайства та безперервний моніторинг. По-третє, удосконалити програмне та інформаційне забезпечення автоматизованої банківської системи з урахуванням інтелектуальних алгоритмів обробки, що дозволить на етапі здійснення шахрайства ідентифікувати шахрая та жертву, попередити здійснення такої операції та виявити злочинця.

Окреслена проблема дозволила обрати об'єкт та предмет дослідження. Об'єкт дослідження – система інформаційних зв'язків та фінансово-економічних відносин між економічними суб'єктами, банківськими установами, а також всередині банку в процесі руху грошових коштів через банківську систему, що супроводжується застосуванням сучасних інформаційних технологій.

Предмет дослідження – методологічні, методичні, організаційні, економіко-математичні та інформаційно-технологічні підходи до побудови ефективної системи боротьби з банківськими кіберзлочинами на мікрорівні (банки) та макрорівні (забезпечення стійкості загальнодержавного фінансового кіберпростору), 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 боротьби з кіберзлочинами в банківській сфері, системи внутрішнього аудиту та моніторингу для боротьби з кібершахрайствами в банківській сфері, як превентивної структури в системі кібербезпеки банку, обґрунтування та розробка організаційно-інституційних засад забезпечення стійкості фінансового кіберпростору на внутрішньобанківському та державному рівнях для забезпечення економічної безпеки держави та захисту прав споживачів фінансових послуг.

Для реалізації поставленої мети необхідно було вирішити наступні завдання:

- проаналізувати кіберзагрози як об'єкт моделювання;
- здійснити первинний та кластерний аналіз кібершахрайств;

- розробити математичні моделі ймовірності виникнення ознак кібершахрайських операцій із використанням Data Mining;
- розробити інформаційні моделі виявлення ознак шахрайства з боку зовнішніх та внутрішніх шахраїв;
- розробити математичні портрети потенційних жертв та шахраїв;
- провести кількісний аналіз збитків банківської системи в результаті кібершахрайств;
- змоделювати кількісну оцінку рівня операційного ризику банку в сфері інформаційної безпеки;
- розробити модель впливу макроекономічних факторів на формування схильності до шахрайства в банківській сфері;
- розробити гравітаційну модель оцінки привабливості країни для легалізації кримінальних доходів;
- створити прототип автоматизованого модулю процесу виявлення шахрайських операцій з банківськими картками.
- 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;
- розробити фронтірну модель оцінювання ефективності роботи внутрішньобанківської системи кібербезпеки;
- розробити заходи удосконалення автоматизованого фінансового моніторингу банку, як інструменту системи кібербезпеки;
- провести оцінку ефективності інвестицій в банківські продукти кіберзахисту;
- розробити методичний підхід для оцінки рівня стійкості фінансового кіберпростору на загальнодержавному рівні;
- провести оцінку ризиків соціо-економіко-політичної стабільності;
- провести оцінку інтегрального індексу загрози економіки та інформаційної безпеки;
- розробити методичний підхід для формалізації інтегральної міри оцінки фінансової безпеки України;
- розробити стратегічні напрями формування інвестиційного потенціалу в Україні на основі ефективного розвитку інформаційних технологій;
- дослідити особливості та перспективи застосування технології блокчейн в системах забезпечення кібербезпеки банків;
- розробити науково-методичне підґрунтя для подальшого формування нормативно-правових актів та внутрішньобанківських інструкцій щодо організації системи кіберзахисту;
- розробити систему заходів удосконалення державного регулювання економічної безпеки національної економіки;
- розробити шляхи забезпечення стійкості фінансового кіберпростору;
- провести ігромоделювання стратегій державного регулювання економічної безпеки національної економіки;
- розробити програму реформування внутрішньобанківської системи кібербезпеки;

- розробити моделі механізму забезпечення та підвищення стійкості системи кіберстійкості банків на сучасному етапі розвитку цифрової економіки країни;
- побудувати фронтірну модель оптимізації ефективності внутрішньобанківської ALM-системи;
- розробити методичні засади реформування внутрішньо-банківської ALM-системи системи;
- провести рейтингування країн за рівнем кібербезпеки та ефективності системи інформаційної безпеки країни.

Методи дослідження – системний підхід, діалектичний метод наукового пізнання, фундаментальні положення банківської справи, моніторингу та аудиту, сучасні математичні методи та моделі (нечітко-множинне моделювання, динамічне моделювання, нейронно-мережеве моделювання та програмування, сучасні концепції моделювання бізнес-процесів, фронтірний DEA-аналіз, ігромоделювання), в також інформаційні технології в банківській сфері, сучасні концепції кібербезпеки, законодавчі та нормативні документи Національного банку України, інструкції банків, наукові праці вітчизняних та зарубіжних фахівців.

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»; АТ “ОТП Банк” в м. Суми; відділення «Сумське» ПАТ «Альфа-Банк»; ФОП «Мартиненко ВМ», ТОВ Видавництво-газета «Ярославна». Одержані у роботі результати можуть бути використані в діяльності Національного банку України щодо створення методологічного інструментарію виявлення та попередження кіберзагроз та організації стратегічної роботи Департаментів кібербезпеки банків. Виконавцями проекту отримано один міжнародний індивідуальний грант. Результати впроваджено у навчальний процес при викладанні дисциплін «Інтелектуальний

аналіз даних», «Інформаційні системи і технології в банківській сфері», «Бізнес-аналітика та прийняття рішень», «Прогнозування соціально-економічних процесів», «Моделювання бізнес-процесів», «Платіжні системи», «Прикладні задачі моделювання економічних процесів», «Інформаційні системи у фінансах», «Інформаційні системи і технології в управлінні», «Моделювання емерджентної економіки», «Моделювання в управління соціально-економічними системами», «Оцінювання та аналіз ризику», «Кількісні методи в економіці».

За результатами НДР опубліковано: 12 статей у журналах, що індексується у БД Scopus, та 8 у БД WoS; 12 – монографії та розділи у монографіях у закордонних виданнях англійською мовою та 9 - монографії та розділи монографій українською мовою, 2 навчальні посібники, 42 фахові статті у виданнях України, прийнято участь у роботі 30 науково-практичних конференцій, захищено 3 докторські дисертації та запланований у грудні захист 2 кандидатських дисертацій; 6 свідоцтв про реєстрацію авторського права на твір; дипломом І ступеня за напрямком «Економічна аналітика і статистика» та диплом ІІІ ступеня за напрямом «Економічна кібернетика» у Всеукраїнському конкурсі студентських наукових робіт; грант Президента України для підтримки наукових досліджень молодих учених.

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

1 МОДЕЛЮВАННЯ ЙМОВІРНОСТІ ВИНИКНЕННЯ ШАХРАЙСЬКИХ ОПЕРАЦІЙ В БАНКАХ

1.1 Дослідження видів кіберзагроз, шахрайств, та причин, які обумовлюють їх появлення

1.1.1 Аналіз кіберзагроз як об’єкту моделювання

Щоденна діяльність банківських систем тісно пов’язана з використанням сучасних комп’ютерних технологій і перебуває в повній залежності від надійної та безперебійної роботи електронно-обчислювальних систем. Світовий досвід свідчить про безумовну уразливість будь-якої компанії з огляду на те, що кіберзлочини не мають державних кордонів, у зв’язку з чим хакери мають можливість в рівній мірі загрожувати інформаційним системам в будь-якій точці світу [1].

Кібернетична загроза (кіберзагроза) – наявні й потенційно можливі явища та чинники, що створюють небезпеку інтересам людини, суспільства й держави через порушення доступності, повноти, цілісності, достовірності, автентичності режиму доступу до інформації, яка циркулює в критичних об’єктах національної інформаційної інфраструктури [2].

Основоположні причини виникнення кіберзагроз полягають в:

– відсутності необхідного законодавства і єдиних стандартів безпеки;

– недостатності фінансування з боку самих банків;

– відсутності корпоративної культури в сфері кібербезпеки всередині банку [1].

Розглянемо найпоширеніші кіберзагрози в банках:

а) атаки мережевого та прикладного рівнів:

1) розрив або призупинення серверів та мережевих ресурсів, підключених до Інтернету;

2) легка атака для будь-кого для запуску, дуже важко для банків вирішити самостійно;

3) пакети атак DDoS легко доступні будь-кому на чорному ринку;

4) атаки DDoS можуть запускатися кіберзлочинцями, щоб відвернути банківський персонал від помітних шахрайських операцій, таких як несанкціоновані перекази коштів;

б) соціальна інженерія:

1) банківські клієнти часто натрапляють на фішингові атаки;

2) банківські клієнти отримують підроблені електронні листи, які використовуються для отримання доступу до їх рахунків або отримання особистої інформації;

3) підроблені електронні листи ретельно створюються, щоб відобразити справжні листи, які зазвичай надсилаються банками.

4) важко виявити, оскільки джерело електронної пошти часто виявляється законним.

в) розвинені стійкі загрози:

1) «Backdoor» для систем встановлюється за допомогою вразливостей («Backdoor» - вразливість в програмі, що дозволяє хакерам зламати систему або здійснити будь-яку недружелюбну дію);

2) за допомогою належного шкідливого коду нападники залишаються непоміченими, щоб як можна довше продовжувати наносити збитки;

г) організована кіберзлочинність:

1) ризик розкрадання інтелектуальної власності, конфіскація банківських рахунків та втрата споживачів внаслідок бізнес-збоїв;

2) в кінцевому рахунку, легше запобігти, ніж усунути, кібер-злочинці спеціалізуються на продажі особистої інформації на чорному ринку, використовуючи викуп та шантаж;

д) порушення основних даних:

1) високоорганізовані хакери, які використовують надійну інфраструктуру для цільових банківських установ, викрадають дані клієнтів та продають їх;

2) за допомогою різних методів розкривається конфіденційна

інформація про банківські установи та їх клієнтів;

3) бізнес порушується, дані про клієнтів та компанії погіршуються, а витрати на відновлення є величезними [3].

DoS (від англ. Denial of Service – відмова в обслуговуванні) – хакерська атака на обчислювальну систему з метою довести її до відмови, тобто створення таких умов, при яких сумлінні користувачі системи не можуть отримати доступ до надаваних системних ресурсів (серверів), або цей доступ ускладнений. Відмова «ворожої» системи може бути і кроком до оволодіння системою. Але частіше – це міра економічного тиску: втрата звичайної служби, що приносить дохід, рахунки від провайдера і заходи по відходу від атаки відчутно б'ють «ціль» по кишені. В даний час DoS і DDoS-атаки найбільш популярні, оскільки дозволяють призвести до відмови практично будь-яку систему, не залишаючи юридично значимих доказів [4].

Якщо атака виконується одночасно з великої кількості комп'ютерів, то говорять про DDoS-атаку (від англ. Distributed Denial of Service, розподілена атака типу «відмова в обслуговуванні»). Така атака проводиться в тому випадку, якщо потрібно викликати відмову в обслуговуванні добре захищеної крупної компанії чи державної організації [5].

DDoS – широкомасштабна координована атака на надання послуг системи жертви або мережевих ресурсів, яка побічно запускається через велику кількість комп'ютерних агентів, що потрапили в Інтернет. Перед застосуванням атаки зловмисник приймає велику кількість комп'ютерних машин під його управлінням через Інтернет, і ці комп'ютери є вразливими машинами. Зловмисник використовує недоліки цих комп'ютерів, вставляючи шкідливий код або іншу техніку хакерства, щоб вони стали під його контролем. Ці вразливі або скомпрометовані машини можуть складати сотні або тисячі осіб, і їх зазвичай називають «зомбі». Група зомбі зазвичай формує «ботнет». Величина атаки залежить від розміру ботнету, для більшого ботнету, атаки є більш серйозними і катастрофічними [6].

Раніше корпоративні комп’ютери часто атакували вірусні програми, які підміняли платіжні доручення, коли бухгалтер намагався провести транзакції, і забирали гроші на підроблені рахунки. Зараз такі програми практично відсутні, але методи шахраїв стали ще більш витонченими. Все частіше стали зустрічатися випадки, коли бухгалтер вставляє спеціальний ключ для доступу до банку, вводить всі паролі, починає проводити транзакцію, а на комп’ютері з’являється картинка, що імітує перезавантаження (програмний код). Насправді за цією картинкою зловмисники використовують вже підготовлену бухгалтером транзакцію для того, щоб перевести гроші на свої рахунки.

Часто злочинці навіть не використовують спеціальні шкідливі програми, обходячись стандартними засобами для віддаленого управління операційною системою, і без всяких картинок підключаються до комп’ютера і переводять гроші. Коли пропажа виявляється, а на комп’ютері немає ніяких вірусів, природно, під підозру відразу потрапляє сам бухгалтер.

Широке поширення отримали програми-вимагачі, які шифрують всі документи на комп’ютері: платіжні доручення, бази даних, звітність, всю документацію, – а для повернення доступу до даних вимагають перерахувати гроші. З корпоративних користувачів вимагають перевести до декількох тисяч доларів або їх еквівалент в біткоінах.

Фішинг – це спосіб, при якому шахрай може отримати інформацію, не маючи жодного контакту з картою. Вся інформація найчастіше викрадається через Інтернет. У власників можуть вкрасти номер карти, термін дії, ПІН-код та CVV/CVC-код. Отримавши всю необхідну інформацію, шахраї з легкістю крадуть гроші з карт. Найбільш поширеним способом фішингу є відправка електронних листів, в яких міститься посилання. Перейшовши по такому посиланню, людина потрапляє на сайт, який нагадує сайт банківської установи, причому його адресу може відрізнятися від справжнього сайту банку на одну або кілька букв. Неуважний користувач може не помітити підміни і подумати, що це офіційний сайт, надавши йому всю конфіденційну інформацію з карти [7].

Представимо наочно масштаби кібернетичних загроз у банківській системі світу ґрунтуючись на Звіті про тенденції «Фінансові кібернетичні загрози першого кварталу 2017 року», який був розроблений Лабораторією Касперського та компанією Telefónica [8]. В звіті використовуються дані Kaspersky Security Network (KSN) – глобального сервісу оперативної реакції на загрози. Коли програма виявляє підозрілі або неперевірені дані на комп'ютері учасника KSN – ці дані автоматично відправляються в вірусну лабораторію Kaspersky. Часовий інтервал для проведеного аналізу містить дані, отримані в період з 1 січня 2017 року по 31 березня 2017 року.

Станом на кінець першого кварталу 2017 року найбільшої шкоди від фішингових атак зазнають банки – 51,70% (рисунок 1.1).

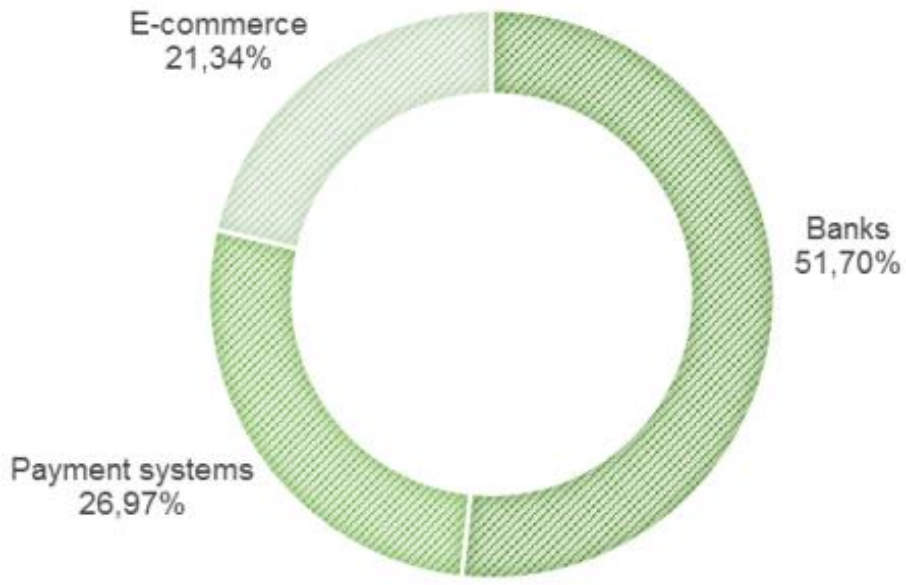


Рисунок 1.1 – Цільовий розподіл фішингу у фінансовому секторі

Так, кількість фішингових атак у фінансовій сфері, зареєстрованих Лабораторією Касперського, скоротилася на 7,1% порівняно з попереднім кварталом; зменшення частки нападів на банківські установи склало -2,53%. Як і в попередньому періоді, найбільше від фішингу страждають користувачі в Китаї та Бразилії. За ними слідують жителі Макао, Російської Федерації та Австралії.

Наведена нижче карта показує країни з найбільшим відсотком кількості користувачів, які стали жертвами фішингових атак (відношення атакованих користувачів до загальної кількості користувачів KSN у країні, на пристроях із включеними компонентами захисту від фішингу) (рис. 1.2).

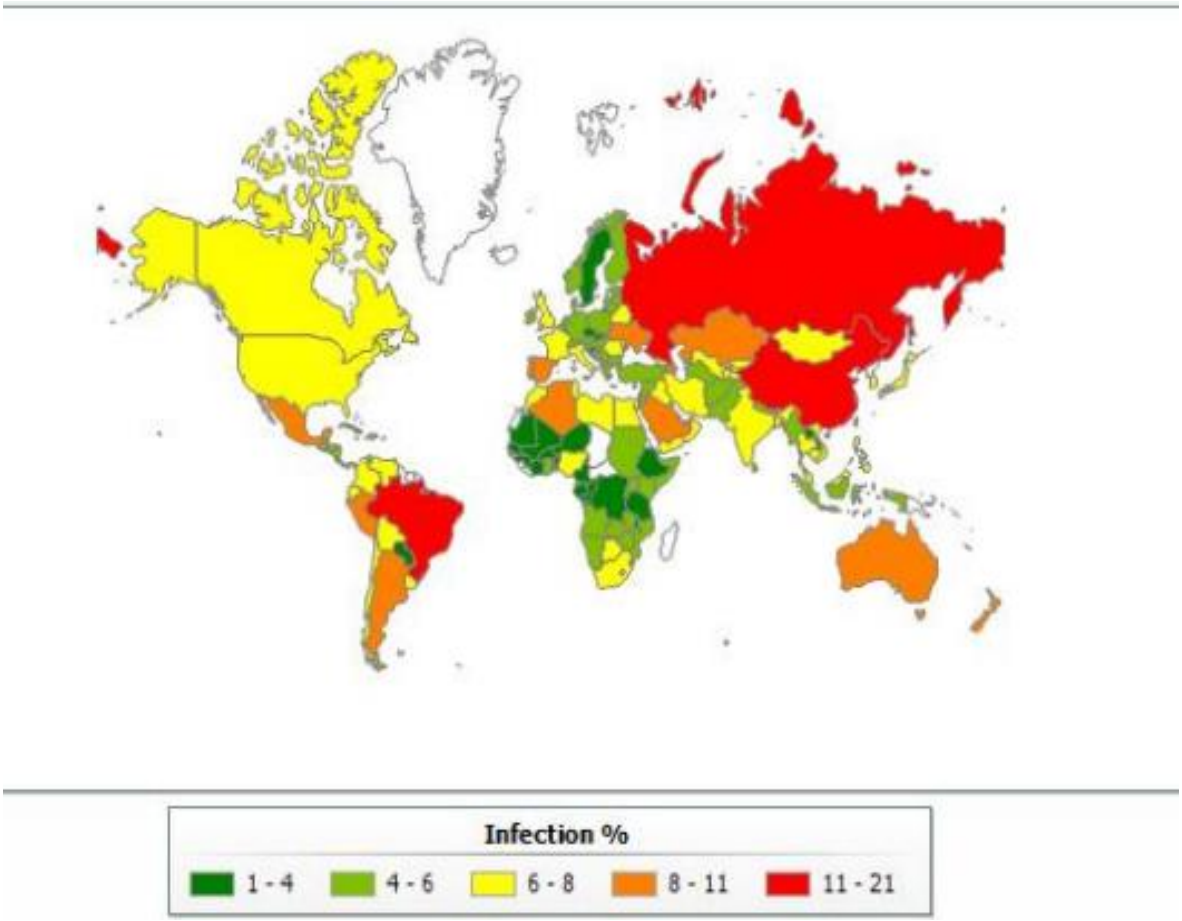


Рисунок 1.2 – Географічне розповсюдження фішингу (1-й квартал 2017 року)

Наведений нижче графік показує динаміку частки унікальних користувачів по всьому світу, які стали жертвами фішингових атак у першому кварталі 2017 року (рис. 1.3). Як і в попередніх кварталах, графік показує коливання, які відповідають окремим фішинговим компаніям.

Країни з найвищим відсотком нападу на користувачів – Китай (20,87%) та Бразилія (19,16%). За ними слідують Макао (11,94%), Російська Федерація (11,29%) та Австралія (10,73%).

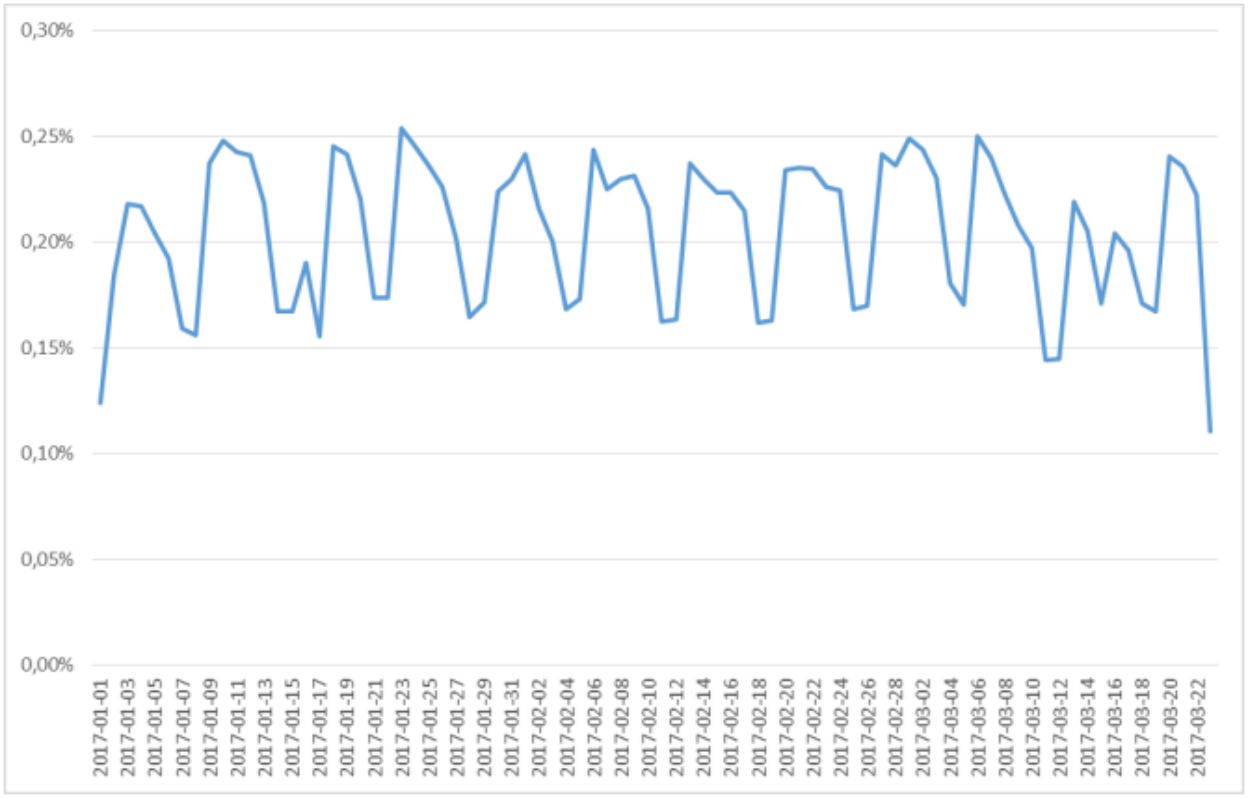


Рисунок 1.3 – Статистика фішингових атак (1-й квартал 2017 року)

Наступний графік показує відсоток користувачів, які стали жертвами фішингових атак у країнах з найбільшим відсотком атакованих користувачів (рисунок 1.4).

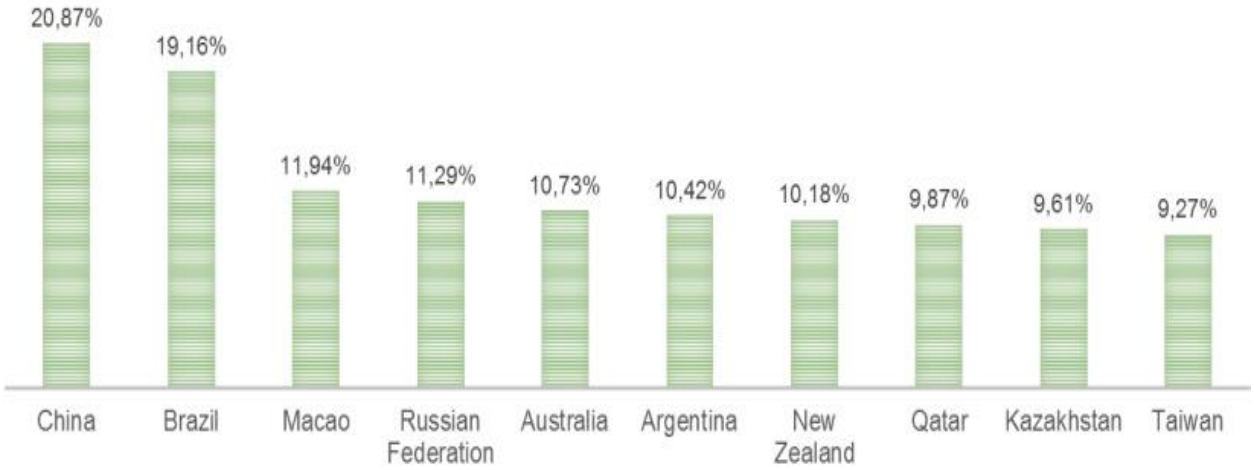


Рисунок 1.4 – Країни з найвищим рівнем жертв від фішингу

Найбільш поширеною мобільною кіберзагрозою є банківські трояни, оскільки в більшості володарів смартфонів є в наявності і банківська карта. А оскільки банки використовують мобільні номери для авторизації (наприклад, відправляють SMS з одноразовими паролями для підтвердження операцій), в шахраїв виникає спокуса цей канал комунікації перехопити і здійснювати перекази і платежі з чужого банківського рахунку.

Основних методів роботи банківських троянців три:

- вони можуть приховувати від користувача банківські SMS з паролями і тут же перенаправляти їх зловмисникові, який скористається ними, щоб перевести гроші на свій рахунок;
- банківські трояни можуть діяти в автоматичному режимі, час від часу відправляючи відносно невеликі суми на рахунку злочинців;
- зловредів відразу маскують під мобільні додатки банків і, отримавши доступ до реквізитів для входу в мобільний інтернет-банк, роблять все те ж саме [9].

За даними Лабораторії Касперського Banker.AndroidOS.Asacub.ar став найпопулярнішим троянським оператором мобільного зв’язку в третьому кварталі 2017 року, замінивши довгострокового лідера Trojan-Banker.AndroidOS.Svpeng.q. Ці мобільні банківські троянські програми використовують фішингові вікна, щоб викрасти дані кредитної картки, логіни та паролі для онлайнових банківських рахунків. Крім того, вони викрадають гроші за допомогою послуг SMS, включаючи мобільний банкінг.

Географія загроз мобільного банкінгу у 3-му кварталі 2017 року (відсоток від усіх атакованих користувачів) зображена на рисунку 1.5.

Частка атакованих користувачів виражена відсотком унікальних користувачів у кожній країні, що зазнали атаки мобільних банківських троянських програм відносно всіх користувачів мобільного продукту безпеки компанії Лабораторії Касперського у країн [10].

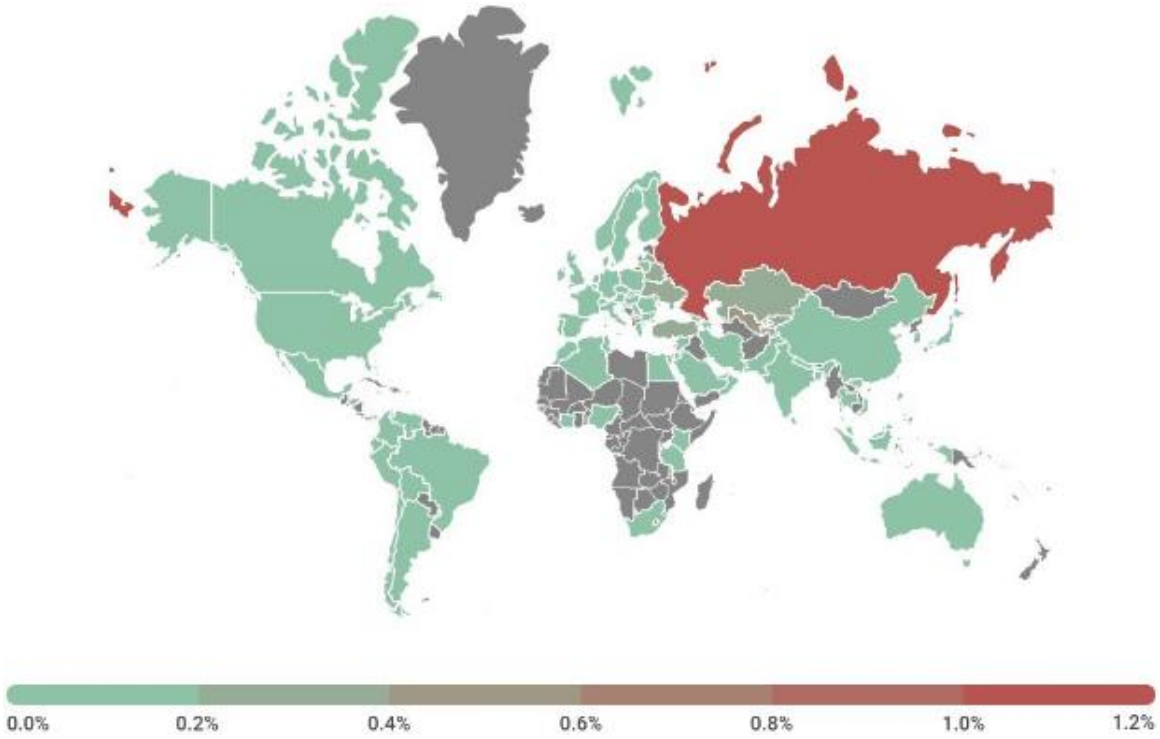


Рисунок 1.5 – Географія загроз мобільного банкінгу у 3-му кварталі 2017

Топ-10 країн, яких атакували мобільні банківські троянські програми (за рейтингом за наслідками атаки користувачів) представлені в таблиці 1.1.

Таблиця 1.1 – Топ-10 країн, атакованих банківськими троянами

№	Країна	Частка атакованих користувачів, %
1	Росія	1,20
2	Узбекистан	0,40
3	Казахстан	0,36
4	Таджикистан	0,35
5	Туреччина	0,34
6	Молдова	0,31
7	Україна	0,29
8	Киргизстан	0,27
9	Білорусь	0,26
10	Латвія	0,23

Розглянемо основні категорії «фізичних» атак (пошкодження або відкриття пристрою, підключення зовнішніх пристроїв), які є традиційними.

Скіммінг – встановлення спеціальних технічних засобів, причому не обов’язково в картоприймач, для розкрадання даних, записаних на магнітну стрічку платіжної картки. PIN-код, як правило, викрадають за допомогою

окремого технічного пристрою – відеокамери або фальшивої накладки на PIN-пад. У ряді випадків відзначено використання нового виду скіммінгового обладнання – так званого перископного.

Шиммінг – встановлення в картоприймач спеціальних технічних засобів, призначених для розкрадання з EMV-чіпа карти даних: історія платежів, інформація, що міститься на Track 2 карти, термін дії.

Black Box – встановлення або підключення технічного пристрою, що взаємодіє з компонентами банкомату (найчастіше з дозатором) і віддає останньому команду для видачі грошових коштів.

Атаки на безконтактні карти (NFC) – створення дублікатів платіжних карт, технічне розкрадання безконтактним методом ряду важливих даних, включаючи тип використовуваного платіжного додатка, термін дії карти, ім’я власника картки, PAN (Primary Account Number) карти та ін.

Підміна процесингу – в цьому випадку банкомат відключається від процесингу кредитної організації і підключається до пристрою, що імітує його. Передові пристрої можуть імітувати нормальний стан банкомату (обслуговування клієнтів) для моніторингу ПЗ. Сутність атаки полягає в передачі банкомату підроблених команд про видачу грошових коштів без порушення загальної логіки його роботи і модифікації компонентів, як апаратних, так і програмних.

Transaction Reversal Fraud (TRF) – отримання готівкових коштів з одночасним впливом на роботу банкомату і процесингового центру, в результаті чого відсутня коректне завершення операції з видачі готівки й не змінюється баланс по карті (маніпулювання картковим рахунком) [10].

Постійний розвиток комп’ютерних технологій, без яких не може обійтись жоден банк, призводить до появи все більшої кількості нових кіберзагроз в банківській сфері. У зв’язку з чим постає питання стосовно необхідності виявлення та попередження цих загроз.

Пункт 1.1.1 цього звіту було виконано із використанням матеріалів проміжного звіту про НДР [11].

1.1.2 Проведення первинного аналізу даних

В процесі підготовки до побудови моделі виявлення ознак кіберзагроз у банку в якості вихідних даних було використано інформацію, що міститься у базі даних мобільного та інтернет-банкінгу банку «X». Оскільки дана інформація є комерційною таємницею, то розголошення назви банківської установи не є можливим. Інформація містить 8 вхідних змінних, включаючи цільову змінну. Назви, зміст, ролі та типи змінних представимо в таблиці 1.2.

Таблиця 1.2 – Опис вхідних змінних

Ім'я змінної	Економічний зміст	Роль	Тип	Допустимі значення
isfraud (*Y*)	Випадки виникнення кіберзагроз	цільова	binary	1 – виявлено ознаки кіберзагроз; 0 – ознак кіберзагроз не виявлено.
amount (X_1)	Загальна сума, що проходила в транзакціях	вхідна	interval	>=0
devicetype (X_2)	Тип пристрою, з якого виконувалась транзакція	вхідна	nominal	M – мобільний банкінг; I – інтернет банкінг.
factlocation (X_3)	Ініційоване місцеположення пристрою, з якого проводилась транзакція	вхідна	nominal	UA – Україна; Other – інша країна.
location (X_4)	Місцеположення, вказане при реєстрації клієнта банкінгу	вхідна	nominal	UA – Україна.
newbalance (X_5)	Баланс клієнта після проведення транзакції	вхідна	interval	>=0
oldbalance (X_6)	Баланс клієнта до проведення транзакції	вхідна	interval	>=0
type (X_7)	Тип виконаної транзакції	вхідна	nominal	CASH_IN – поповнення коштів; CASH_OUT – зняття коштів; DEBIT – списання коштів з рахунку; PAYMENT – проведення оплати; TRANSFER – переведення коштів.

Вибірка даних склала 200000 спостережень, взятих на прикладі інформації за транзакціями користувачів мобільного та інтернет-банкінгу банку «A».

Змінна Y надає дані про те, чи мають місце в банківській транзакції ознаки кіберзагроз, виходячи з інформації за відповідною транзакцією.

Змінна X_1 представлена загальною сумою, що використана певним користувачем банку під час проведення різноманітних транзакцій.

Змінна X_2 вказує на тип пристрою, з якого було проведено транзакцію: мобільний банкінг – мобільний телефон; інтернет-банкінг – комп'ютер.

Змінна X_3 відображає ініційоване місцеположення пристрою, з якого проведено транзакцію: Україна або інша країна.

Змінна X_4 показує, яка країна була вказана користувачем мобільного або інтернет-банкінгу при реєстрації.

Змінна X_5 містить суму, що знаходиться на балансі клієнта після проведення транзакції.

Змінна X_6 містить суму, що знаходилась на балансі клієнта до проведення транзакції.

Змінна X_7 надає інформацію про тип транзакції, яку було проведено користувачем мобільного або інтернет-банкінгу.

Проаналізуємо вхідні дані для виявлення певних закономірностей і тенденцій. На рисунку 1.6 зобразимо кругову діаграму розподілу транзакцій за ймовірністю виникнення ознак кіберзагроз.

Серед набору вхідних даних про банківські операції, 22% транзакцій мають ознаки кібернетичних загроз, а у 78% – ознак кіберзагроз не виявлено. Тобто майже 1/5 всієї вибірки має ознаки кібернетичних загроз.

На рисунку 1.7 представимо розподіл банківських транзакцій за їх типами. Найбільшу долю серед проведених транзакцій становлять проведення оплати (37%), зняття коштів (33%) та поповнення коштів (21%). Незначна частка транзакцій приходиться на переведення коштів (8%) та списання коштів (1%).

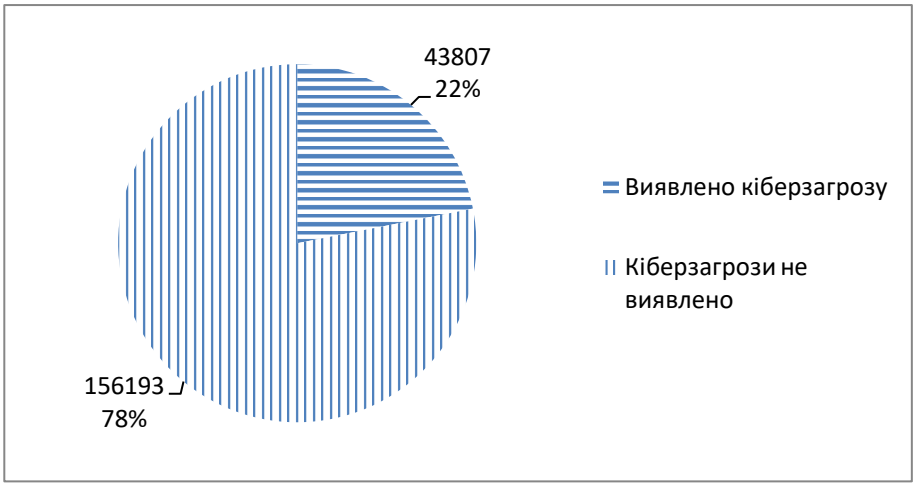


Рисунок 1.6 – Розподіл транзакцій за ймовірністю виникнення ознак кіберзагроз

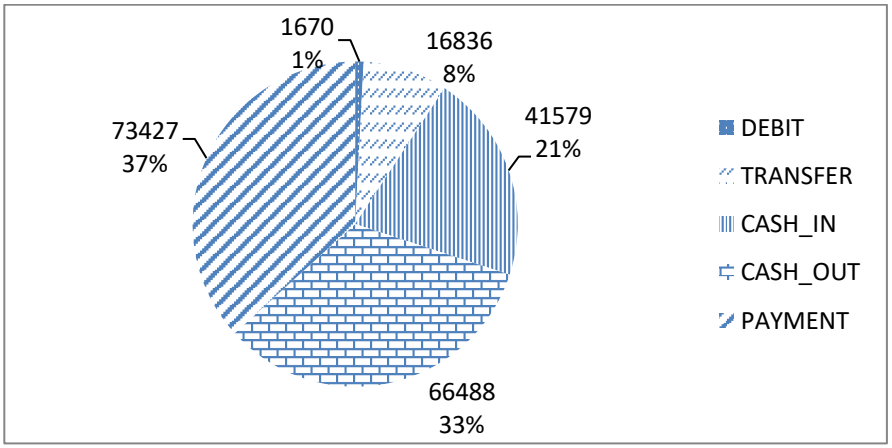


Рисунок 1.7 – Розподіл транзакцій за їх типами

На рисунку 1.8 зобразимо розподіл банківських транзакцій за типами пристроїв, з яких вони виконувались. Розподіл пристроїв мобільного (51%) та інтернет-банкінгу (49%) майже однаковий.

На рисунку 1.9 представимо розподіл банківських транзакцій за місцеположенням пристрою, з якого проводилась транзакція. В більшості виконаних транзакцій (78%) місцеположення пристрою визначалось як Україна, 22% транзакцій було зафіксовано в інших країнах.

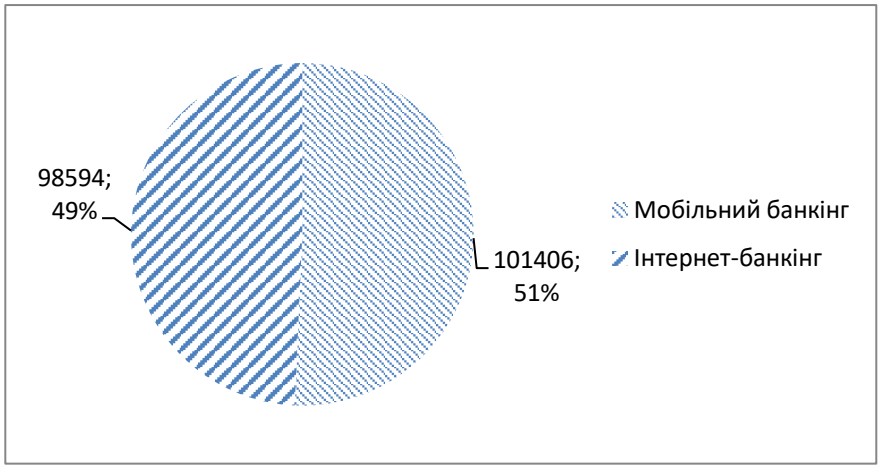


Рисунок 1.8 – Розподіл транзакцій за типами пристроїв, з яких вони виконувались

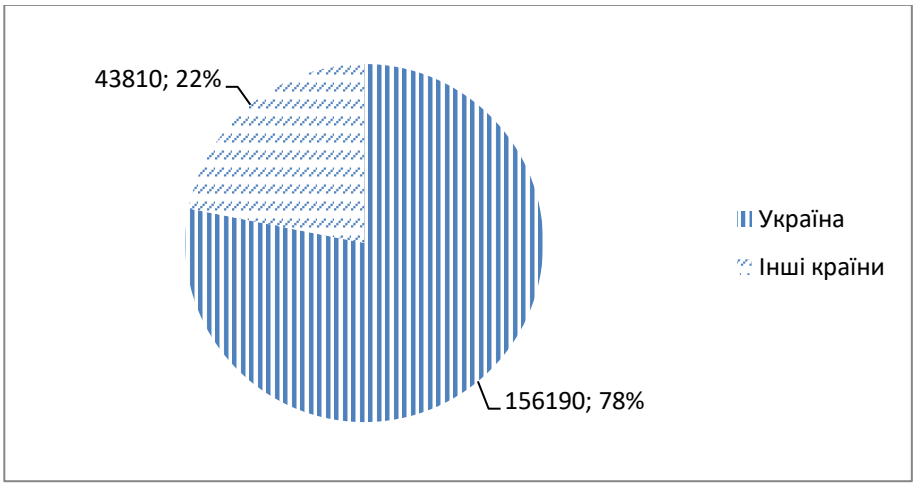


Рисунок 1.9 – Розподіл транзакцій за місцеположенням пристрою, з якого проводилась транзакція

Таким чином, було обрано вхідні змінні для подальшого їх застосування з метою побудови моделей виявлення кіберзагроз в банках методами інтелектуального аналізу.

Для попереднього аналізу пданих щодо виявлення кібернетичних загроз в банківських установах з метою майбутнього попередження цих загроз в разі їх виникнення скористаємося аналітичним пакетом SAS Enterprise Miner.

SAS Enterprise Miner полегшує і систематизує процес інтелектуального аналізу даних, дозволяючи створювати високоточні передбачувальні і описові моделі на основі аналізу величезної кількості інформації, що збирається у всій

організації. Цей пакет інструментів допомагає вирішувати широке коло завдань, що вимагають вивчення інформації і можливості передбачити хід подій, а саме: виявляти випадки шахрайства, визначати і мінімізувати рівень ризиків, прогнозувати потреби в ресурсах, попереджати інциденти, підвищувати рівень відгуку на маркетингові кампанії, знижувати відтік клієнтів та інші.

Цей пакет являє собою найбільш потужне і повнофункціональне рішення з усіх наявних на ринку для передбачувальної аналітики та інтелектуального аналізу даних. SAS Enterprise Miner дозволяє користувачам досліджувати і аналізувати складні дані, знаходити стійкі закономірності і, ґрунтуючись на фактах і отриманих висновках, приймати виважені рішення.

SAS Enterprise Miner створений для фахівців з аналізу даних, статистиків, маркетингових аналітиків, маркетологів, експертів з аналізу ризиків, фахівців з виявлення шахрайських дій. Цей інструмент також активно використовується інженерами, науковцями та бізнес-аналітиками, яким необхідно розуміти і аналізувати постійно зростаючі обсяги даних, розпізнавати критичні завдання бізнесу або наукових досліджень і приймати обґрунтовані рішення [12].

Для реалізації поставленої задачі відкриємо програму SAS Enterprice Miner та створимо новий проект. В створеному проекті виконаємо підключення бібліотек та створимо діаграму з ім’ям Bank.

File > New diagram > Name = Bank.

Задамо джерело даних banking.sas7bdat.

File > New > Data Source > Next > Browse > banking.sas7bdat > Next.

Додана вибірка даних містить 200000 записів і 8 параметрів.

На кроці 4 Metadata Advisor Options натиснемо Advanced > Customize > змінимо значення властивостей та натиснемо Next.

Class Levels Count Threshold = 2, означає, що тільки бінарні чисельні змінні будуть сприйматися як категоріальні. А всі інші чисельні змінні у яких більш ніж два рівня будуть сприйняті як інтервальні (безперервні).

Reject Levels Count Threshold = 100, означає, що змінні не будуть відхилені з аналізу через велику кількість рівнів.

Для цільової змінної з набору даних isfraud, яка відповідає за відгук, задамо роль Target, рівень – Binary (рис. 1.10). Завдяки цьому система автоматично обере логістичну регресію):

1 – так (виконана транзакція є загрозою);

0 – ні.

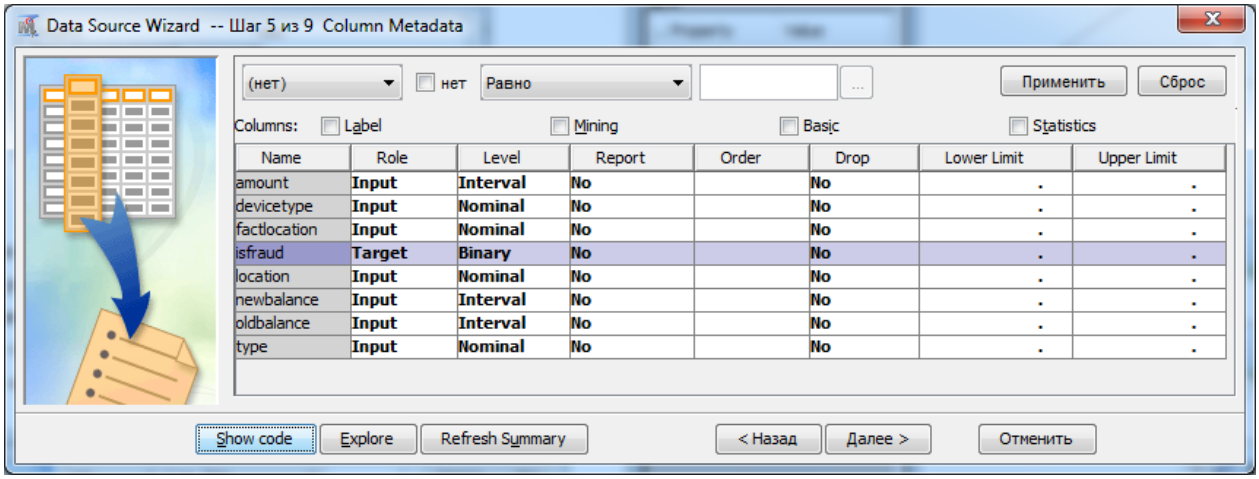


Рисунок 1.10 – Визначення ролей вхідних змінних

Для завершення створення джерела даних обираємо Next > Next > Next > Finish.

Виконаємо первинний аналіз вхідних даних за допомогою інструмента StatExplore пакету SAS Enterprise Miner.

Перетягнемо джерело даних BANKING у вікно робочої області Bank. Додамо інструмент StatExplore та об’єднаємо з джерелом даних (рис. 1.11).

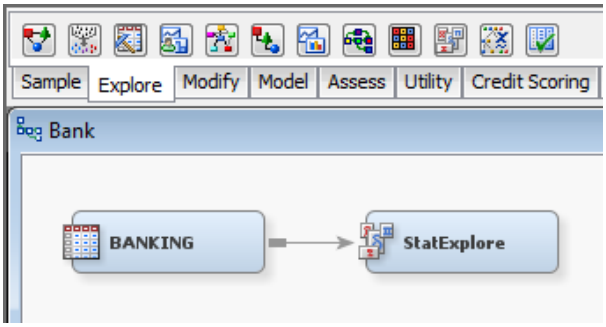


Рисунок 1.11 – Об’єднання інструмента StatExplore з джерелом даних

Натиснемо правою кнопкою по вузлу StatExplore і виберемо Run з меню швидкого виклику. Переглянемо результати ходу виконання даного вузла.

На рисунку 1.12 відображені категоріальні змінні та їх основні властивості: роль змінної, кількість рівнів, пропущенні значення, мода.

Output

Data Role=TRAIN

Data Role	Variable Name	Role	Number of Levels	Missing	Mode	Mode Percentage	Mode2	Mode2 Percentage
TRAIN	devicetype	INPUT	2	0	M	50.53	I	49.47
TRAIN	factlocation	INPUT	2	0	UA	79.12	Other	20.88
TRAIN	type	INPUT	5	0	PAYMENT	39.51	CASH_OUT	30.72
TRAIN	isfraud	TARGET	2	0	0	79.12	1	20.88

Рисунок 1.12 – Основні властивості вхідних категоріальних змінних

На рисунку 1.13 відображена інформація стосовно цільової змінної isfraud: частоти позитивного та негативного відгуку, а також долі від цілого.

Output

Data Role=TRAIN

Data Role	Variable Name	Role	Level	Frequency Count	Percent
TRAIN	isfraud	TARGET	0	79124	79.124
TRAIN	isfraud	TARGET	1	20876	20.876

Рисунок 1.13 – Статистична інформація щодо цільової змінної isfraud

Доля проведених банківських транзакцій, які виявились кібернетичними загрозами становить 20,9 %, в свою чергу в 79,1% проведених операцій не виявлено кіберзагроз.

На рисунку 1.14 відображена статистична інформація по інтервальних змінних: роль змінної, середнє значення, стандартне відхилення, пропущені значення, мінімум, медіана, максимум.

Output

Data Role=TRAIN

Variable	Role	Mean	Standard Deviation	Non Missing	Missing	Minimum	Median	Maximum	Skewness	Kurtosis
amount	INPUT	187512.4	478553.1	99962	38	0	54609	33966807	19.2124	877.3581
newbalance	INPUT	661149.4	2386766	98091	1909	0	0	99696007	16.28264	486.3307
oldbalance	INPUT	652039.6	2365850	98165	1835	0	18545	99696007	16.56692	501.0274

Рисунок 1.14 – Статистичні характеристики вхідних інтервальних змінних

В результаті проведеного первинного аналізу було отримано основні статистичні характеристики вхідних змінних, визначено ролі змінних у моделюванні, а також виявлено, що у вхідному масиві даних відсутні пропущені значення в інтервальних змінних.

Для розбиття набору даних на тренувальний, тестовий та перевірочний набори даних скористаймося інструментом Data Partition пакету SAS Enterprise Miner. Додамо даний інструмент та об’єднаємо з джерелом даних. У властивостях вузла Data Partition оберемо частки даних для навчання (50%) та перевірки (50%).

Далі, проаналізувавши графіки інтервальних змінних, можна побачити, що розподіл даних величин не відповідає нормальному закону розподілу (рис. 1.15).

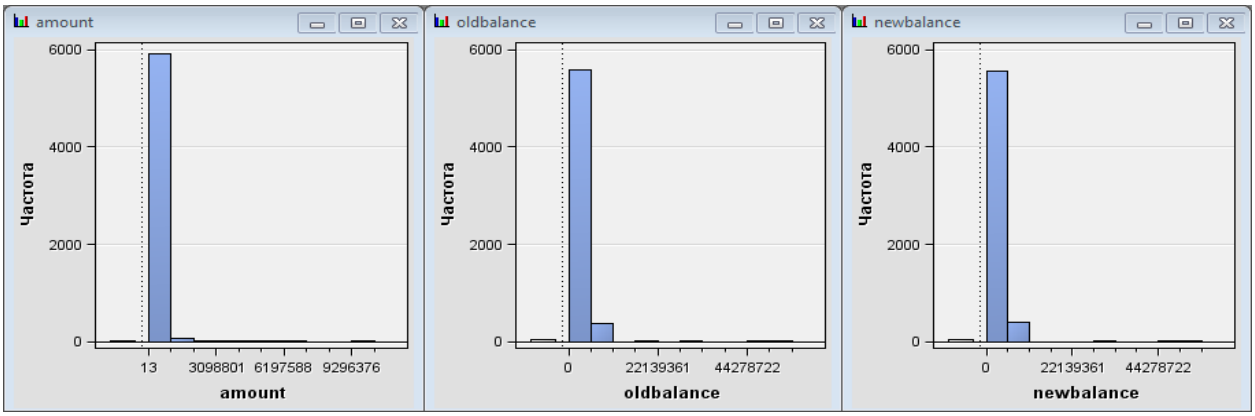


Рисунок 1.15 – Перевірка нормального закону розподілу у вхідних інтервальних змінних

А тому, для подальшої побудови моделей необхідно пролагорифмувати вхідні змінні. Для цього скористаймося інструментом Transform Variables пакету SAS Enterprise Miner. Додамо у вікно робочої області інструмент Transform Variables та об’єднаємо з вузлом Data Partition (рис. 1.16).

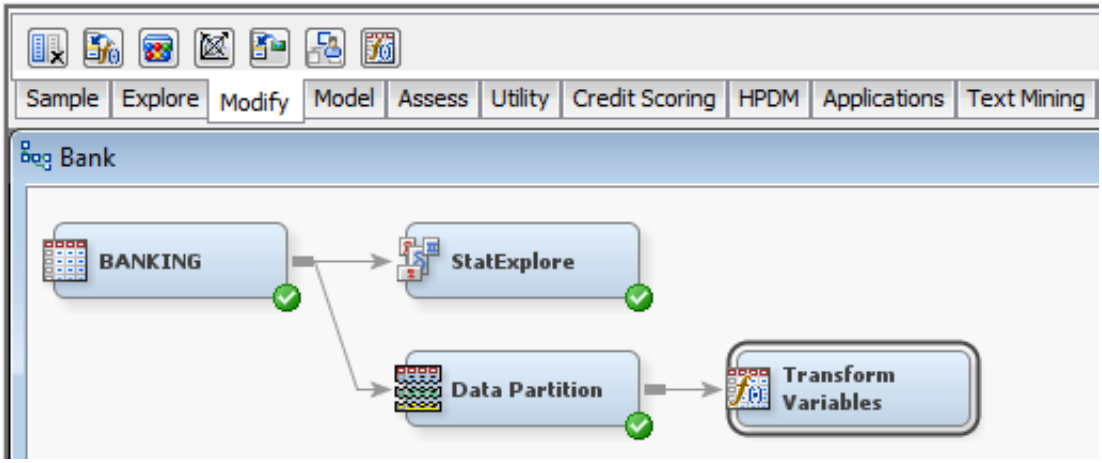


Рисунок 1.16 – Додавання вузла Transform Variables в робочу область

У властивостях вузла Transform Variables оберемо Variables та вкажемо для інтервальних змінних amount, oldbalance та newbalance метод Log (рис. 1.17).

Variables - Trans2

(нет) нет Равно

Columns: Label Mining

Name	Method	Number of Bins	Role	Level
amount	**Log**	**4**	Input	Interval
devicetype	**Default**	**4**	Input	Nominal
factlocation	**Default**	**4**	Input	Nominal
isfraud	**Default**	**4**	Target	Binary
location	**Default**	**4**	Input	Nominal
newbalance	**Log**	**4**	Input	Interval
oldbalance	**Log**	**4**	Input	Interval
type	**Default**	**4**	Input	Nominal

Рисунок 1.17 – Логарифмування вхідних інтервальних змінних

Після проведення первинного аналізу даних та логарифмування вхідних змінних, джерело даних можна застосовувати для інтелектуального аналізу даних.

Пункт 1.1.2 цього звіту було виконано із використанням матеріалів проміжного звіту про НДР [11].

1.1.3 Кластерний аналіз як інструмент дослідження первинних даних

Задача кластеризації подібна до задачі класифікації, є її логічним продовженням, але її відмінність в тому, що класи набору даних, що вивчається заздалегідь не визначені.

Мета кластеризації – пошук існуючих структур. Кластеризація є описовою процедурою, вона не робить жодних стратегічних висновків, проте дає можливість провести розвідчий аналіз та вивчити структуру даних.

Нехай X – множина об'єктів, Y - множина номерів (імен, міток) кластерів. Задана функція відстані між об'єктами $\rho(x, x')$ Є кінцева навчальна вибірка об'єктів $X^m = \{x_1, x_2, \dots, x_m\} \in X$. Потрібно розбити вибірку на непересічні підмножини, які називаються кластерами, так, щоб кожен кластер складався з об'єктів, близьких за метрикою ρ, а об'єкти різних кластерів істотно відрізнялися. При цьому кожному об'єкту $x_i \in X^m$ приписується номер кластера y_i.

Алгоритм кластеризації – це функція $\alpha: X \to Y$, яка будь-якому об'єкту $x \in X$ ставить у відповідність номер кластера $y \in Y$. Множина Y в деяких випадках відома заздалегідь, однак частіше ставиться завдання визначити оптимальне число кластерів, з точки зору того чи іншого критерію якості кластеризації.

Кластер можна охарактеризувати як групу об’єктів, що мають спільні властивості. Характеристиками кластера можна назвати дві ознаки:

– внутрішня однорідність;

– зовнішня ізольованість.

Існує велика кількість підходів до кластеризації:

– алгоритми, засновані на поділі даних (Partitioning algorithms), в тому числі ітеративні: поділ об’єктів на k кластерів; ітеративний перерозподіл об’єктів для поліпшення кластеризації;

– ієрархічні алгоритми (Hierarchy algorithms);

– методи, засновані на концентрації об’єктів (Density-based methods);

– грід-методи (Grid-based methods);

– модельні методи (Model-based).

Слід зазначити, що в результаті застосування різних методів кластерного аналізу можуть бути отримані кластери різної форми. В результаті застосування різних методів кластеризації можуть бути отримані неоднакові результати, це є особливістю роботи того чи іншого алгоритму. Однак створення подібних кластерів різними методами вказує на правильність кластеризації.

Задачі кластерного аналізу можна об'єднати в наступні групи:

– розробка типології або класифікації;

– дослідження корисних концептуальних схем групування об'єктів;

– представлення гіпотез на основі дослідження даних;

– перевірка гіпотез або досліджень для визначення, чи дійсно типи (групи), виділені тим чи іншим способом, присутні в наявних даних.

Як правило, при практичному використанні кластерного аналізу одночасно вирішується кілька із зазначених задач [13].

Досліджуючи один або більше атрибутів або класів, можна згрупувати окремі елементи даних разом, отримуючи структурований вивід. На простому рівні при кластеризації використовується один або декілька атрибутів в якості основи для визначення кластера подібних результатів. Кластеризація корисна при визначенні різної інформації, тому що вона корелюється з іншими прикладами так, що можна побачити, як подібність і діапазони узгоджуються між собою. Метод кластеризації працює в обидві сторони. Можна припустити, що в певній точці мається кластер, а потім використовувати свої критерії ідентифікації, щоб перевірити це [14].

У непараметричному випадку ми не маємо інформації про загальний вигляд функцій $f_j(X, \Theta_j)$. Ми можемо мати лише окремі загальні відомості про них: компактність або обмеженість діапазонів змінювання компонент класифікованих багатовимірних спостережень, неперервність або гладкість відповідних законів розподілу ймовірностей тощо. Вихідні дані зазвичай подають у вигляді матриці спостережень, яка містить значення всіх ознак для кожного із досліджуваних

об’єктів, або матриці подібності, що містить попарні відстані між класифікованими спостереженнями.

Бажано, щоб компоненти вектора X відповідали одному й тому самому типу даних. Для цього зазвичай використовують перехід від кількісних ознак до порядкових та від порядкових до номінальних. Але слід ураховувати, що при цьому втрачається частина корисної інформації.

Для формалізації задачі класифікації кожний об’єкт зручно інтерпретувати як точку в багатовимірному просторі ознак. Геометрична близькість точок у такому просторі відповідає близькості досліджуваних об’єктів з погляду досліджуваних властивостей.

Класичними непараметричними методами класифікації без навчання є методи кластерного аналізу (таксономії). За їх допомогою вирішують проблему такого розбиття (класифікації, кластеризації) множини об’єктів, за якого всі об’єкти, що належать до одного класу, були б більш подібними один до одного, ніж до об’єктів інших класів. З формальної точки зору, основне завдання методів кластерного аналізу можна сформулювати, як визначення класів еквівалентності й рознесення за ними досліджуваних об’єктів. Під класом, як правило, розуміють генеральну сукупність, що описується одномодальною функцією щільності ймовірності f(X) або, у випадку дискретних ознак, – одномодальним полігоном імовірностей. Номери класів не мають змістового навантаження й використовуються лише для того, щоб відрізняти їх один від одного.

Для формування кластерів застосовують міри подібності та відмінності даних, які можуть бути поділені на три основних види:

– міри подібності (відмінності) типу «відстань» (при їх застосуванні об’єкти вважають тим більш подібними один до одного, чим меншою є відстань між ними);

– міри подібності типу «зв’язок» (у цьому випадку об’єкти вважають тим більш подібними, чим сильнішим є зв’язок між ними);

– інформаційна статистика [15].

Як і будь-які інші методи, методи кластерного аналізу мають певні слабкі сторони, тобто деякі складності, проблеми та обмеження. При проведенні кластерного аналізу слід враховувати, що результати кластеризації залежать від критеріїв розбиття сукупності вихідних даних. При зниженні розмірності даних можуть виникнути певні спотворення, за рахунок узагальнень можуть загубитися деякі характеристики об’єктів.

Існує ряд складнощів при проведенні кластеризації:

1. Складність вибору характеристик, на основі яких проводиться кластеризація. Необдуманий вибір призводить до неадекватного розбиття на кластери і, як наслідок, – до невірного рішення задачі;

2. Складність вибору методу кластеризації. Цей вибір вимагає хорошого знання методів і передумов їх використання. Щоб перевірити ефективність конкретного методу в певній предметній області, доцільно застосувати таку процедуру: розглядають кілька апріорі різних між собою груп і перемішують їх представників між собою випадковим чином. Далі проводиться кластеризація для відновлення вихідного розбиття на кластери. Частка збігів об’єктів в виявлених і вихідних групах є показником ефективності роботи методу;

3. Проблема вибору числа кластерів. Якщо немає ніяких відомостей щодо можливого числа кластерів, необхідно провести ряд експериментів і в результаті перебору різного числа кластерів вибрати оптимальне їх число;

4. Проблема інтерпретації результатів кластеризації. Форма кластерів в більшості випадків визначається вибором методу об’єднання. Проте слід враховувати, що конкретні методи прагнуть створювати кластери певних форм, навіть якщо в досліджуваному наборі даних кластерів насправді немає [13].

Для виявлення прихованих, неочевидних тенденцій та закономірностей у вхідних даних, проведемо більш серйозний, глибинний статистичний аналіз – кластерний. Дослідження виконаємо у пакеті SAS Enterprise Miner.

Спочатку обираємо вхідні змінні для кластерного аналізу. Вхідні змінні повинні мати наступні властивості: бути значимими для цілей аналізу; бути відносно незалежними; бути обмеженими по кількості [16].

Зважаючи на ці вимоги, було обрано наступні вхідні змінні з таблиці 1.2 (табл. 1.3).

Таблиця 1.3 – Опис вхідних змінних для кластерного аналізу

Ім'я змінної	Економічний зміст	Роль змінної	Тип
amount (X_1)	Загальна сума, що була проходила в транзакціях	вхідна	interval
devicetype (X_2)	Тип пристрою, з якого виконувалась транзакція	вхідна	nominal
factlocation (X_3)	Зафіксоване місцеположення пристрою, з якого проводилась транзакція	вхідна	nominal
newbalance (X_5)	Баланс клієнта після проведення транзакції	вхідна	interval
type (X_7)	Тип виконаної транзакції	вхідна	nominal

Додамо в область діаграми інструмент Cluster та об'єднаємо з вузлом Transform Variables (рис. 1.18).

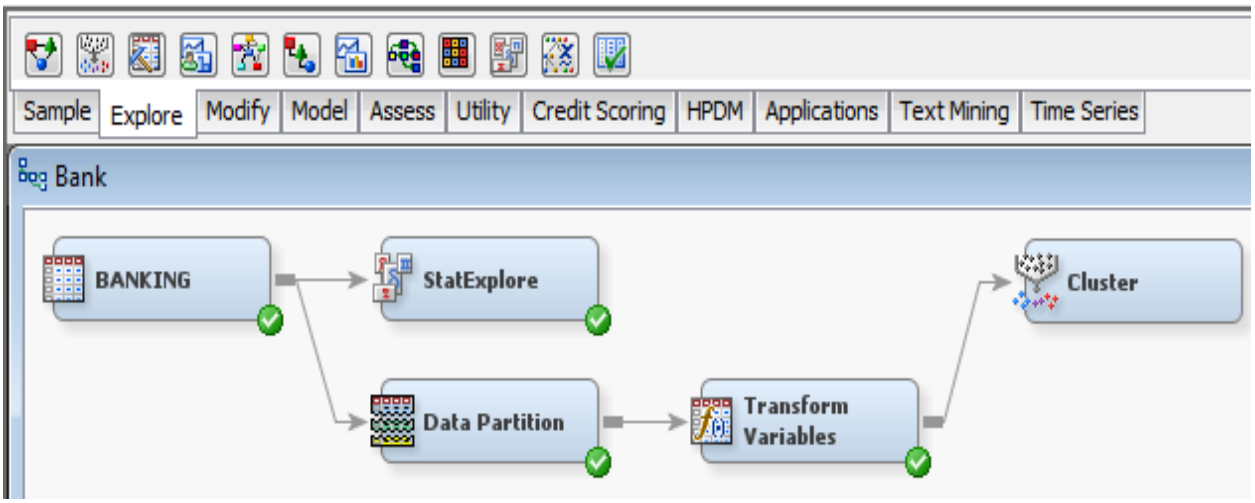


Рисунок 1.18 – Додавання інструмента Cluster в робочу область діаграми

У властивостях вузла Cluster вкажемо самостійно максимальну кількість кластерів – 4. Результатом кластерного аналізу даних у пакеті SAS Enterprise Miner є виділення 4-х кластерів з наступними статистичними характеристиками (табл. 1.4).

Таблиця 1.4 – Статистика у розрізі окремих кластерів в пакеті SAS Enterprise Miner

Характеристики	№ сегмента кластеру			
	1	2	3	4
Кількість випадків, що потрапили у кластер	48026	43793	60528	47653
Відсоток випадків, що потрапили у кластер	24,01	21,9	30,26	23,83
Найближчий кластер до даного	4	3	1	1
Середнє значення LOG_amount у кластері	8,5590	11,7833	11,1866	11,8361
Середнє значення LOG_newbalance у кластері	10,0476	0,0002	0,0087	13,5509

Діаграму розподілу даних по кластерам представлено на рис. 1.19.

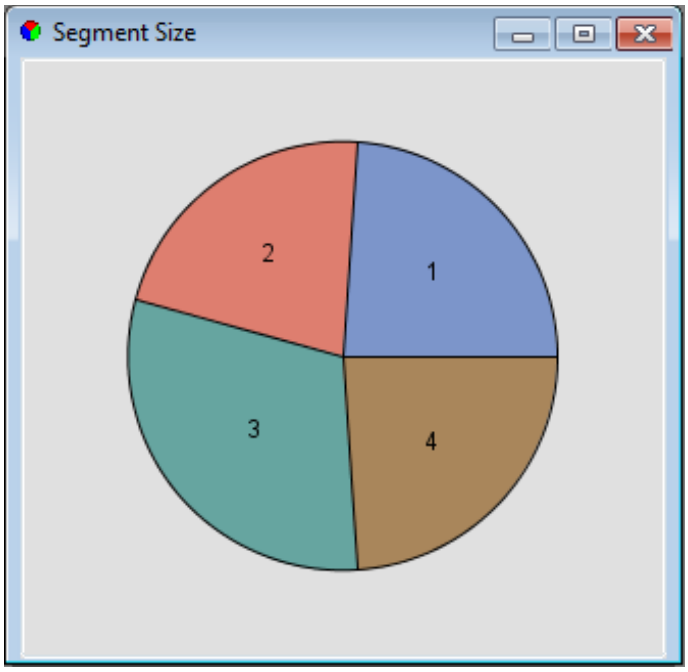


Рисунок 1.19 – Розподіл даних на кластери в пакеті SAS Enterprise Miner

Отже, кількість випадків, що класифіковано у 1-й кластер – 48026, у 2-й – 43793, у 3-й – 60528, у 4-й – 47653. Тобто, за величиною випадків кластери є приблизно однаковими.

Оскільки для генерування сегментів використовується більше трьох змінних, інтерпретація таких графіків стає складнішою. Для цього в SAS Enterprise Miner є інструмент для інтерпретації композиції кластерів: Segment Profile на панелі Assess, який дозволяє порівнювати розподіл змінної в

конкретному сегменті з розподілом змінної в загальному наборі даних. Також, змінні упорядковуються відносно того, наскільки добре вони характеризують даний сегмент. Додаємо інструмент Segment Profile з набору інструментів Assess в робочу область діаграми та з'єднуємо його з вузолом Cluster для дослідження кожного кластеру окремо (рис. 1.20).

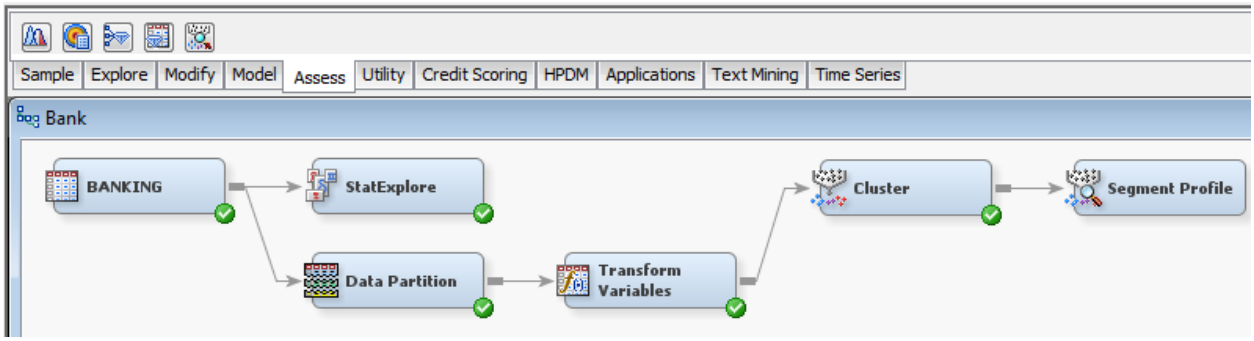


Рисунок 1.20 – Додавання інструменту Segment Profile в область діаграми

Запускаємо на виконання вузол вузол Segment Profile і обираємо Results. Відкриється вікно Results. Профільне дослідження кластерів та важливість кожної змінної у формуванні того чи іншого кластеру наведені на рисунках 1.21 – 1.22. Таким чином, при формуванні першого кластеру найбільшу вагу мали змінні LOG_amount та LOG_newbalance, незначний вплив становила змінна factlocation. На формування другого кластеру найбільше вплинула змінна factlocation та менш значно вплинули змінні LOG_newbalance та LOG_amount. Змінна LOG_newbalance спричинила значний вплив на формування третього та четвертого кластерів, в той час як вплив змінних LOG_amount та factlocation на ці кластери був меншим.

Отже, за допомогою кластерного аналізу було досліджено інформацію про проведені транзакції клієнтами мобільного та інтернет-банкінгу. Визначено, що існує певна закономірність між місцеположенням пристроїв, з яких виконувались транзакції, сумами коштів на рахунках клієнтів та балансами після виконання транзакцій. Їх значення та зміни впливають на ознаку втручання у банківську систему.

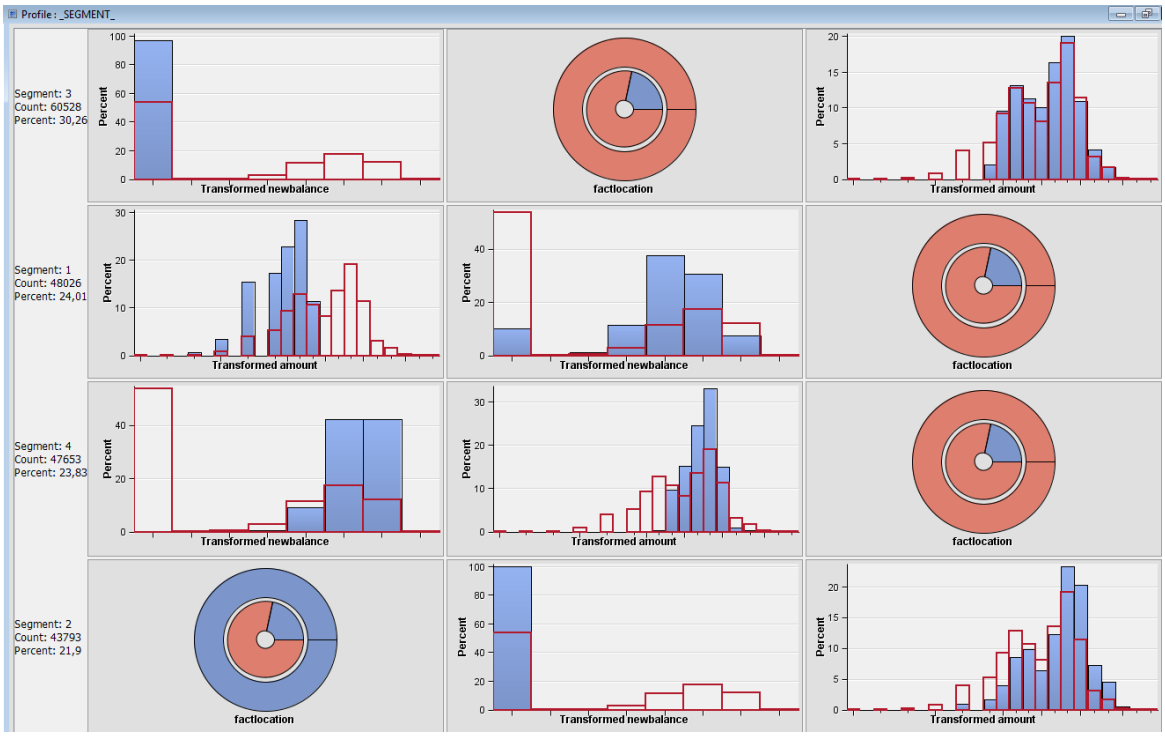


Рисунок 1.21 – Профільний аналіз кластерів в пакеті SAS Enterprise Minner

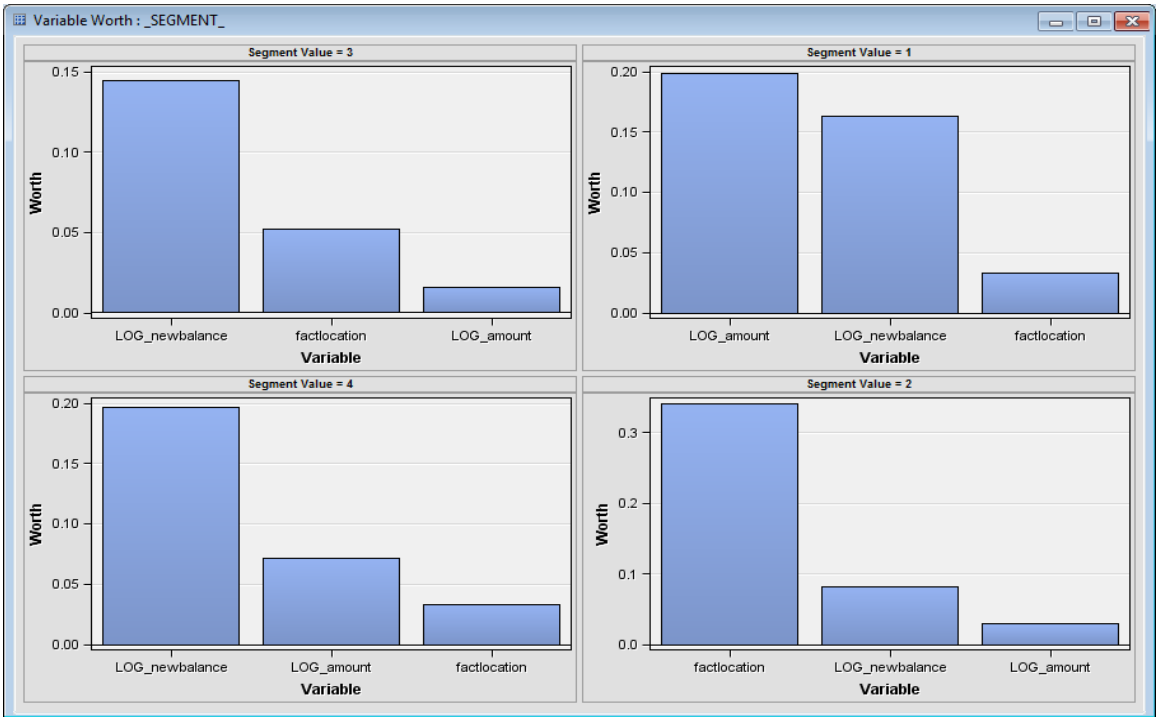


Рисунок 1.22 – Вага кожної змінної у формуванні відповідного кластеру в пакеті SAS Enterprise Miner

Пункт 1.1.3 цього звіту було виконано із використанням матеріалів проміжного звіту про НДР [11].

1.2 Розробка математичних моделей ймовірності виникнення шахрайських операцій, як одного із різновидів кіберзагроз, в банках

1.2.1 Побудова моделей Data Mining для визначення ймовірності виникнення шахрайських операцій

Для побудови моделі було висунуто ряд гіпотез стосовно вірогідності виникнення ознак кіберзагроз під час проведення транзакцій користувачами мобільного та інтернет-банкінгу. Виходячи з аналізу статистичних даних виділимо показники, що можуть вказувати на можливе виникнення кіберзагрози в процесі виконання банківської операції [5]:

1) транзакція має ознаки загрози, якщо її ініційовано на території іншої країни. В більшості банків прийнята практика необхідності повідомлення банка клієнтом про його виїзд за кордон та зазначення країн, які будуть відвідані. В іншому випадку служба безпеки банку може заблокувати карту, якщо по ній будуть ініційовано транзакції з іншої країні. Це пов’язано з тим, що хакери, зламуючи доступ до мобільного або інтернет-банкінгу та привласнюючи чужі кошти, застосовують спеціальні програми для шифрування їх місцеположення;

2) на ймовірність виникнення кіберзагрози впливає тип пристрою, з якого виконувалась транзакція. Існують різні способи злому мобільних пристроїв та комп’ютерів, завдяки яким зловмисники з легкістю отримують доступ до мобільного та інтернет-банкінгу користувачів банківських послуг. Також банк не в змозі контролювати, хто є користувачем та де він користується пристроєм. Частіше за все такі операції можуть містити ознаки кіберзагроз;

3) тип проведеної транзакції впливає на ймовірність виникнення ознак кіберзагрози. Широке коло типів банківських транзакцій сприяє впровадженню нових заходів з боку зловмисників, направлених на заволодіння чужими коштами та порушення безпеки інформації в банку;

4) обнуління рахунків клієнтів банку вказує на ймовірні ознаки кіберзагроз. Сьогодні досить розповсюдженими є безготівкові розрахунки, коли

платежі відбуваються без використання готівкових коштів. Тому, в більшості випадків на банківському рахунку людини завжди присутня певна сума коштів. Якщо під час транзакції зі зняття всієї суми можливо має місце ознака порушення користування рахунком або несанкціоноване зняття коштів.

З урахуванням означених гіпотез обрано вхідні та вихідні показники для моделювання, опис яких представлено в таблиці 1.2. Враховуючи обрані змінні та гіпотези було розроблено концептуальну модель виявлення ознак кіберзагроз в транзакціях користувачів мобільного та інтернет-банкінгу (рис. 1.23).

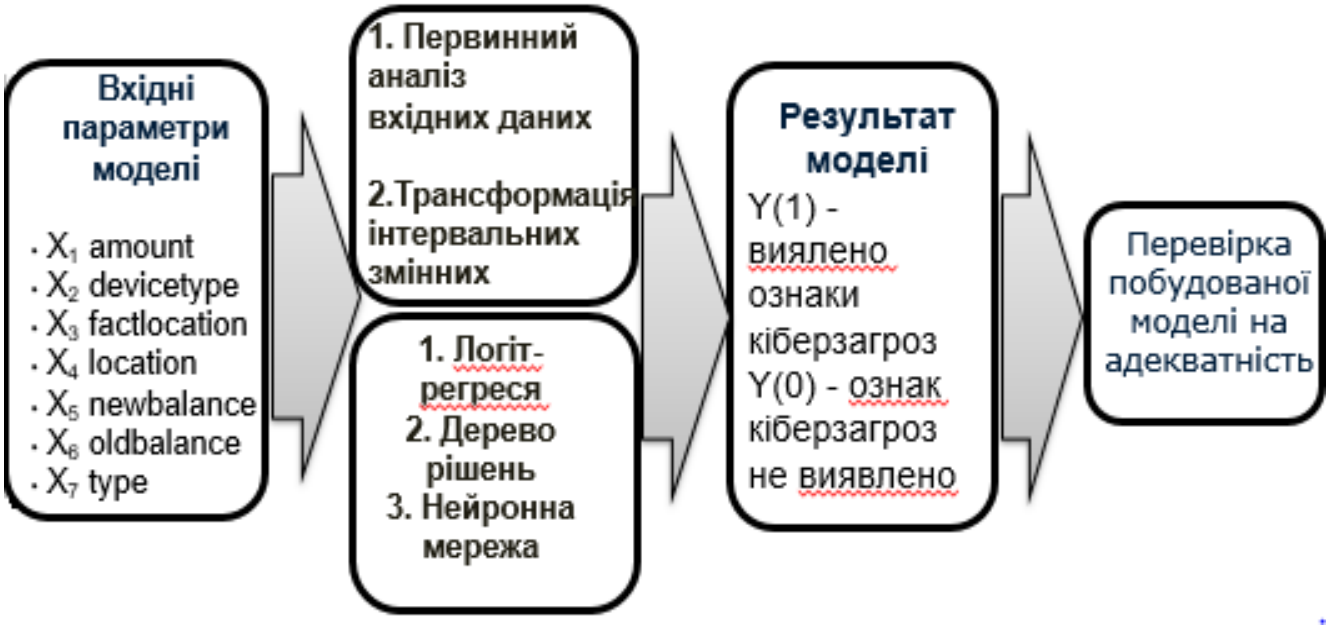


Рисунок 1.23 – Концептуальна модель виявлення ознак кіберзагроз в банківських транзакціях

На першому кроці реалізації концептуальної моделі було проведено первинний аналіз, де було зроблено перевірку інтервальних вхідних змінних на відповідність нормальному закону розподілу. Оскільки гіпотеза не підтвердилася, було проведено трансформацію вхідних змінних шляхом їх логарифмування.

На наступному кроці було обрано такі методи інтелектуального аналізу, як логіт-регресія, дерево рішень та нейронна мережа. Даний вибір обумовлено тим, що дані методи є досить ефективними для оцінки ймовірності. Побудову моделей було виконано за допомогою аналітичного пакету “SAS Enterprise Miner” [11].

В результаті побудови логіт-регресії отримано результати оцінки, представлені на рисунку 1.24. [17]

Output

Analysis of Maximum Likelihood Estimates

Parameter	DF	Estimate	Standard Error	Wald Chi-Square	Pr > ChiSq	Standardized Estimate	Exp(Est)
Intercept	1	-3.4043	0.3518	93.65	<.0001		0.033
LOG_newbalance	1	-0.8950	0.0910	96.66	<.0001	-3.1280	0.409
LOG_oldbalance	1	0.8738	0.0846	106.81	<.0001	2.7445	2.396
factlocation Other	1	5.1102	0.2700	358.11	<.0001		165.707

Рисунок 1.24 – Результати оцінки параметрів логіт-регресії

У результаті покрокового відбору було обрано 3 значущі фактори:

1) ініційоване місцеположення пристрою, з якого проводилась транзакція (інша країна) ($X_{3.2}$);

2) баланс клієнта після проведення транзакції (X_5);

3) баланс клієнта до проведення транзакції (X_6).

Розраховані значення ймовірності < 0,0001, що свідчить про високу статистичну значущість параметрів регресії. Використовуючи отримані значення, побудовано математичну модель логіт-регресії для оцінки вірогідності виникнення ознак кіберзагроз під час проведення транзакцій користувачами мобільного та інтернет-банкінгу (формула 1.1):

$$P = \frac{1}{1 + E^{-(-3{,}4+5{,}11X_{3.2}-0{,}89X_5+0{,}87X_6)}} \quad (1.1)$$

Отже, ймовірність того, що банківська транзакція буде мати ознаки кіберзагрози, зростає із присутністю зафіксованого факту проведення транзакції в іншій країні, з великим значенням балансу до проведення транзакції та зменшується із великим значенням балансу після проведення транзакції.

На наступному кроці побудовано трирівневе дерево рішення (рис. 1.25). [17]

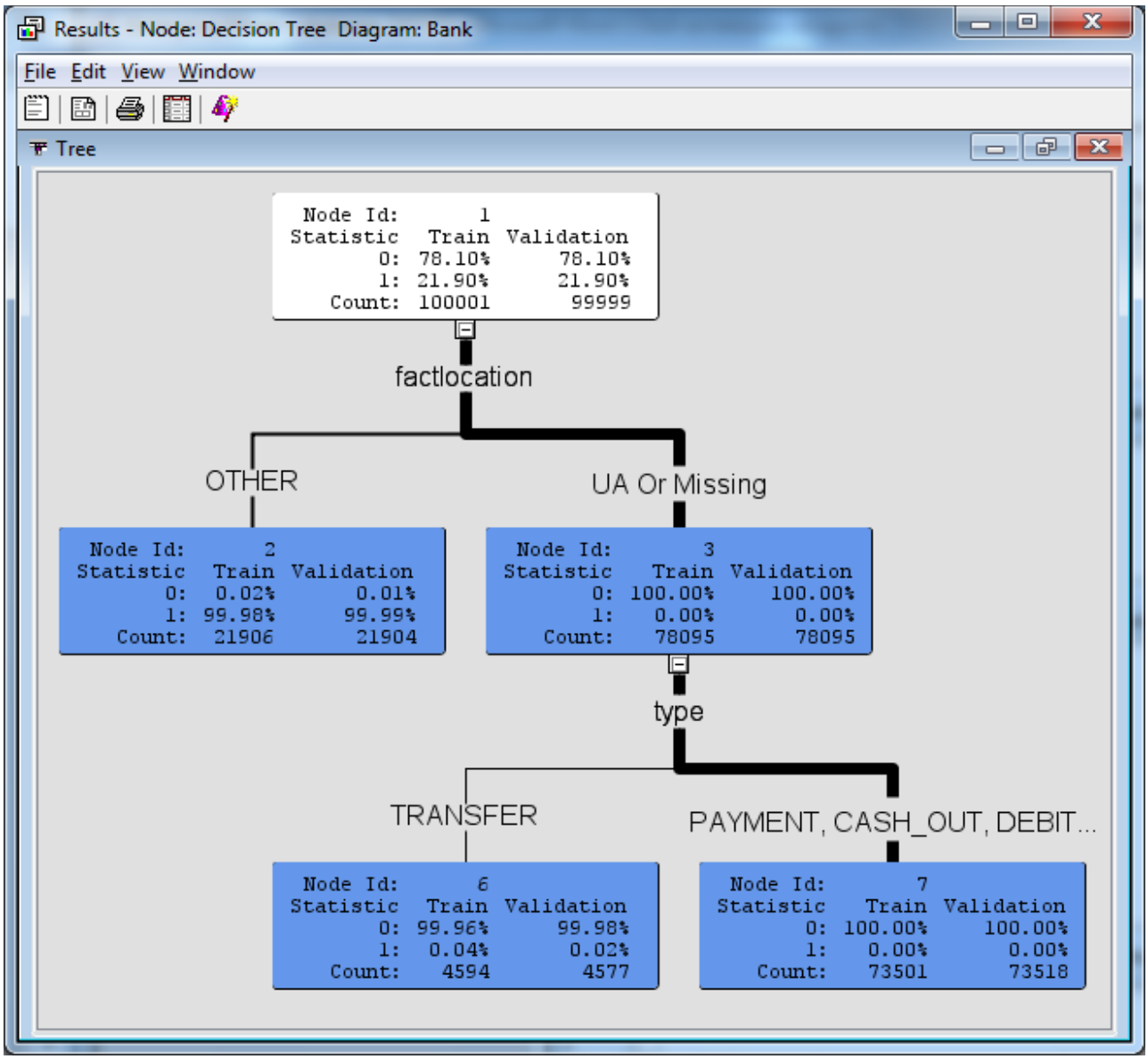


Рисунок 1.25 – Результат побудови дерева рішень

З побудованої діаграми дерева рішень (рис. 2.3) видно, що найбільш вагомий фактор – це ініційоване місцеположення пристрою, з якого виконувалась транзакція. Після нього за важливістю є тип операції, який здійснював клієнт банку.

Таким чином, найімовірніше виконана транзакція не містить ознак кіберзагроз, якщо фіксоване місцеположення виконання транзакції клієнтом банкінгу – Україна. А також з’ясовано, що безпечними для користувачів на

випадок наявності ознак кіберзагрози є наступні типи операцій: поповнення та зняття коштів, списання коштів з рахунку та проведення оплати.

На наступному кроці побудовано нейронну мережу. Результатом є мережа, яка складається з 1-го прихованого шару з двома нейронами (рис. 1.26). [17]

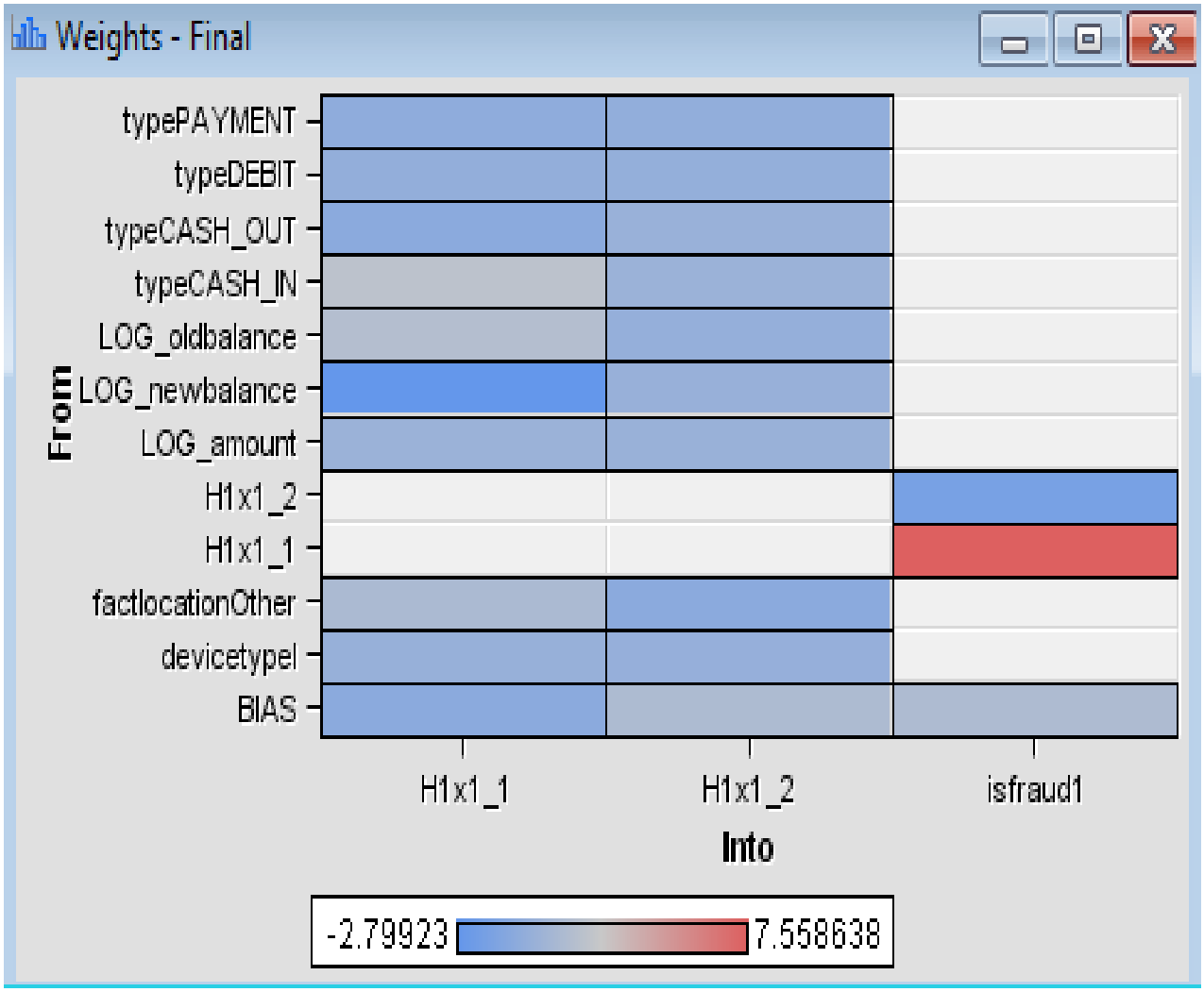


Рисунок 1.26 – Архітектура побудованої нейронної мережі

Отримані вагові коефіцієнти нейронної мережі представлено на рисунку 1.27.

Table: Weights - Final

Label	From	Into	Weight
LOG_amount -> H1x1_1	LOG_amount	H1x1_1	0.044417
LOG_newbalance -> H1x1_1	LOG_newbalance	H1x1_1	-2.79923
LOG_oldbalance -> H1x1_1	LOG_oldbalance	H1x1_1	1.360785
LOG_amount -> H1x1_2	LOG_amount	H1x1_2	-0.05355
LOG_newbalance -> H1x1_2	LOG_newbalance	H1x1_2	-0.11025
LOG_oldbalance -> H1x1_2	LOG_oldbalance	H1x1_2	-0.25139
devicetypel -> H1x1_1	devicetypel	H1x1_1	-0.13465
factlocationOther -> H1x1_1	factlocationOther	H1x1_1	0.867504
typeCASH_IN -> H1x1_1	typeCASH_IN	H1x1_1	1.775061
typeCASH_OUT -> H1x1_1	typeCASH_OUT	H1x1_1	-0.75885
typeDEBIT -> H1x1_1	typeDEBIT	H1x1_1	-0.34715
typePAYMENT -> H1x1_1	typePAYMENT	H1x1_1	-0.57974
devicetypel -> H1x1_2	devicetypel	H1x1_2	-0.23464
factlocationOther -> H1x1_2	factlocationOther	H1x1_2	-0.78262
typeCASH_IN -> H1x1_2	typeCASH_IN	H1x1_2	0.048199
typeCASH_OUT -> H1x1_2	typeCASH_OUT	H1x1_2	-0.0721
typeDEBIT -> H1x1_2	typeDEBIT	H1x1_2	-0.30449
typePAYMENT -> H1x1_2	typePAYMENT	H1x1_2	-0.39577
BIAS -> H1x1_1	BIAS	H1x1_1	-0.77711
BIAS -> H1x1_2	BIAS	H1x1_2	0.991864
H1x1_1 -> isfraud1	H1x1_1	isfraud1	7.558638
H1x1_2 -> isfraud1	H1x1_2	isfraud1	-1.75976
BIAS -> isfraud1	BIAS	isfraud1	1.022777

Рисунок 1.27 – Вагові коефіцієнти нейронної мережі

Математичну інтерпретацію отриманої нейронної мережі наведено у формулах 1.2-1.4:

$$Y = 1{,}02 + 7{,}56 \cdot H_1 x_1 - 1{,}76 \cdot H_2 x_2; \tag{1.2}$$

$$H_1 = \tanh(-0{,}78 + 0{,}04 \cdot LOGX_1 - 0{,}13 \cdot X_{2.2} + 0{,}87 \cdot X_{3.2} - 2{,}8 \cdot LOGX_5 + 1{,}36 \cdot LOGX_6 + 1{,}78 \cdot X_{7.1} - 0{,}76 \cdot X_{7.2} - 0{,}35 \cdot X_{7.3} - 0{,}58 \cdot X_{7.4}); \tag{1.3}$$

$$H_2 = \tanh(0{,}99 - 0{,}05 \cdot LOGX_1 - 0{,}23 \cdot X_{2.2} - 0{,}78 \cdot X_{3.2} - 0{,}11 \cdot LOGX_5 - 0{,}25 \cdot LOGX_6 + 0{,}05 \cdot X_{7.1} - 0{,}07 \cdot X_{7.2} - 0{,}3 \cdot X_{7.3} - 0{,}4 \cdot X_{7.4}). \tag{1.4}$$

Отримана нейронна мережа показує, що на ймовірність того, що банківська транзакція буде мати ознаки кіберзагрози, впливає: місцеположення пристрою, з якого проводилась транзакція – інша країна ($X_{3.2}$); баланс клієнта після

проведення транзакції (X_5) та до проведення (X_6); загальна сума транзакції (X_1); тип пристрою – Інтернет-банкінг ($X_{2.2}$); типи транзакцій – поповнення коштів ($X_{7.1}$), зняття коштів ($X_{7.2}$), списання коштів з рахунку ($X_{7.3}$), проведення оплати ($X_{7.4}$).

Для вибору найбільш точної моделі використано частку неправильної класифікації та середньоквадратичної похибки (табл. 1.5). [17]

Таблиця 1.5 – Порівняльна характеристика моделей

№ з/п	Модель	Частка неправильної класифікації (Misclassification Rate, MISC)		Середньоквадратична похибка (Mean Square Error, MSE)	
		Валідаційна	Навчальна	Валідаційна	Навчальна
1	Нейронна мережа	0,00002	0,00005	0,001094	0,001105
2	Дерево рішень	0,00003	0,00009	0,001097	0,001112
3	Логіт-регресія	0,00003	0,0001	0,001091	0,001119

Моделі, представлені в таблиці 1.5, розташовані від найкращої до найгіршої за кількісними оцінками частки неправильної класифікації та середньоквадратичної похибки. Модель тим краще описує набір даних, чим менші значення цих показників. Найточнішою моделлю виявилась нейронна мережа, оскільки її представлені показники мають найнижчі значення. Інші моделі є також досить точними – їх значення наближаються до 0.

Результат розрахованих значень коефіцієнтів підкріплюється графіками ROC-кривих. На рисунку 1.28 відображено ROC-криві для навчального та валідаційного наборів даних. Синьою лінією зображено криву дерева рішень, червоною – регресії, а зеленою – нейронної мережі. Чим більше крива віддаляється від базової лінії, тим краще модель класифікує дані, тобто прогнозує ймовірність виникнення ознаки кіберзагрози. Представлені на рисунку ROC-криві моделей накладаються одна на одну, що свідчить про приблизно однакову якість класифікації моделей.

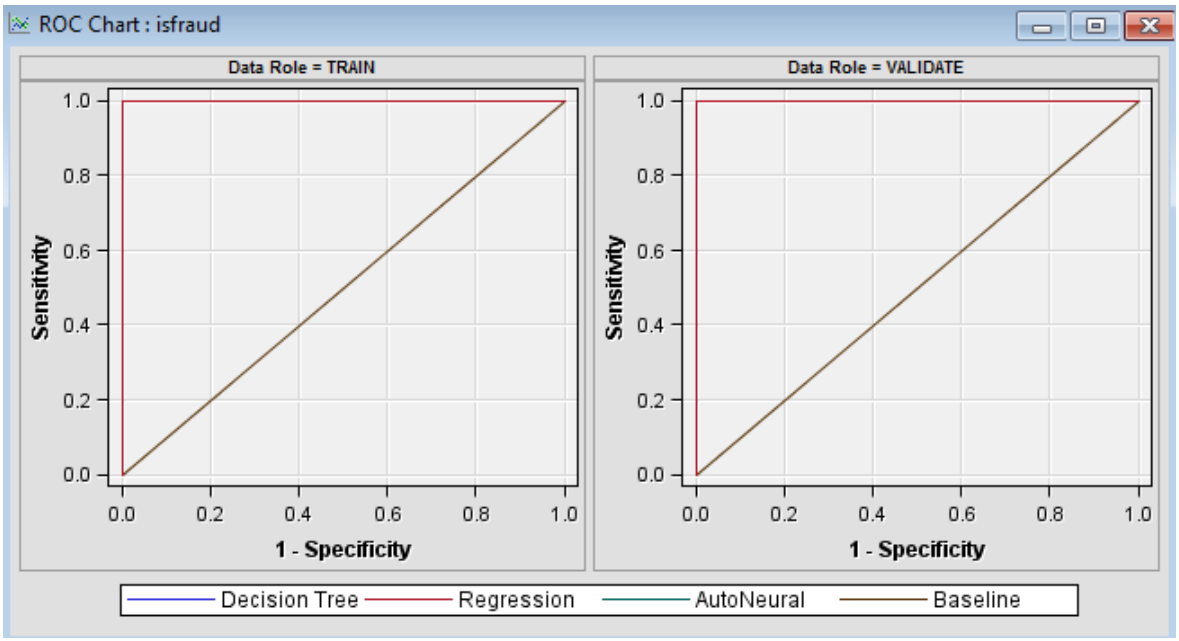


Рисунок 1.28 – ROC-криві дерева рішень, регресії та нейронної мережі

Оскільки нейронна модель є більш точнішою та враховуючи властивість адаптивності нейронних мереж до змін, оберемо її для перевірки на адекватність. З цією метою на новому наборі вхідних даних проведемо розрахунки та порівняємо характеристики класифікаційних властивостей нейронної мережі (табл. 1.6).

Таблиця 1.6 – Характеристика класифікаційних властивостей нейронної мережі

Цільова змінна	Результат	Цільова змінна, %	Результат, %	Частота випадків	Загальна класифікація, %
Навчальна вибірка					
0	0	99,9949	99,9987	78096	78,0952
1	0	0,0051	0,0183	4	0,0040
0	1	0,0046	0,0013	1	0,0010
1	1	99,9954	99,9817	21900	21,8998
Валідаційна вибірка					
0	0	99,9987	99,9987	78095	78,0958
1	0	0,0013	0,0046	1	0,0010
0	1	0,0046	0,0013	1	0,0010
1	1	99,9954	99,9954	21902	21,9022

Результати в таблиці 1.6 показують, що модель на навчальній вибірці вірно класифікує 99,99% транзакцій, які не мають ознаки кіберзагрози, та 99,98%

транзакцій, які мають ці ознаки. Однак, модель класифікувала 0,018% транзакцій, що мали ознаки кіберзагрози, як ті, що не мають таких ознак, і 0,001% транзакцій, які не виявились кіберзагрозами, було класифіковано, як ті, що є кіберзагрозами. Щодо абсолютних величин, то модель правильно класифікувала 78096 транзакцій, як ті, що не мають ознак кіберзагрози, та 21900, як ті, що мають. Неправильно класифіковано всього 5 транзакцій. Тобто, частка неправильної класифікації не перевищує 5%.

У результаті проведеного дослідження було побудовано логіт-регресію, нейронну мережу і дерево рішень. Проаналізовано їх результати та встановлено, що усі побудовані моделі майже однаково точно описують вхідні дані, проте найбільш точною виявилась модель нейронної мережі, яка пройшла перевірку на адекватність.

Нейронна мережа, як і будь-яка інша модель, потребує постійного оновлення та удосконалення у зв’язку з появою нових ознак загроз для банківських клієнтів. Тому необхідно постійно доповнювати вибірку даних актуальною інформацією про виконані користувачами транзакції.

Застосування отриманої моделі на практиці допоможе працівникам банківського сектору виявляти в транзакціях ознаки кібернетичних загроз, тим самим попереджаючи користувачів мобільного та інтернет-банкінгу від можливих збитків, завданих злочинними діями. Інтеграція моделі в існуючу систему кіберзахисту банку дозволить проводити регулярний моніторинг транзакцій на предмет наявності ознак кіберзагроз, сприятиме підвищенню рівня довіри клієнтів до банків через підвищення захищеності та надійності.

Пункт 1.2.1 цього звіту було виконано із використанням матеріалів проміжного звіту про НДР [11] та публікацій виконавців [17, 18].

1.2.2 Розробка математичних портретів потенційних жертв та шахраїв

Для дослідження даної проблематики було взято статистичні дані по шахрайствам в Великій Британії за 2015-2018 роки за різними видами фінансових продуктів. Статистика була надана агентством звітності споживчого кредитування “Experian”, яке збирає та обробляє інформацію про понад мільярд людей та підприємств по всьому світу та входить в трійку найбільших кредитних бюро США. На жаль аналітичні агентства та банки України не публікують подібного роду статистику в періодиці або в офіційних виданнях. Тому в даному досліджені буде представлений узагальнений підхід до моделювання портретів потенційного шахрая та жертви, виконаний на прикладі даних Великої Британії, який можна застосовувати для формування таких портретів в різних країнах та з урахуванням їх умов.

Для дослідження було використано статистику за двома основними групами шахраїв. Перша група включає в себе осіб, які є споживачами послуг банків чи фінансово-кредитних компаній, тобто шахраї від першої сторони – безпосередні учасники. Шахрайство починається тоді, коли клієнт не має наміру в подальшому погасити виплати за фінансовим продуктом. Саме в цьому намірі й полягає найбільша різниця між кредитним ризиком та ризиком не повернення коштів в результаті шахрайства. Кредитний ризик включає клієнтів, які отримали товари чи послуги з наміром їх погасити, але просто не мають ресурсів для виконання своїх зобов'язань в зв’язку з непередбачуваними для них самих обставинами. За другим варіантом людина цілеспрямовано не віддає кошти. Такий вид шахрайства може включати широкий спектр тактик. Наприклад, коли одна особа передає відповідальність за виплату коштів на іншу особу. Тобто шахрай дуже гарно знає особу, на яку оформлює кредит, за виплату якого буде відповідати жертва, а не шахрай. Найуспішними шахрайствами є випадки, коли шахраї поєднуються з хорошими клієнтами, які мають гарну кредитну історію, що створює підґрунтя для довгострокових масштабних шахрайств. [19]

Другу групу складають шахрайства від третьої сторони, тобто від осіб, які не пов’язані ні з провайдером фінансово-кредитних послуг, ні з їх клієнтами. Таке шахрайство здійснюється сторонніми особами шляхом використання фальшивих ідентифікаційних документів, без відома особи, чия особа використовується для здійснення шахрайства. Сюди ж відноситься шахрайська діяльність, пов’язана з незаконним отриманням конфіденційних даних клієнтів банків, ПІН-кодів та CVV2-кодів банківських карток, логінів та паролів від інтернет-банкінгу, заволодівання мобільними фінансовими номерами клієнтів, за якими здійснюється аутентифікація, тощо. У випадку шахрайства від третьої сторони вкрай складно визначити особу самого шахрая, відслідкувати його місцезнаходження. Тому такі види шахрайств є найбільш популярними, оскільки зловмисники часто залишаються не спійманими. [20]

Так, розподіл шахрайств від першої сторони за видами фінансових продуктів в Великій Британії за 2015-2018 роки представлений на рисунку 1.29. [21]

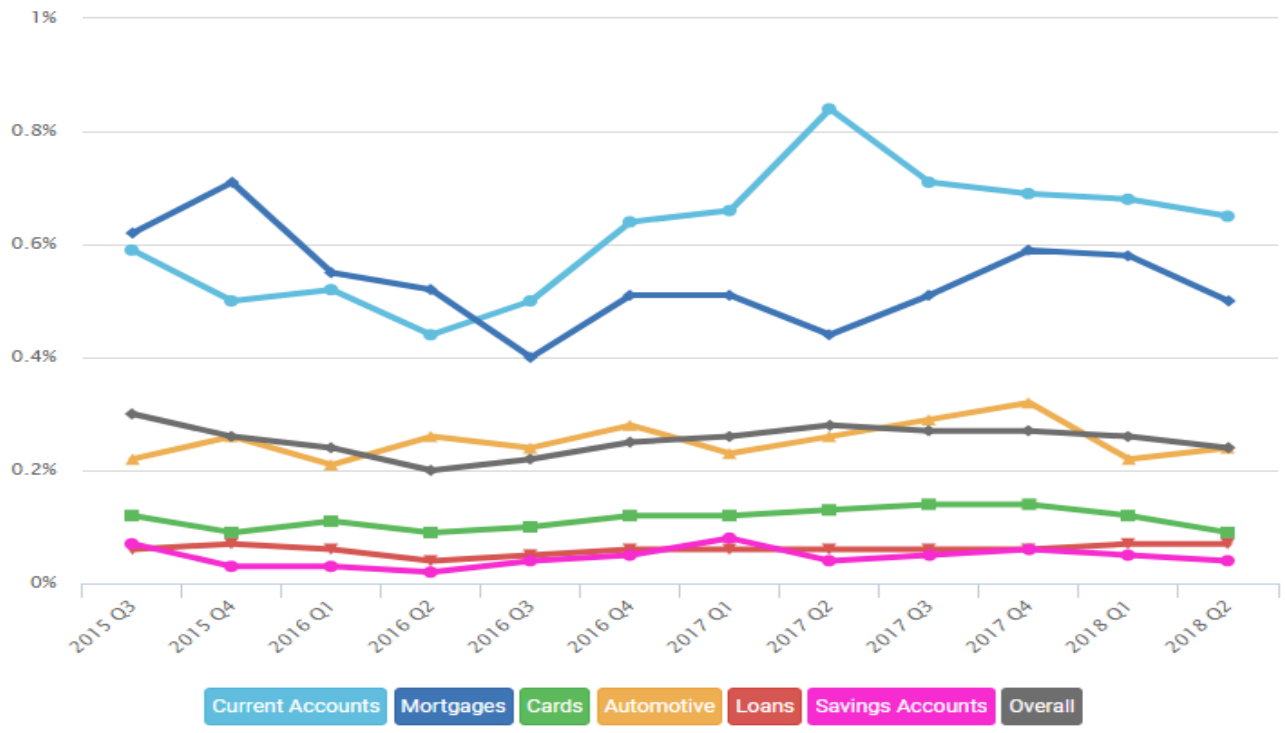


Рисунок 1.29 – Розподіл шахрайств від першої сторони за видами фінансових продуктів в Великій Британії за 2015-2018 роки

Шахрайства від першої сторони найбільш ймовірно припадають на шахрайства з поточними банківськими рахунками (Current Accounts) та іпотеку (Mortgages) (рис. 1.29). В даному випадку розглядається традиційне іпотечне шахрайство, яке включає в себе заходи, спрямовані на те, щоб обдурити кредитора, наприклад, намагання шахраєм отримати кредит, на який він не може законно претендувати, коли позичальники хибно представляють свою фінансову інформацію. [22]

Що стосується шахрайств від третьої сторони, то вони здійснюються переважно над поточними рахунками клієнтів (Current Accounts). Також популярними є шахрайства з банківськими картками (Cards) та ощадними рахунками (Saving Accounts) (рис. 1.30).

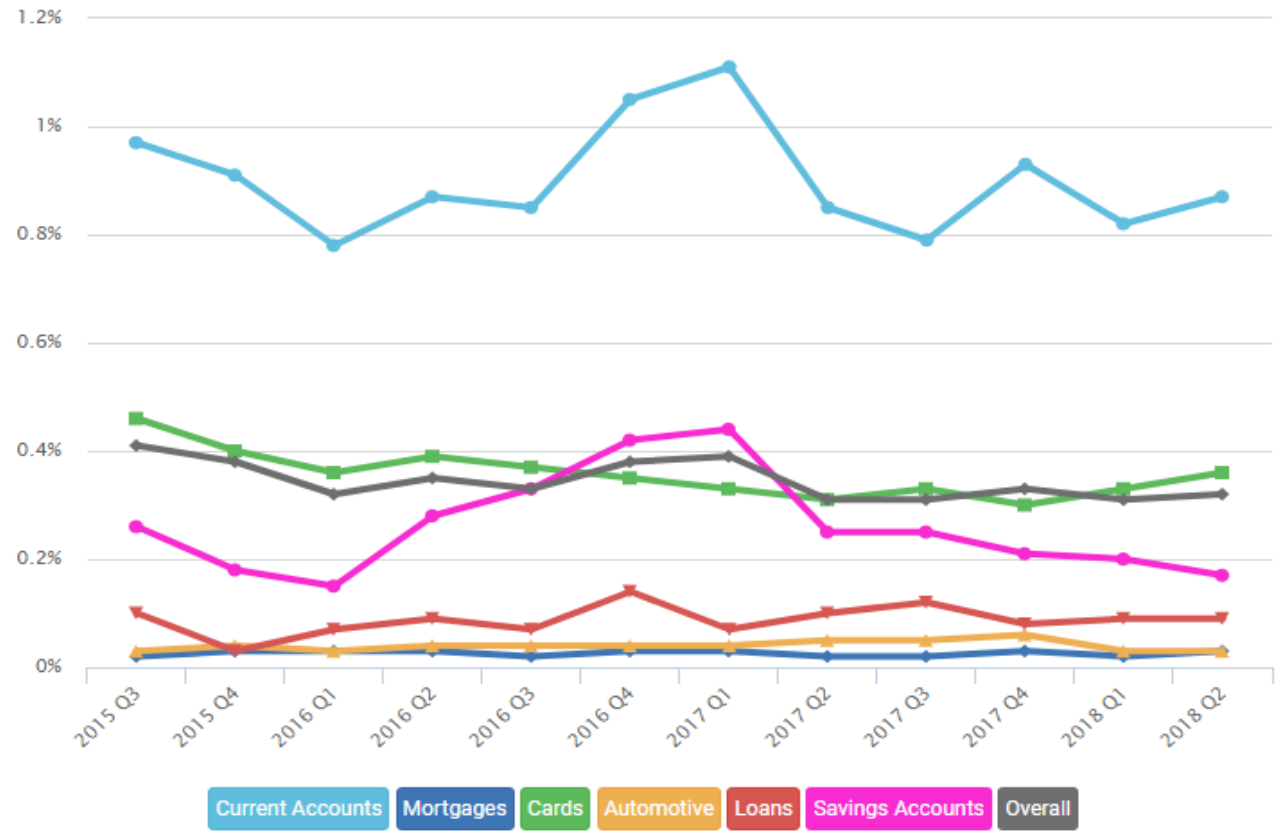


Рисунок 1.30 – Розподіл шахрайств від третьої сторони за видами фінансових продуктів у Великій Британії за 2015-2018 роки

Тобто шахраї можуть отримати доступ до рахунку клієнта шляхом застосування методів соціальної інженерії, що є найбільш популярним способом шахрайства. Також можливі випадки, коли ідентифікаційні дані клієнта викрадаються з бази даних банку. Відомі випадки, коли банківські працівники продавали бази даних стороннім особам, за рахунок чого шахраї отримували доступ до даних клієнтів. Тут певну роль відіграє нехтування клієнтами елементарних правил безпеки власних конфіденційних даних, їх необережність при здійсненні розрахункових операцій та довірливість. За останні три роки шахрайства від третьої сторони переважають над шахрайствами від першої. У 2017 році співвідношення шахрайств від першої сторони до шахрайств від третьої складає 44%, а шахрайств від третьої сторони до шахрайств від першої – 56%, тоді як ще в 2014 році ситуація була протилежною. Можна припустити, що це пов’язано з більш масовим використанням Інтернет-технологій для здійснення банківських операцій, оскільки в просторах Інтернету набагато складніше забезпечити максимальну конфіденційність даних.

Використовуючи статистику по розподілу шахраїв від першої сторони на групи за віком, статтю та соціальним статусом, а також статистику по жертвах шахрайств з боку третьої сторони за такими ж параметрами, авторами побудовано два ймовірнісні дерева, які являють собою змодельовані портрети потенційного шахрая від першої сторони та потенційної жертви шахрайств з боку третіх сторін.

Дерево ймовірностей – це модель, яка широко застосовується для прийняття рішення, та складається з вузлів, які відповідають моменту настання події, в нашому випадку – здійснення шахрайства з фінансовими продуктами. Гілки дерева – це можливі варіанти розвитку події, кожна зі своєю ймовірністю.

На першому етапі побудови дерева розподіляємо клієнтів (потенційних шахраїв) за статтю. Ймовірності для гілок будуть дорівнювати: 68,9 % – ймовірність першого варіанту розвитку подій, при якому шахрай виявиться чоловіком (Male); 31,1 % – ймовірність того, що шахраєм буде жінка (Female).

На наступному етапі враховуємо розподіл шахраїв за віковими групами (Age). Ймовірність кожної наступної гілки отримуємо, як добуток ймовірностей

фактору статі до ймовірності кожної з вікових груп. На другому етапі отримуємо з двох гілок – двадцять, за різними варіантами розвитку подій. На третьому етапі аналогічним чином уточнюємо модель, включивши фактор приналежності до однієї з 15 соціальних груп. В результаті отримали дерево, в якому буде 300 гілок, тобто ми змоделювали 300 можливих варіантів розвитку подій і розрахували їх ймовірності.

Побудоване дерево рішень, тобто модель потенційного шахрая від першої сторони за ознаками статі, віку та соціальної групи, представлено на рисунку 1.31. В матриці результатів моделі її елементи мають різні кольори у відповідності із рівнем ймовірності: зелений колір – найменша ймовірність шахрайства, жовтий – середня, червоний – найвищий рівень ймовірності шахрайства. В результаті побудованої моделі шахрая (рис. 1.31) отримано, що найбільш схильною до шахрайства групою клієнтів є чоловіки у віці від 25 до 29 років, які мешкають в мультикультурних кварталах міста. Ця група складає 2,14% від усіх шахраїв і є найбільш ризикованою групою клієнтів для банків та інших фінансово-кредитних організацій. Також до великої схильності шахрайства можна віднести чоловіків у віці від 30 до 34 років, що також мешкають у містах, чоловіків у віці 25-29 років, які наймають помешкання. Серед жінок можна виділити групи у віці 25-29 років та 30-34 років, що також мешкають в мультикультурних кварталах міста або наймають житло. Це можливо пояснити за рахунок того, що люди у віці 25-34 ще можливо не мають стабільного кар’єрного зросту, постійного місця проживання, тому й стикаються з певними фінансовими труднощами, які схиляють їх до шахрайств.

Найменша ймовірність того, що шахраєм виявиться жінка або чоловік у віці від 50 років, які відносяться до соціальної групи «Senior security», тобто подружні жінки та чоловіки, які живуть окремо від своїх дітей у власних зручних приватних будинках і мають достатній рівень фінансової забезпеченості для спокійного та розміреного життя. Лише 0,03% шахрайських випадків з боку клієнтів фінансових установ здійснюються представниками цієї групи.

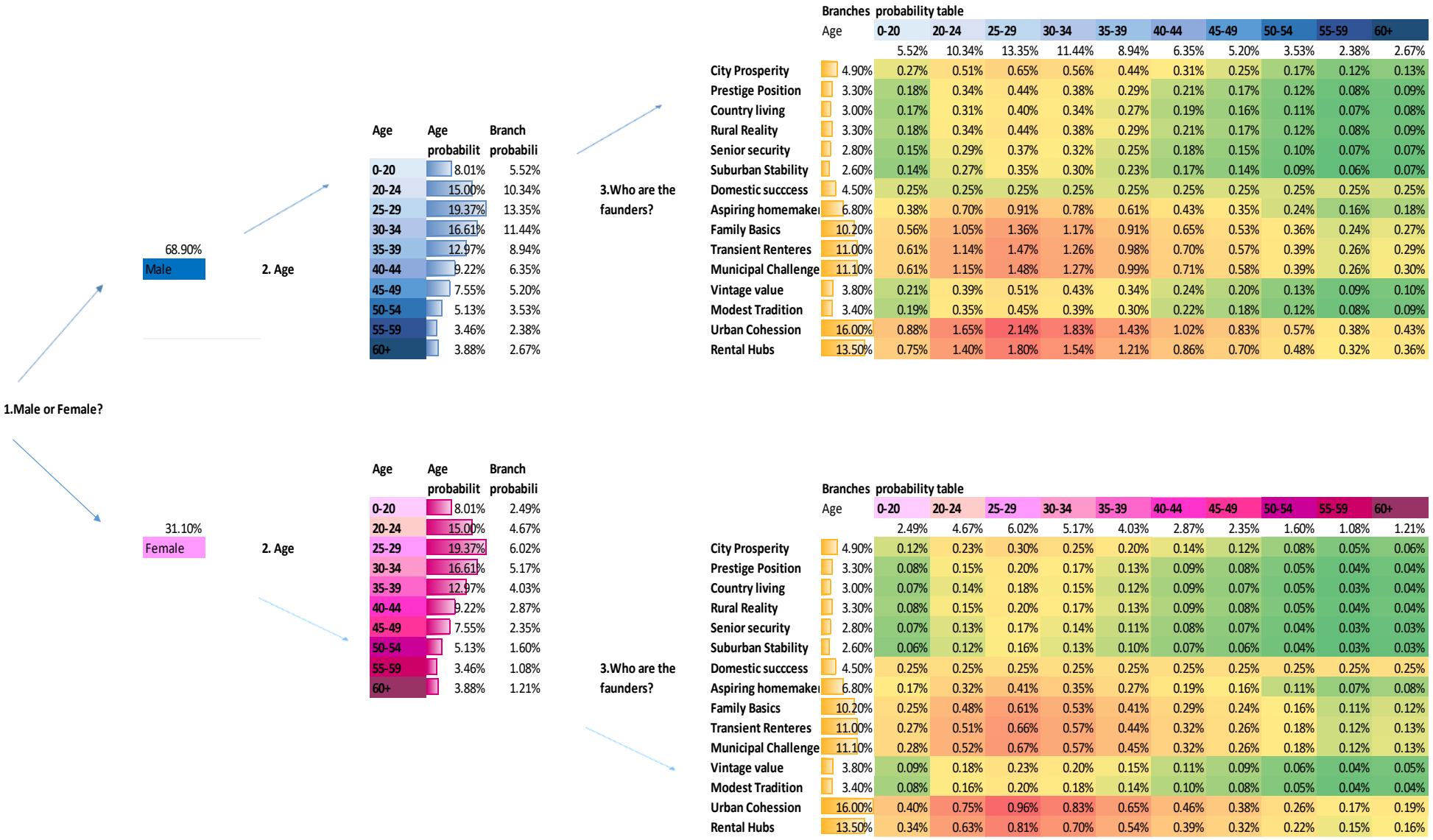


Рисунок 1.31 – Модель портрету потенційного шахрая від першої сторони за ознаками статі, віку та соціальної групи [23]

Такий же відсоток шахрайств припадає на жінок та чоловіків, що класифікуються як «Country living» (доброзичливі домовласники, які живуть в сільській місцевості, часто фермери), «Suburban Stability» (домовласники, що мають заміську нерухомість), «Sity Prosperity» (міські жителі із стабільним середнім доходом); «Prestige Position» (міські жителі із високим доходом).

Отримана модель дає можливість швидко визначити рівень ймовірності шахрайства для тієї чи іншої особи-клієнта враховуючи три основні фактори: стать, вік та соціальну групу. Вона може бути корисною при прийнятті рішення про видачу позики, реалізації будь-яких ризикованих фінансових операцій, для забезпечення яких може використовуватися нерухомість, тощо. При впровадженні даної моделі у практичну діяльність банк може самостійно відслідковувати різні групи та ознаки, за якими може бути виникати шахрайство.

Результат побудованої моделі потенційного жертви шахрайства від третьої сторони за ознаками статі, віку та соціальної групи, представлено на рисунку 1.32. Отримана модель вказує на те, що найбільше від сторонніх шахраїв потерпають чоловіки в віці 25 - 44 років, які відносяться до соціальної групи «Rental Hubs» – переважно молоді, одинокі люди, та люди середнього віку, які живуть у міських поселеннях та орендують свої будинки, перебуваючи на ранній або середній стадіях своєї кар'єри або продовжують навчання.

Схожі результати й для жінок, які знаходяться у віці 25 - 39 років та також орендують житло. Це можна пояснити більшою фінансовою активністю даної групи людей, які частіше здійснюють будь-які фінансові операції через Інтернет або мобільні пристрої, частіше користуються послугами фінансово-кредитних організацій, онлайн-сервісами, програмними додатками.

Найменша ймовірність бути жертвою шахрая є у чоловіків та жінок у віці до 20 років за різними соціальними групами. Це пов’язано з тим, що ця група – це молоді люди, які ще навчаються у навчальних закладах, коледжах та не мають самостійності у фінансах.

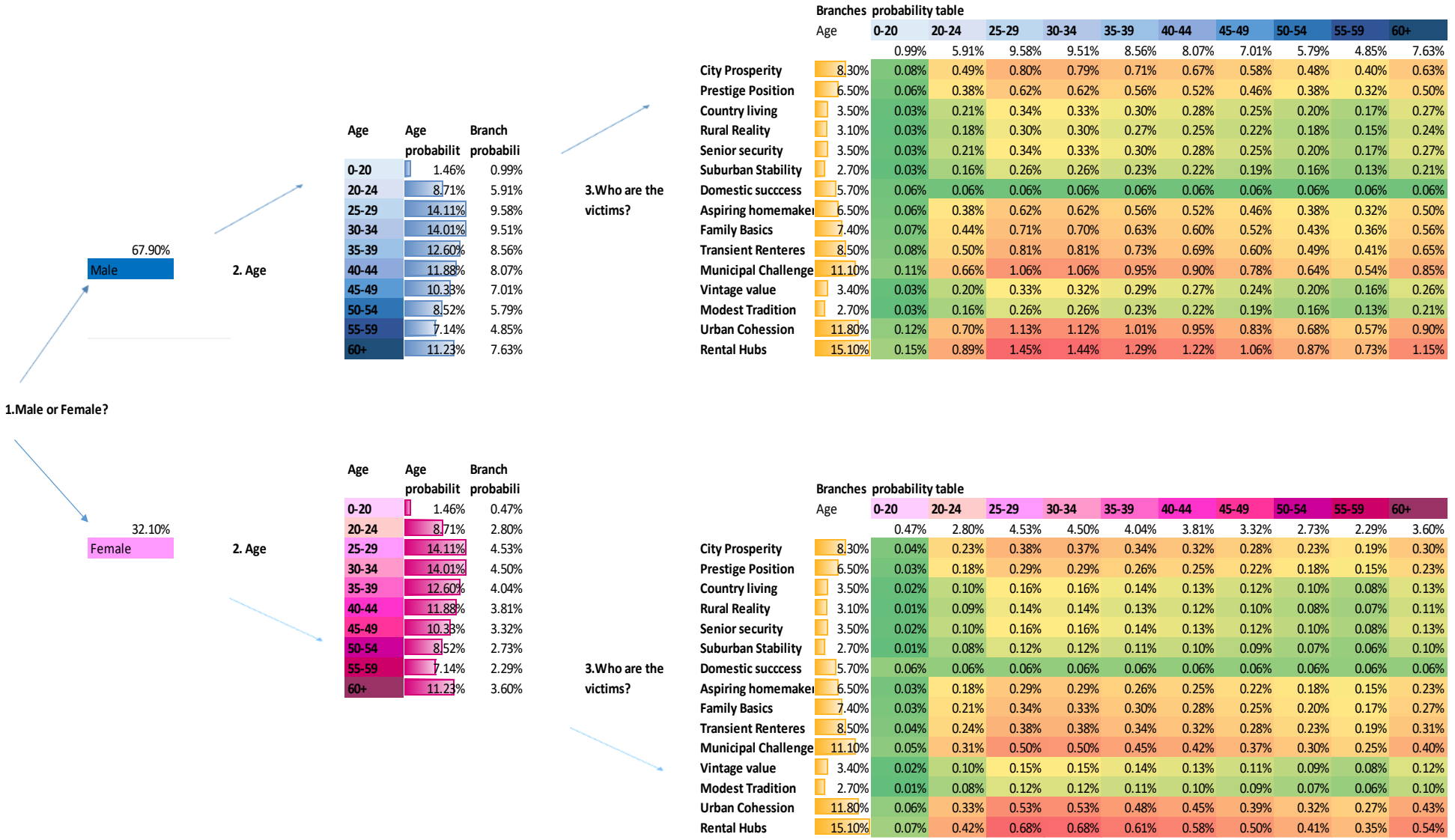


Рисунок 1.32 – Модель портрету потенційної жертви шахрайства від третьої сторони за ознаками статі, віку та соціальної групи [23]

Найменша ймовірність з даної групи бути жертвою шахрая, це жінки з соціальної групи «Modest Tradition», які живуть в приватних недорогих будинках, в скромних сім'ях, та вже давно прижились на певній території.

Розроблена модель допомагає вирізнити тих клієнтів, для яких потрібно посилити систему безпеки за всіма видами банківських продукті, особливо банківських карт, поточних та ощадних рахунків, щоб уникнути небажані збитки. Можливе також введення додаткових заходів для інформування клієнтів про найпоширеніші актуальні схеми банківських шахрайств. Дану методику побудови портретів шахраїв можна використати й в роботі українських банків. Ймовірно, що портрети будуть відрізнятися, оскільки співвідношення віку, статі та фінансової стабільності клієнта є різними для громадян з розвинутої країни та країни, що розвивається. Але застосування цієї методики дозволить вже на етапі здійснення операції визначити потенційного шахрая чи жертву. Це призведе до коригування інструкцій в банках та зменшить навантаження на людину в процесі прийняття рішення.

Для ефективної взаємодії фінансово-кредитних установ та їх клієнтів, та для зменшення ймовірності отримати збитки від шахрайських операцій, необхідно застосовувати нові інструменти. В якості такого інструменту може виступати побудова моделей потенційних шахраїв та жертв банківських шахрайств. Портрети представляють собою моделі дерева рішень, які дозволяють визначити ймовірність шахрайства у відповідності з рядом ознак. Методика є вкрай простою та може враховувати не тільки вік, стать, соціальне становище, але й способи здійснення операцій (Інтернет, мобільний телефон, тощо), історію клієнта, місце здійснення операції, та інше. Оскільки шахраї вдосконалюють свої інструменти, відповідно банківські підрозділи кіберзахисту повинні швидко реагувати на ці зміни. Це можливо, якщо банки будуть використовувати математичні методи для розробки алгоритмів моніторингу, перевірки клієнтів та операцій на предмет виникнення ймовірності шахрайства. Отримані результати повинні накопичуватися та формувати банк даних, використання якого надасть можливість оперативно

оновлювати інформацію щодо шахрайств та модернізовувати портрети. В свою чергу, це сприятиме більш ефективному прийняттю рішення з боку банківського персоналу та попередженню шахрайства.

Пункт 1.2.2 цього звіту було виконано із використанням матеріалів проміжного звіту про НДР [11] та публікацій виконавців [18, 23].

1.2.3 Розробка інформаційної моделі виявлення ознак шахрайств у банках

Розглянемо банк як складну систему, складовими якої виступають внутрішнє середовище: персонал, менеджмент банку, його власники, автоматизована банківська система (АБС); та зовнішнє середовище: клієнти, кіберзлочинці, пов’язані особи, програмно-технічні пристрої. Тобто банк є системою взаємозв’язаних суб’єктів та об’єктів внутрішнього та зовнішнього середовища. До складу системи будь-якої природи входять елементи різного рівня надійності, або які можуть вторгнутися в певний момент за певних умов, що може призвести до негативних наслідків. По суті кожен з цих елементів може стати джерелом потенційного шахрайства або ініціатором, або співучасником, або бути опосередковано залученим. Різні дослідження в сфері банківського шахрайства розглядають в основному зовнішнє середовище, як ініціатора шахрайства, що є не зовсім коректно. 80% від усього обсягу шахрайства пов’язано із персоналом банку. Тому можливості вторгнення повинні враховувати також і внутрішні аспекти загрози.

Отже, при окресленні банківської системи будемо користуватись принципом професійного песимизму, яким керуються аудитори, і який не виключає зловживань на будь-якому робочому місці банку та не виключає ймовірності вторгнення сторонніх осіб задля здійснення шахрайства або шкоди. Тобто, шахрайство може бути здійснено будь-ким, будь-де та з використанням

будь-яких інструментів та способів. Відповідно система повинна враховувати зміни негативного характеру та реагувати на них. Виходячи з цього, представляємо архітектуру АБС з урахуванням модулю моніторингу, який є центральною ланкою, що пов'язує інформаційні потоки, які генерують суб'єкти та об'єкти зовнішнього та внутрішнього середовища (рис. 1.33).

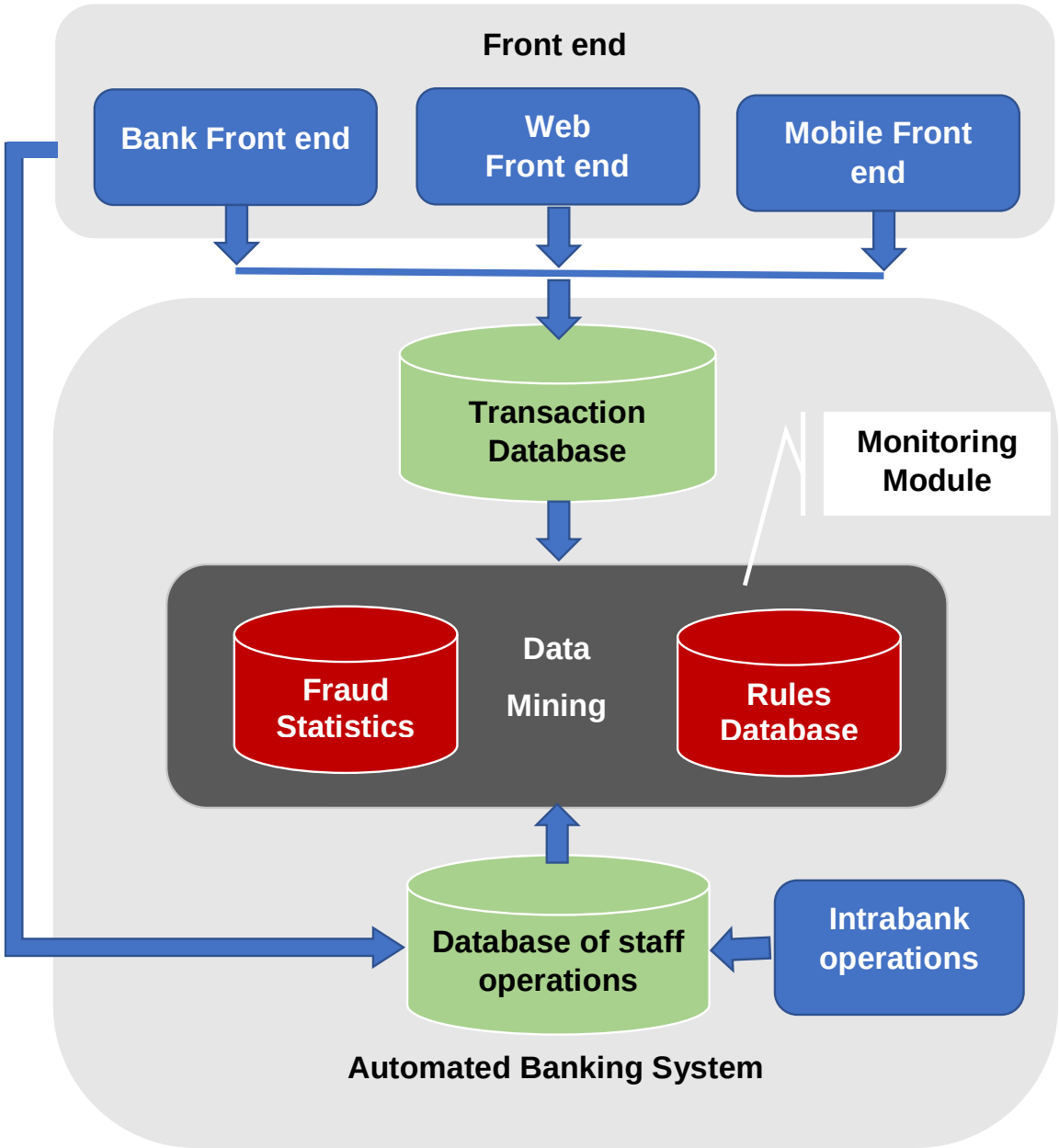


Рисунок 1.33 – Архітектура автоматизованої банківської системи з урахуванням модулю моніторингу [24]

Система повинна передбачати ймовірність шахрайства, виявляти та попереджувати. Тому доцільно, що така система буде мати модуль моніторингу “Monitoring Module”, побудований за принципами застосування методів інтелектуального аналізу “Data Mining” та створення бази даних із статистикою шахрайств “Fraud Statistics” й бази правил (критеріїв) для відслідковування ознак шахрайств “Rules Database” (рисунок 1.33). Його головне призначення – виявляти потенціальні шахрайства незалежно від природи ініціатора (зовнішнього – клієнта банку та його операцій “Transaction Database”, чи внутрішнього – персоналу банку та його операцій “Database of Staff Operation”). Операції перевіряються на відповідність певним критеріям, які визначають, чи має операція ознаки шахрайської, які сформовані у базі правил з урахуванням накопичених статичних даних щодо шахрайства.

Відповідно до запропонованої структури АБС побудуємо інформаційну модель виявлення ознак шахрайств для операцій, ініційованих зовнішнім середовищем, яка відображає інформаційні потоки, що будуть функціонувати у середовищі АБС, а саме у модулі моніторингу (рисунок 1.34). [24]

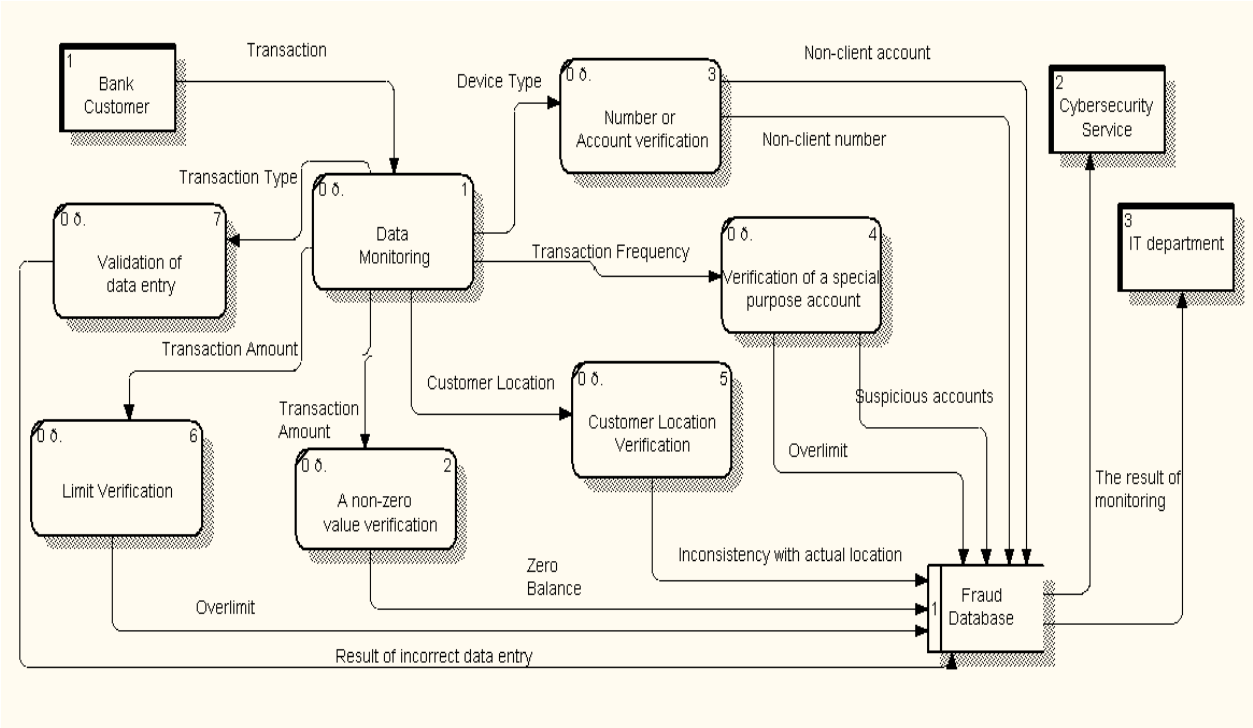


Рисунок 1.34 – Інформаційна модель виявлення ознак шахрайств клієнтів

Модель побудовано у нотації DFD (data flow diagrams) [25], яка є одним із інструментів структурного моделювання та проектування інформаційних систем, із використанням програмного забезпечення “All Fusion Process Modeller”. DFD-модель дозволяє описати потоки даних.

Побудована на рисунку 1.34 модель відображає інформаційні потоки, які будуть задіяні в модулі моніторингу для виявлення ознак шахрайств та їх попередження. Це відбувається шляхом перевірки банківської транзакції (“Transaction”), яку здійснює клієнт (сутність “Bank Customer”), із використанням функцій “Data Monitoring”.

Перевіряються:

– суми транзакцій (“Transaction Amount”) на предмет обнуління рахунку (“A non-zero value verification”). Частіше всього шахрай в процесі шахрайської операції знімає усі кошти з рахунку, що ймовірніше за все не є типовим для власника рахунку. В результаті отримується інформація про те, що на рахунку нульовий баланс “Zero Balance”;

– суми транзакцій (“Transaction Amount”) на перевищення встановлених лімітів (“Limit Verification”). В процесі шахрайства операції можуть перевищувати встановлені банком або клієнтом ліміти “Overlimit”, що дозволить сигналізувати про спробу здійснення незаконної операції;

– локації клієнта (“Customer Location Verification”), оскільки операція може здійснюватися з будь-якої країни, міста та може не відповідати фактичній геолокації клієнта;

– рахунку цільового призначення (“Verification of a special purpose account”). Рахунок може бути в “чорному списку” клієнтів (“Suspicious accounts”) або може бути перевищення лімітів по сумі транзакції (“Overlimit”), якщо цільовий рахунок відкрито в іншому банку;

– номера та аккаунти клієнта (“Number or Account verification”) в залежності від типу пристрою (“Device Type”), з якого ініціюється операція. У випадку, коли операцію намагаються здійснити з номера та аккаунта, які не належать клієнту (“Non-client account” та “Non-client number”);

– правильності введених даних (“Validation of data entry”) в залежності від типу транзакції (“Transaction Type”). Результати неправильних спроб (“Result of incorrect data entry”) можуть сигналізувати про ймовірне зламування акаунту клієнта.

Інформація щодо ймовірні порушення, шахрайства, зламування надходить до бази даних шахрайств (“Fraud Database”), обробляється. Результати моніторингу (“The Result of Monitoring”) передаються відділам IT (“IT Department”) та кібербезпеки банку (“Cybersecurity Service”).

У відповідністю із запропонованою інформаційною моделлю (рисунок 1.34) розроблено схему процесу здійснення операції клієнтом з урахуванням її перевірки на ознаки шахрайства у нотації BPMN 2.0 (Business Process Model and Notation) [26] із використанням програмного забезпечення “Bizagi Modeller” (рисунок 1.35).

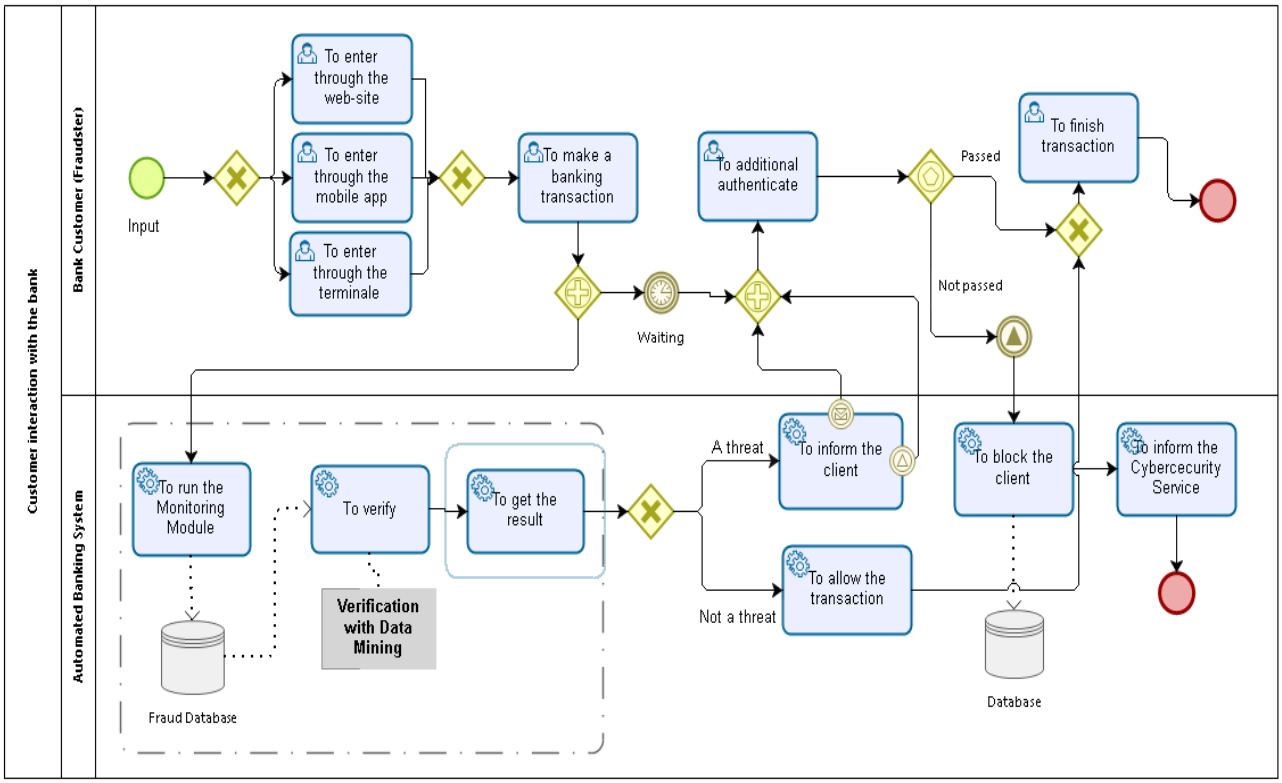


Рисунок 1.35 – Схема процесу здійснення операції клієнтом банку [24]

Процес виглядатиме наступним чином (рисунок 1.35):

1) клієнт банку або потенційний шахрай (“Bank Customer (Fraudster)”) здійснює вхід до системи або з використанням веб-сайту, або мобільного пристрою, або терміналу;

2) клієнт банку або потенційний шахрай здійснює операцію (“To make a banking transaction”);

3) АБС (“Automated Banking System”) перевіряє операцію на наявність ознак шахрайства із застосуванням модулю моніторингу, в якому реалізовано методи інтелектуального аналізу (“Verification with Data Mining”). Перевірка проводитиметься за тими критеріями, які представлені на рисунку 1.35, та які сформовані у базі даних (“Fraud Database”);

4) якщо результат перевірки не виявляє ознак потенційного шахрайства, то система дозволяє здійснити операцію (“To allow the transaction”) та клієнт її завершує (“To finish the transaction”);

5) якщо результат перевірки виявляє ознаки шахрайства, система робить запит на підтвердження операції шляхом sms-повідомлення або дзвінка, або іншим способом (“To inform the client”);

6) клієнт здійснює додаткову аутентифікацію (“To additional authenticate”);

7) якщо операція була ініційована клієнтом, то її успішно буде завершено;

8) у випадку, якщо клієнт виявиться шахраєм, тобто він не зможе пройти додаткову аутентифікацію, то його буде заблоковано (“To block the client”) та проінформовано систему безпеки (“To inform the Cybersecurity Service”).

Що стосується випадків внутрішніх шахрайств, то було розроблено інформаційну модель виявлення шахрайства, якщо шахраєм виступає персонал банку, у нотації DFD (рисунок 1.36).

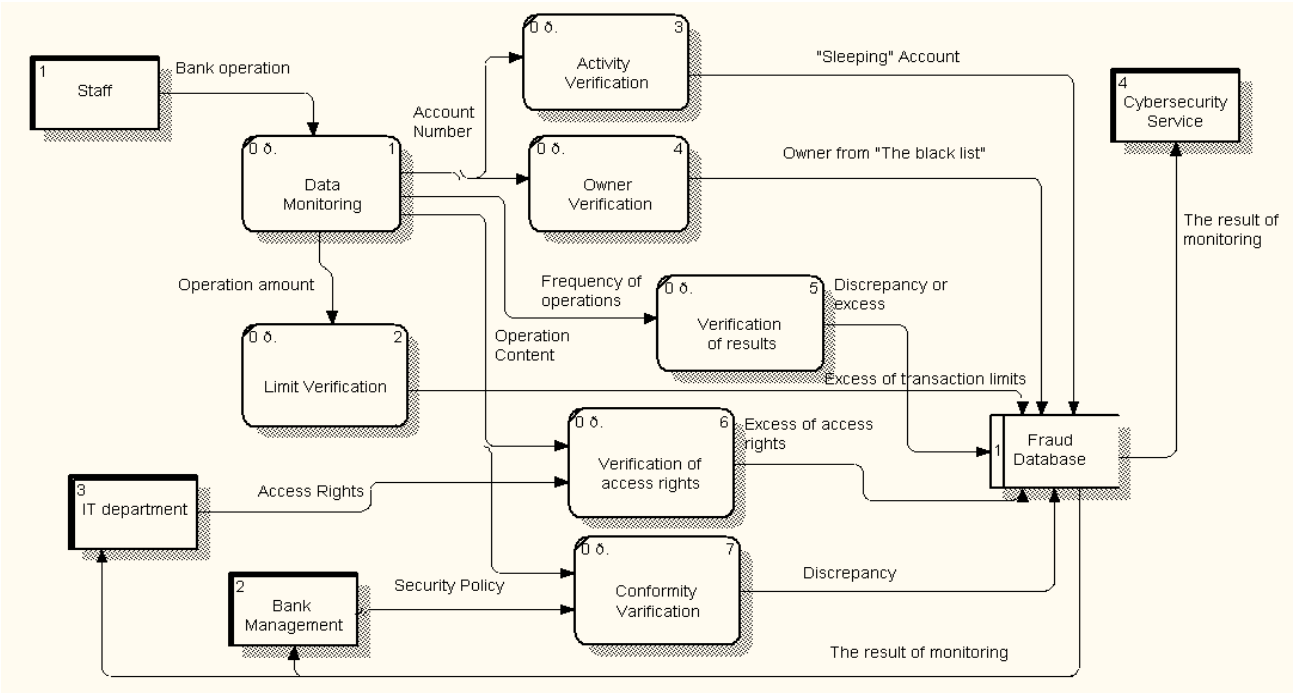


Рисунок 1.36 – Інформаційна модель виявлення ознак шахрайств персоналу банку [24]

Модель, представлена на рисунку 1.36, відображає інформаційні потоки, які циркулюють в процесі перевірки модулем моніторингу (“Data Monitoring”) операцій (“Bank operation”), що здійснюються персоналом банку (“Staff”) на предмет виявлення ознак шахрайства. Перевіряються:

– активності рахунку (“Activity Verification”) у випадку, коли персонал у власних цілях використовує “сплячі рахунки” (“Sleeping Account”);

– власники рахунку (“Owner Verification”), якщо власник присутній у “чорному списку” або є іноземцем, померлим тощо (“Owner from “The black list””);

– ліміти по операціям, що здійснюються у відповідності із вимогами НБУ, політикою банку, посадовими інструкціями тощо (“Limit Verification”), в результаті чого виявляються надлишки по лімітам (“Excess of transaction limits”);

– активності банківських співробітників (“Frequency of operations”) на предмет дотримання банківських нормативів, які співробітник може перевищувати чи недовиконувати (“Discrepancy or excess”);

– операції працівників на відповідність належним їм правам доступу (“Verification of access rights”). Це може бути випадок, коли працівники перевищують свої права (“Excess of access rights”) і, наприклад, проводять операції, які не відповідають їх функціональним обов'язкам та посадовим інструкціям;

– операції працівників на відповідність політиці безпеці банку (“Conformity Verification”). Це можуть бути випадки копіювання бази даних, користування некорпоративною поштою, перегляду рахунків клієнтів, особливо VIP-клієнтів, тощо.

Результати накопичуються у базі даних шахрайств, обробляються та надсилаються відділу кібербезпеки банку (“Cybersecurity Service”), IT-відділу (“IT Department) та менеджменту банку (“Bank Management”).

У відповідністю із запропонованою інформаційною моделлю (рисунок 1.36) розроблено схему процесу здійснення операції персоналом з урахуванням її перевірки на ознаки шахрайства у нотації BPMN 2.0 (рисунок 1.37).

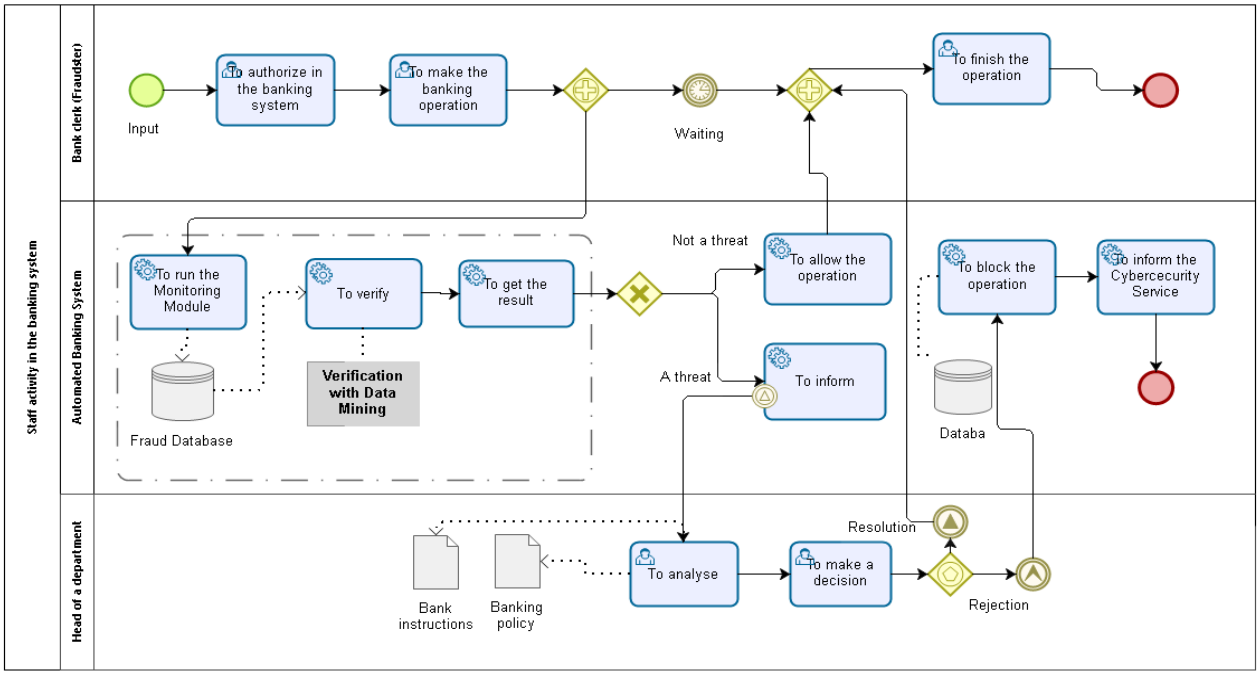


Рисунок 1.37 – Схема процесу здійснення операцій персоналом банку [24]

Процес виглядатиме наступним чином:

1) банківський співробітник, який може бути потенційним шахраєм, (“Bank clerk (Fraudster)”) авторизується в банківській системі (“To authorize in the banking system”) та здійснює банківську операцію (“To make the banking operation”);

2) АБС (“Automated Banking System”) перевіряє операцію на предмет шахрайства (“Verification with Data Mining”) із використанням критеріїв (“Fraud Database”), представлених в інформаційні моделі на рисунку 1.36;

3) якщо операція відповідає всім критеріям та не містить ознаки шахрайства з боку персоналу, то система дозволяє здійснення операції (“To allow the operation”) та працівник її завершує (“To finish the operation”);

4) якщо система виявляє ознаки шахрайства, то вона повідомляє керівника відповідного департаменту (“Head of department”), де було здійснено операцію, який аналізує інформацію (“To analyse”) та приймає рішення (“To make a decision”);

5) якщо операція допустима, то працівник отримує дозвіл (“Resolution”) та завершує операцію;

6) в протилежному випадку операція блокується (“To block the operation”) та інформація надходить до служби безпеки (“To inform the Cybersecurity Service”).

Реалізація запропонованих моделей дозволить виявити передумови та ознаки, наслідком яких може бути здійснення шахрайства або протиправної дії, або дії, яка призведе до негативних наслідків як для банка, так і для клієнта. Їх побудова із використанням системного підходу дозволить поєднати всіх учасників незалежно від належності до їх зовнішнього чи внутрішнього середовища. Розроблені моделі слугують передумовою для створення автоматизованого модулю моніторингу для перевірки банківських операцій та транзакцій на предмет наявності ознак шахрайства. Це продиктовано необхідністю у інструментах, які системно вирішують проблеми виявлення та попередження шахрайств у банках. В результаті даний підхід сприятиме

комплексній інтеграції всіх бізнес-процесів банку в єдину автоматизовану банківську систему. Врешті-решт впровадження автоматизованої системи моніторингу підвищить ефективність системи управління за рахунок своєчасного попередження та оперативного прийняття рішення.

Пункт 1.2.3 цього звіту було виконано із використанням матеріалів проміжного звіту про НДР [11] та публікацій виконавців [18, 24].

1.3 Оцінка рівня втрат банків від шахрайських операцій

1.3.1 Кількісний аналіз збитків банківської системи в результаті кібершахрайств

За даними Національного банку України збитки вітчизняних банків в 2017р. склали 24,4 мільярда гривень. Безумовно, переважна частина даної суми акумульована в наслідок збільшення відрахувань до обов'язкових банківських резервів, вимоги до обсягу яких значно зросли в останні три роки. Проте певна частина з даної суми збитків банківського сектору виникла в наслідок залучення банків до шахрайських операцій. В той же час, менеджмент банків, в своїй більшості, зосереджує увагу на фінансовому моніторингу власних операцій, оскільки цього вимагає державний регулятор. До ймовірного обсягу збитків, які можуть бути отримані в наслідок залучення фінансової установи до шахрайських операцій, менеджмент банку, відноситься досить скептично. Але, на нашу думку, це необхідний елемент внутрішньобанківської системи протидії залучення фінансової установи до незаконних операцій, оскільки кількісне оцінювання збитків банків від їх залучення до шахрайських операцій, дозволить встановити центри їх виникнення та визначити відповідальних осіб за їх нейтралізацію даних збитків.

Ціллю є розробка науково-методичного підходу до ідентифікації релевантних факторів ризиків, визначення витратних матриць виникнення

негативних наслідків від їх настання, побудови дерева рішень можливих альтернатив нівелювання ризиків банківської діяльності, що надасть можливість провести оцінку ймовірних збитків банків від їх залучення до шахрайських операцій.

Проведемо поетапну реалізацію науково-методичного підходу до визначення ймовірних збитків банку від їх залучення до шахрайських операцій:

1 етап. Формування ознакового простору основних індикаторів збитків банку від їх залучення до шахрайських операцій з урахуванням як зовнішніх, так і внутрішніх змін середовища функціонування банку. В рамках даного етапу виникає необхідність визначення як релевантних факторів ризиків шахрайських операцій, притаманних банківській діяльності, так і переваг, які отримує банк у випадку уникнення або подолання наслідків впливу даних ризиків.

2 етап. Вибір або розробка математичних моделей для надання кількісної характеристики кожного із виділених релевантних факторів ризиків шахрайських операцій. На даному етапі виникає необхідність врахування того факту, що фактори ризику набувають як якісних, так і кількісних значень.

3 етап. Визначення співставності факторів банківських ризиків та переваг, які отримує банку у випадку уникнення або подолання наслідків впливу ризиків шахрайських операцій, а також формалізація ідентифікованої відповідності в табличному вигляді. Крім того, в рамках даного етапу виникає необхідність проведення аналізу чутливості релевантних факторів ризиків шахрайських операцій, притаманним банкам, враховуючи суми бінарних показників таблиць співставності релевантних факторів ризиків та відповідних переваг.

4 етап. Реалізація витратного підходу для релевантних факторів ризиків шахрайських операцій, які не надають можливості отримати відповідні переваги для банків, шляхом побудови витратних матриць та визначення ймовірностей їх отримання в кожній конкретній ситуації.

5 етап. Формування дерева рішень можливих альтернатив подолання ризиків шахрайських операцій банківської діяльності.

Таким чином, дослідивши послідовність визначення ймовірних збитків банків від їх залучення до шахрайських операцій необхідно більш детально розглянути формалізацію наведених етапів та визначити математичне забезпечення для реалізації кожного з них.

Так, в розрізі аналізованих релевантних факторів ризиків шахрайських операцій необхідно виділити наступні групи аналізу [27]:

1) шахрайство з використанням банкомату (зняття готівки з використанням "білого" пластику (Z1), використання скіммінгових інструментів (копіювання даних платіжних карток у т.ч. з магнітної смуги, запис ПІН-коду тощо) (Z2), зняття коштів із використанням банкомату без відображення цієї операції на рахунку (Transaction Reversal Fraud) (Z3), зняття готівки держателем платіжної картки без її фізичного отримання (Cash Trapping) (Z4), фізичні атаки на банкомати(Z5));

2) шахрайство в термінальній мережі (здійснення операцій із використанням підробленої/викраденої/втраченої платіжної картки (S1), отримання готівки через касу банку за підробленими документами та платіжною карткою (S2), проведення дублюючих операцій касиром/оператором (S3), проведення несанкціонованого/неточного списання (коли сума на чеку та сума, яка включена до розрахунку, відрізняються) (S4), компрометація касиром даних платіжної картки під час розрахунків у торговельно-сервісній мережі з метою їх подальшого несанкціонованого використання (S5), використання накладок (скімерів) на термінальному обладнанні, яке дозволяє під час здійснення розрахунку зчитувати та передавати дані платіжної картки (протиправна домовленість з касирами) (S6), встановлення шкідливих програм які пошкоджують програмне забезпечення терміналів (S7));

3) інтернет шахрайство (використання шкідливих програм (вірусів), підроблених сайтів з метою компрометації реквізитів електронних платіжних

засобів та/або логінів/паролів доступу до систем інтернет/мобільного банкінгу (RC1), розповсюдження (продаж, поширення) інформації щодо скомпрометованих даних (RC2));

4) шахрайство в системах дистанційного обслуговування (ДБО) - несанкціоноване втручання та/або встановлення шкідливих програм (вірусів), які пошкоджують програмне забезпечення персональних комп'ютерів та перехоплюють паролі доступу до рахунків, інформацію з секретних ключів/токенів тощо (RK1);

5) соціальна інженерія - виманювання шахраями, які входять в довіру до власників рахунків/держателів карток, їх персональних даних, реквізитів платіжних карток або спонукання власників рахунків до здійснення переказу коштів на користь шахраїв (RP1)).

У випадку уникнення або подолання наслідків впливу ризиків шахрайства з використанням банкомату, шахрайства в термінальній мережі, інтернет шахрайства, шахрайства в системах дистанційного обслуговування, соціальної інженерії, банк отримує наступний перелік переваг: нарощування обсягів фінансових потоків; розширення клієнтської бази банку; інтенсифікація попиту на банківські послуги; збереження ліцензії на здійснення банківських послуг; стабільне функціонування фінансової установи; співпраця з міжнародними партнерами.

Дослідження та ідентифікація релевантних факторів ризиків шахрайських операцій, притаманних банківській діяльності, а також переваг, отриманих в наслідок їх уникнення та подолання, є основою проведення наступного етапу реалізації методичного підходу до визначення ймовірних збитків банків від їх залучення до шахрайських операцій і відповідно побудови таблиці відповідності (див. табл. 1.7).

Таблиця 1.7 – Встановлення відповідності досягнутих переваг банків внаслідок подолання притаманних її діяльності ризиків шахрайських операцій релевантним факторам, які обумовлюють отримання даних переваг

Релевантні фактори ризиків шахрайських операцій, притаманних банківській діяльності	Переваги, які отримує банк у випадку уникнення або подолання наслідків впливу ризиків шахрайських операцій					
	Нарощування обсягів фінансових потоків (Р1)	Розширення клієнтської бази банку (Р2)	Інтенсифікація попиту на банківські послуги (Р3)	Збереження ліцензії на здійснення банківських послуг (Р4)	Стабільне функціонування фінансової установи (Р5)	Співпраця з міжнародними партнерами (Р6)
Шахрайство з використанням банкомату						
Z1	z_{11}	z_{12}	z_{13}	z_{14}	z_{15}	z_{16}
Z2	z_{21}	z_{22}	z_{23}	z_{24}	z_{25}	z_{26}
Z3	z_{31}	z_{32}	z_{33}	z_{34}	z_{35}	z_{36}
Z4	z_{41}	z_{42}	z_{43}	z_{44}	z_{45}	z_{46}
Z5	z_{51}	z_{52}	z_{53}	z_{54}	z_{55}	z_{56}
Шахрайство в термінальній мережі						
S1	s_{11}	s_{12}	s_{13}	s_{14}	s_{15}	s_{11}
S2	s_{21}	s_{22}	s_{23}	s_{24}	s_{25}	s_{21}
…	…	…	…	…	…	…
S7	s_{111}	s_{112}	s_{113}	s_{114}	s_{115}	s_{111}
Інтернет шахрайство						
RC1	c_{11}	c_{12}	c_{13}	c_{14}	c_{15}	c_{16}
RC2	c_{21}	c_{22}	c_{23}	c_{24}	c_{25}	c_{26}
Шахрайство в системах дистанційного обслуговування						
RK1	k_{11}	k_{12}	k_{13}	k_{14}	k_{15}	k_{16}
Соціальна інженерія						
RP1	p_{11}	p_{12}	p_{13}	p_{14}	p_{15}	p_{16}

Розглядаючи математичні позначення, наведені в табл. 1.7, необхідно зазначити, що їх визначення проводиться за формулами 1.5-1.10:

$$r_{lj} = \begin{cases} 1, \text{якщо } l - \text{й релевантний фактор ризиків надає } j - \text{ту перевагу} \\ 0, \text{якщо } l - \text{й релевантний фактор ризиків не надає } j - \text{тої переваги} \end{cases} \quad (1.5)$$

де $r_{lj} = z_{lj}$ - в розрізі групи ризиків шахрайства з використанням банкомату;

$r_{lj} = s_{lj}$ - в розрізі групи ризиків шахрайства в термінальній мережі;

$r_{lj} = c_{lj}$ - в розрізі групи ризиків інтернет шахрайства;

$r_{lj} = k_{lj}$ - в розрізі групи ризиків шахрайства в системах дистанційного обслуговування;

$r_{lj} = p_{lj}$ - в розрізі групи ризиків соціальної інженерії.

Дослідивши загальні підходи до встановлення відповідності досягнутих переваг банків внаслідок подолання притаманних її діяльності ризиків релевантним факторам, які обумовлюють отримання даних переваг розглянемо наступні правила формалізації даної відповідності на прикладі фактору Z1 (зняття готівки з використанням "білого" пластику) (таблиця 1.8).

Таблиця 1.8 – Відповідність переваг банків загальним факторам ризиків шахрайських операцій її діяльності в розрізі аналізу зняття готівки з використанням "білого" пластику

Релевантні фактори ризиків шахрайських операцій	Переваги, які отримує банк у випадку уникнення або подолання наслідків впливу ризиків шахрайських операцій					
	Нарощування обсягів фінансових потоків (Р1)	Розширення клієнтської бази банку (Р2)	Інтенсифікація попиту на банківські послуги (Р3)	Збереження ліцензії на здійснення послуг (Р4)	Стабільне функціонування фінансової установи (Р5)	Співпраця з міжнародними партнерами (Р6)
Високий	$z_{11}=0$	$z_{12}=0$	$z_{13}=0$	$z_{14}=0$	$z_{15}=0$	$z_{16}=0$
Низький	$z_{11}=1$	$z_{12}=1$	$z_{13}=1$	$z_{14}=1$	$z_{15}=1$	$z_{16}=1$

Переходячи до наступного етапу методичного підходу до визначення ймовірних збитків банків від їх залучення до шахрайських операцій, перейдемо до застосування витратного підходу для базових факторів ризиків, які не надають можливості отримати відповідні переваги на ринку банківських послуг, шляхом побудови витратних матриць та визначення імовірностей їх

отримання в кожній конкретній ситуації. На даному етапі виникає необхідність побудови таблиці витрат з відповідними умовними позначеннями (таблиця 1.9).

Таблиця 1.9 – Обсяги витрат банків як результат настання негативних наслідків дії ризиків шахрайських операцій,

Релевантні фактори ризиків шахрайських операцій, притаманних банківській діяльності	Переваги, які отримує банку випадку уникнення або подолання наслідків впливу ризиків шахрайських операцій					
	Нарощування обсягів фінансових потоків (P1)	Розширення клієнтської бази банку (P2)	Інтенсифікація попиту на банківські послуги (P3)	Збереження ліцензії на здійснення банківських послуг (P4)	Стабільне функціонування фінансової установи (P5)	Співпраця з міжнародними партнерами (P6)
Шахрайство з використанням банкомату						
Z1	v_{lj}	v_{lj}	v_{lj}	v_{lj}	v_{lj}	v_{lj}
Z2	v_{lj}	v_{lj}	v_{lj}	v_{lj}	v_{lj}	v_{lj}
Z3	v_{lj}	v_{lj}	v_{lj}	v_{lj}	v_{lj}	v_{lj}
Z4	v_{lj}	v_{lj}	v_{lj}	v_{lj}	v_{lj}	v_{lj}
Z5	v_{lj}	v_{lj}	v_{lj}	v_{lj}	v_{lj}	v_{lj}
Шахрайство в термінальній мережі						
S1	v_{lj}	v_{lj}	v_{lj}	v_{lj}	v_{lj}	v_{lj}
S2	v_{lj}	v_{lj}	v_{lj}	v_{lj}	v_{lj}	v_{lj}
…	…	…	…	…	…	…
S7	v_{lj}	v_{lj}	v_{lj}	v_{lj}	v_{lj}	v_{lj}
Інтернет шахрайство						
RC1	v_{lj}	v_{lj}	v_{lj}	v_{lj}	v_{lj}	v_{lj}
Шахрайство в системах дистанційного обслуговування						
RK1	v_{lj}	v_{lj}	v_{lj}	v_{lj}	v_{lj}	v_{lj}
Соціальна інженерія						
RP1	v_{lj}	v_{lj}	v_{lj}	v_{lj}	v_{lj}	v_{lj}

Значення, наведені в таблиці 1.9, пропонується обраховувати наступним чином:

$$v_{lj} = \begin{bmatrix} L_{lj}|_{1-r_{lj}=1} \\ 0|_{1-r_{lj}=0} \end{bmatrix} \quad (1.6)$$

де $v_{lj}|_{l=1\div5,\, j=1\div6}$ - індикатор витрат банку як результат настання негативних наслідків дії групи ризиків шахрайства з використанням банкомату, притаманних банківській діяльності; для зазначених значень індексів L_{lj} - обсяг витрат, які несе банківська установи у випадку невиконання встановлених вимог в розрізі ризику зняття готівки з використанням "білого" пластику, використання скіммінгових інструментів, зняття коштів із використанням банкомату без відображення цієї операції на рахунку, зняття готівки держателем платіжної картки без її фізичного отримання, фізичні атаки на банкомати;

$v_{lj}|_{l=6\div16,\, j=1\div6}$ - індикатор витрат банку як результат настання негативних наслідків дії групи ризиків шахрайства в термінальній мережі, притаманних банківській діяльності; для зазначених значень індексів L_{lj} - обсяг витрат, які несе банк у випадку невиконання встановлених вимог в розрізі ризику здійснення операцій із використанням підробленої/викраденої/втраченої платіжної картки, отримання готівки через касу банку за підробленими документами та платіжною карткою, проведення дублюючих операцій касиром/оператором, проведення несанкціонованого/неточного списання, компрометація касиром даних платіжної картки під час розрахунків у торговельно-сервісній мережі з метою їх подальшого несанкціонованого використання, використання накладок (скімерів) на термінальному обладнанні, встановлення шкідливих програм;

$v_{lj}|_{l=17\div19,\, j=1\div6}$ - індикатор витрат банку як результат настання негативних наслідків дії групи ризиків Інтернет шахрайства, притаманних банківській діяльності; для зазначених значень індексів L_{lj} - обсяг витрат, які несе банк у

випадку невиконання встановлених вимог в розрізі ризику інтернет шахрайство;

$v_{lj}\,|_{l=20\div25,\,j=1\div6}$ - індикатор витрат банку як результат настання негативних наслідків дії групи ризиків шахрайства в системах дистанційного обслуговування, притаманних банківській діяльності; для зазначених значень індексів L_{lj} - обсяг витрат, які несе банк у випадку невиконання встановлених вимог в розрізі ризику шахрайства в системах дистанційного обслуговування;

$v_{lj}\,|_{l=26\div36,\,j=1\div6}$ - індикатор витрат банку як результат настання негативних наслідків дії групи ризиків соціальної інженерії, притаманних банківській діяльності; для зазначених значень індексів L_{lj} - обсяг витрат, які несе банк у випадку невиконання встановлених вимог в розрізі ризику соціальна інженерія.

На базі наведених вище таблиці 1.9 та формул 1.7, перейдемо послідовно до побудови *витратних матриць:*

$$L = \begin{matrix} & \min\left\{L_{lj}|_{1-r_{lj}=1}\right\} & \max\left\{L_{lj}|_{1-r_{lj}=1}\right\} \\ \min\left\{L_{lj}|_{1-r_{lj}=1}\right\} & \begin{pmatrix}\min\left\{L_{lj}|_{1-r_{lj}=1}\right\}+\\+\min\left\{L_{lj}|_{1-r_{lj}=1}\right\}\end{pmatrix} & \begin{pmatrix}\min\left\{L_{lj}|_{1-r_{lj}=1}\right\}+\\+\max\left\{L_{lj}|_{1-r_{lj}=1}\right\}\end{pmatrix} \\ \max\left\{L_{lj}|_{1-r_{lj}=1}\right\} & \begin{pmatrix}\max\left\{L_{lj}|_{1-r_{lj}=1}\right\}+\\+\min\left\{L_{lj}|_{1-r_{lj}=1}\right\}\end{pmatrix} & \begin{pmatrix}\max\left\{L_{lj}|_{1-r_{lj}=1}\right\}+\\+\max\left\{L_{lj}|_{1-r_{lj}=1}\right\}\end{pmatrix} \end{matrix} \qquad (1.7)$$

Визначення ймовірностей їх отримання в кожній конкретній ситуації:

$$P = \begin{matrix} & maxP\left[\min\left\{L_{lj}|_{1-r_{lj}=1}\right\}\right] & minP\left[\max\left\{L_{lj}|_{1-r_{lj}=1}\right\}\right] \\ maxP\left[\min\left\{L_{lj}|_{1-r_{lj}=1}\right\}\right] & \begin{pmatrix}maxP\left[\min\left\{L_{lj}|_{1-r_{lj}=1}\right\}\right]\times\\\times maxP\left[\min\left\{L_{lj}|_{1-r_{lj}=1}\right\}\right]\end{pmatrix} & \begin{pmatrix}maxP\left[\min\left\{L_{lj}|_{1-r_{lj}=1}\right\}\right]\times\\\times minP\left[\max\left\{L_{lj}|_{1-r_{lj}=1}\right\}\right]\end{pmatrix} \\ minP\left[\max\left\{L_{lj}|_{1-r_{lj}=1}\right\}\right] & \begin{pmatrix}minP\left[\max\left\{L_{lj}|_{1-r_{lj}=1}\right\}\right]\times\\\times maxP\left[\min\left\{L_{lj}|_{1-r_{lj}=1}\right\}\right]\end{pmatrix} & \begin{pmatrix}minP\left[\max\left\{L_{lj}|_{1-r_{lj}=1}\right\}\right]\times\\\times minP\left[\max\left\{L_{lj}|_{1-r_{lj}=1}\right\}\right]\end{pmatrix} \end{matrix} \qquad (1.8)$$

де L - матриця витрат банку при різних комбінаціях виникнення негативних наслідків настання ризиків шахрайських операцій;

P - імовірність виникнення витрат банку в кожній конкретній ситуації.

Переходячи до визначення сум витрат, обсяги яких не будуть перевищувати певну заздалегідь встановленого значення, що дозволяє сформувати певний резервний фонд, виникає необхідність проведення наступних наведених нижче обчислень. Математично реалізацію даного етапу пропонується здійснити на базі формування рішень можливих альтернатив подолання ризиків шахрайських операцій банківської діяльності:

$$R = \begin{Bmatrix} \begin{pmatrix} min\left\{L_{lj}|_{1-r_{lj}=1}\right\}+ \\ +min\left\{L_{lj}|_{1-r_{lj}=1}\right\} \end{pmatrix} & \begin{pmatrix} min\left\{L_{lj}|_{1-r_{lj}=1}\right\}+ \\ +max\left\{L_{lj}|_{1-r_{lj}=1}\right\} \end{pmatrix} & \begin{pmatrix} max\left\{L_{lj}|_{1-r_{lj}=1}\right\}+ \\ +max\left\{L_{lj}|_{1-r_{lj}=1}\right\} \end{pmatrix} \\ \begin{pmatrix} maxP\left[min\left\{L_{lj}|_{1-r_{lj}=1}\right\}\right]\times \\ \times maxP\left[min\left\{L_{lj}|_{1-r_{lj}=1}\right\}\right] \end{pmatrix} & \begin{pmatrix} minP\left[max\left\{L_{lj}|_{1-r_{lj}=1}\right\}\right]\times \\ \times maxP\left[min\left\{L_{lj}|_{1-r_{lj}=1}\right\}\right] \end{pmatrix} & \begin{pmatrix} minP\left[max\left\{L_{lj}|_{1-r_{lj}=1}\right\}\right]\times \\ \times minP\left[max\left\{L_{lj}|_{1-r_{lj}=1}\right\}\right] \end{pmatrix} \end{Bmatrix} \quad (1.9)$$

$$\begin{Bmatrix} L \\ P(R \le L) \end{Bmatrix} = \begin{Bmatrix} \begin{pmatrix} min\left\{L_{lj}|_{1-r_{lj}=1}\right\}+ \\ +min\left\{L_{lj}|_{1-r_{lj}=1}\right\} \end{pmatrix} & \begin{pmatrix} min\left\{L_{lj}|_{1-r_{lj}=1}\right\}+ \\ +max\left\{L_{lj}|_{1-r_{lj}=1}\right\} \end{pmatrix} & \begin{pmatrix} max\left\{L_{lj}|_{1-r_{lj}=1}\right\}+ \\ +min\left\{L_{lj}|_{1-r_{lj}=1}\right\} \end{pmatrix} \\ \begin{pmatrix} maxP\left[min\left\{L_{lj}|_{1-r_{lj}=1}\right\}\right]\times \\ \times maxP\left[min\left\{L_{lj}|_{1-r_{lj}=1}\right\}\right] \end{pmatrix} & \begin{pmatrix} maxP\left[min\left\{L_{lj}|_{1-r_{lj}=1}\right\}\right]\times \\ \times maxP\left[min\left\{L_{lj}|_{1-r_{lj}=1}\right\}\right]+ \\ +minP\left[max\left\{L_{lj}|_{1-r_{lj}=1}\right\}\right]\times \\ \times maxP\left[min\left\{L_{lj}|_{1-r_{lj}=1}\right\}\right] \end{pmatrix} & 1 \end{Bmatrix} \quad (1.10)$$

Підсумовуючи результати проведеного дослідження, необхідно зазначити, що використання у практичній діяльності науково-методичних підходів до визначення ймовірних збитків банків від їх залучення до шахрайських операцій, на основі математичної формалізації проведення вищевказаних розрахунків, із застосуванням витратного підходу, побудови витратних матриць, формування дерева рішень можливих альтернатив подолання ризиків шахрайських операцій банківської діяльності, паралельно з підвищенням системи внутрішньобанківського моніторингу сприятиме ще отриманню банком ряду наступних переваг: нарощування обсягів фінансових потоків; розширення клієнтської бази; інтенсифікація попиту на банківські

послуги; збереження ліцензії на здійснення банківських послуг; стабільне функціонування фінансової установи; співпраця з міжнародними партнерами.

Пункт 1.3.1 цього звіту було виконано із використанням матеріалів проміжного звіту про НДР [11] та публікацій виконавців [18, 28, 29].

1.3.2 Моделювання кількісної оцінки рівня операційного ризику банку в сфері інформаційної безпеки

Урівноваженість банківської діяльності дуже часто порушується через виникненням додаткових витрат, що пов’язані з ліквідацією або попередження дестабілізуючих чинників. Причинами значної частки витрат, що з’являються в результаті виникнення операційних ризиків банків в сфері інформаційної безпеки, можуть бути: шахрайства в банківській сфері; зловживання службовими обов’язками; відмови систем; порушення технологій здійснення банківських операцій.

Ефективність керування операційними ризиками комерційного банку в сфері інформаційної безпеки досягається за допомогою прийняття обґрунтованих рішень стосовно їх регулювання, основу яких становить кількісна оцінка ступеня цих ризиків.

Визначити оцінку ступеня операційного ризику комерційного банку в сфері інформаційної безпеки запропоновано шляхом формування групи показників $K_{ij}, i = 1 \div n, j = 1 \div m$, кожен із яких у відповідній мірі описує той чи інший j-й інцидент (причину) виникнення операційного ризику в сфері інформаційної безпеки.

Запропоновані показники можуть характеризувати певний окремий інцидент, а також частково декілька інцидентів виникнення операційного ризику інформаційної безпеки. Така можливість пов’язана з тим, що деякі

показники одночасно висвітлюють характеристики різних інцидентів причому з різою мірою впливаючи на них.

Визначити кількісну характеристику операційного ризику інформаційної безпеки за допомогою показників, що відображають як однозначний, так і не однозначний вплив різних інцидентів, пропонується наступна методика.

Базуючись на тому, що показники, що характеризують рівень операційного ризику інформаційної безпеки, відображають різні аспекти функціонування банківської установи і відповідно є різнорідними, потрібно переформувати їх у до співставного значення (визначити нормалізований показник).

І для цього використовується така формула (формула 1.11) [30]:

$$NK_i = \frac{K_i}{\overline{K_i}} \tag{1.11}$$

де $NK_i i = 1 \div n$ - нормалізоване значення i-го показника кількісної оцінки ступеня операційного ризику інформаційної безпеки;

K_i - абсолютне значення i-го показника кількісної оцінки ступеня операційного ризику інформаційної безпеки;

$\overline{K_i}$ - середнє значення i-го показника за визначеною статистичною інформацію (при дослідженні структури) або за визначений проміжок (при дослідженні динаміки).

Запропонований підхід нормалізації значення i-го показника кількісної оцінки ступеня операційного ризику інформаційної безпеки дає можливість привести показники до співставного вигляду залежно від мети аналізу: дослідження структури чи динаміки розвитку операційного ризику інформаційної безпеки. Також, вказаний підхід дозволяє провести нормалізацію показників не враховуючи напрямок їх впливу, що є дуже важливим за умови суттєвої кількості показників.

Так як показники, що характеризують основні властивості операційних ризиків інформаційної безпеки, можуть однозначно і неоднозначно відображати певну групу інцидентів ризику, постає необхідність їх розділення на три групи:

- показники, що показують властивості виключно однієї групи інцидентів операційного ризику інформаційної безпеки;
- показники, що у відповідних співставленнях відображують дві групи інцидентів ризику;
- показники, що описують три або чотири інциденти операційного ризику в сфері інформаційної безпеки.

Отже, виникає потреба встановити ступінь впливу кожного окремого інциденту на операційний ризик банку в сфері інформаційної безпеки. Таким чином, з ціллю обчислення числових значень характеристик ступеня впливу відповідного інциденту на рівень показника операційного ризику інформаційної безпеки проведено даний аналіз (формула 1.12) [30]. Слід зауважити, що показники операційного ризику інформаційної безпеки відтворюють кожний інцидент ризику у відповідних співставеннях. Для проведення наступного аналізу представимо групи інцидентів операційного ризику інформаційної безпеки в якості фіктивних змінних, а саме змінних, що набувають значення «1» за можливості їх опису певним показником, або «0» в іншому випадку.

$$K_i = \beta_0 + \beta_1 F_{1i} + \beta_2 F_{2i} + \beta_3 F_{3i} + \beta_4 F_{4i} + \varepsilon \qquad (1.12)$$

де K_i - абсолютне значення i-го показника кількісної оцінки ступеня операційного ризику інформаційної безпеки;

$F_{ij}, j = 1 \div 4$ - фіктивна змінна характеристики i-го показника j-го інциденту операційного ризику інформаційної безпеки;

$\beta_m, m = 0 \div 4$ - сталі величини;

ε - похибка (відхилення фактичного і теоретичного рівнів відповідного i-го показника кількісної оцінки ступеня операційного ризику інформаційної безпеки).

Розрахувати числові значення характеристик ступеня впливу відповідного інциденту на рівень показника операційного ризику інформаційної безпеки до j-х інцидентів на основі рівняння (3.8) є неможливим. Так, щоб визначити на скільки відсотків кожен з інцидентів пояснює виникнення операційного ризику інформаційної безпеки за певним показником (формула 1.13) [30]:

$$K_i = \alpha_1 F_{1i} + \alpha_2 F_{2i} + \alpha_3 F_{3i} + \alpha_4 F_{4i} + \varepsilon \qquad (1.13)$$

де K_i - абсолютне значення i-го показника кількісної оцінки ступеня операційного ризику інформаційної безпеки;

$F_{ji}, j = 1 \div 4$ - фіктивна змінна характеристики *i*-го показника j-го інциденту операційного ризику інформаційної безпеки;

$\alpha_m, m = 1 \div 4$ - сталі величини, які відображають значення характеристик ступеня впливу певного інциденту на рівень показника операційного ризику інформаційної безпеки до j-х інцидентів;

ε - похибка (відхилення фактичного і теоретичного рівнів відповідного i-го показника кількісної оцінки ступеня операційного ризику інформаційної безпеки).

Коефіцієнти $\alpha_m, m = 1 \div 4$ рівняння (1.13) визначаються за наступною формулою (1.14) [30]:

$$\alpha_m = \beta_m \frac{\sigma_{F_j}}{\sigma_{K_i}} \qquad (1.14)$$

де K_i - абсолютне значення i-го показника кількісної оцінки ступеня операційного ризику інформаційної безпеки;

σ_{F_j}, σ_{K_i} - середні квадратичні відхилення факторних і результативної ознак відповідно, які визначаються за формулами (1.15) і (1.16) [30]:

$$\sigma_{F_j} = \sqrt{\overline{F_j^2} - \overline{F_j}^2}, \tag{1.15}$$

$$\sigma_{K_i} = \sqrt{\overline{K_i^2} - \overline{K_i}^2}. \tag{1.16}$$

Так як метою аналізу є встановлення абсолютного значення ступеня впливу інцидентів на показники операційного ризику інформаційної безпеки, то отримані показники, в разі невідповідності знаків, беруться по модулю. Базуючись на скорегованих числових характеристиках (α_m^*) знаходиться відносний показник структури (формула 1.17) [30], що характеризує питому вагу впливу інцидентів на рівень операційного ризику інформаційної безпеки.

$$\alpha_m^* = \frac{\alpha_m}{\sum_{m=1}^{4} \alpha_m}, \tag{1.17}$$

Визначені числові значення характеристик ступеня впливу окремого інциденту на рівень певного показника кількісної оцінки ступеня операційного ризику інформаційної безпеки відповідним пояснюючим ознакам, а також абсолютні значення самих показників наведемо у таблиці 1.10.

За допомогою даних таблиці 1.10 та формули (3.7) обчислимо значення нормалізованих показників кількісної оцінки ступеня операційного ризику інформаційної безпеки зважених на характеристики впливу конкретного

інциденту на рівень показника операційного ризику інформаційної безпеки (таблиця 1.11).

Таблиця 1.10 - Значення характеристик ступеня впливу окремого інциденту на рівень показника операційного ризику інформаційної безпеки

№	Показник ($K_i, i=1\div n$)	Значення характеристик ступеня впливу окремого інциденту на рівень показника операційного ризику інформаційної безпеки			
		ризик, пов'язаний з діями працівників та безпекою робочого місця $j=1$	ризик систем і технологій $j=2$	ризик помилки у банківських процесах (ризик взаємовідносин) $j=3$	ризик пов'язаний з зовнішніми чинниками $j=4$
А	Б	1	2	3	4
	I група				
1	K_1	α_{111}	α_{112}	α_{113}	α_{114}
2	K_2	α_{121}	α_{122}	α_{123}	α_{124}
…	…				
l	K_l	α_{1l1}	α_{1l2}	α_{1l3}	α_{1l4}
	II група				
l+1	K_{l+1}	α_{2l+11}	α_{2l+12}	α_{2l+13}	α_{2l+14}
l+2	K_{l+2}	α_{2l+21}	α_{2l+22}	α_{2l+23}	α_{2l+24}
…	…				
k	K_k	α_{2k1}	α_{2k2}	α_{2k3}	α_{2k4}
	III група				
k+1	K_{k+1}	α_{3k+11}	α_{3k+12}	α_{3k+13}	α_{3k+14}
k+2	K_{k+2}	α_{3k+21}	α_{3k+22}	α_{3k+23}	α_{3k+24}
…	…				
n	K_n	α_{3n1}	α_{3n2}	α_{3n3}	α_{3n4}

Отже, описаний алгоритм виступає *першим етапом* у загальної методиці розрахунку кількісної оцінки ступеня операційного ризику інформаційної безпеки, коли було обрано певний набір показників діяльності банківських установ, що дає сигнал про потенційне виникнення операційного ризику

інформаційної безпеки, а також зведення їх до співставного вигляду з урахуванням утворюючих їх чинників.

Таблиця 1.11 – Відображення структури операційного ризику інформаційної безпеки залежно від формуючих їх інцидентів

№	Значення нормалізованого показника зваженого на характеристику впливу конкретного інциденту на рівень показника операційного ризику інформаційної безпеки			
	ризик, пов'язаний з діями працівників та безпекою робочого місця $j=1$	ризик систем і технологій $j=2$	ризик помилки у банківських процесах (ризик взаємовідносин) $j=3$	ризик пов'язаний з зовнішніми чинниками $j=4$
A	1	2	3	4
	I група			
1	$\alpha_1 NK_1$	$\alpha_2 NK_1$	$\alpha_3 NK_1$	$\alpha_4 NK_1$
2	$\alpha_1 NK_2$	$\alpha_2 NK_2$	$\alpha_3 NK_2$	$\alpha_4 NK_2$
…	…	…	…	…
l	$\alpha_1 NK_l$	$\alpha_2 NK_l$	$\alpha_3 NK_l$	$\alpha_4 NK_l$
	…	…	…	…
	II група			
l+1	$\alpha_1 NK_{l+1}$	$\alpha_2 NK_{l+1}$	$\alpha_3 NK_{l+1}$	$\alpha_4 NK_{l+1}$
l+2	$\alpha_1 NK_{l+2}$	$\alpha_2 NK_{l+2}$	$\alpha_3 NK_{l+2}$	$\alpha_4 NK_{l+2}$
…				
k	$\alpha_1 NK_k$	$\alpha_2 NK_k$	$\alpha_3 NK_k$	$\alpha_4 NK_k$
	…	…	…	…
	III група			
k+1	$\alpha_1 NK_{k+1}$	$\alpha_2 NK_{k+1}$	$\alpha_3 NK_{k+1}$	$\alpha_4 NK_{k+1}$
k+2	$\alpha_1 NK_{k+2}$	$\alpha_2 NK_{k+2}$	$\alpha_3 NK_{k+2}$	$\alpha_4 NK_{k+2}$
…	…	…	…	…
n	$\alpha_1 NK_n$	$\alpha_2 NK_n$	$\alpha_3 NK_n$	$\alpha_4 NK_n$

Другий етап передбачає оцінку можливих (граничних) значень для визначених нормалізованих показників, що зважені на певне значення характеристик ступеня впливу відповідного інциденту на рівень кожного з показників кількісної оцінки ступеня операційного ризику інформаційної безпеки (створення «коридору» допустимих значень нормалізованих показників). Для цього розрахуємо оптимістичний і песимістичний варіанти нормованих показників кількісної оцінки ступеня операційного ризику інформаційної безпеки банку, беручи до уваги, що всі показники можуть

набувати будь-якого значення в діапазоні $0 \div NK_i$, де $i = 1 \div n$. Так, за оптимістичної характеристики ступеня впливу відповідного інциденту - значення «0», що свідчить про відсутність, а для песимістичного варіанту набуває значення «1», отже операційний ризик інформаційної безпеки не тільки присутній, але ще й досягає максимально можливого значення.

Ґрунтуючись на одержаному діапазоні допустимих значень нормалізованих показників можна обчислити рівні кількісної оцінки ступеня операційного ризику інформаційної безпеки банківської установи за кожним окремим показником:

- якщо $0 \le \alpha_m^* NK_i < 0{,}3NK_i$, нормальний рівень;

- якщо $0{,}3NK_i \le \alpha_m^* NK_i < 0{,}5NK_i$, підвищений рівень;

- якщо $0{,}5NK_i \le \alpha_m^* NK_i < 0{,}7NK_i$, високий рівень;

- якщо $0{,}7NK_i \le \alpha_m^* NK_i \le NK_i$, критичний рівень.

Беручи до уваги наведену класифікацію, зробимо висновок, що допустимим (граничним) рівнем для виявлених нормалізованих показників, зважених на певне значення характеристик ступеня впливу окремого інциденту, виступає діапазон $0 \le \alpha_m^* NK_i < 0{,}3NK_i$.

На третьому етапі методики визначення кількісної оцінки ступеня операційного ризику банку в сфері інформаційної безпеки проводиться формування бінарних показників, що в основному залежать від знайдених раніше допустимих величин: так, якщо значення нормалізованого показника, зваженого від відповідного розміру характеристик ступеня впливу окремого інциденту, відноситься до «коридору» граничних значень, то відповідний бінарний показник набуває значення «0», в протилежному випадку – «1».

Щоб розрахувати бінарні характеристики за нормалізованими показниками $NK_i i = 1 \div n$ візьмемо наступну формулу (1.18) [30]:

$$NKbin_i \begin{cases} =1; \alpha_m^* \overline{NK_m} \geq \alpha_m^* NK_i, \\ =0; \alpha_m^* NK_i < \alpha_m^* \overline{NK_m} \end{cases}, \quad (1.18)$$

де $NKbin_i$ - бінарні характеристики по певному показнику кількісної оцінки ступеня операційного ризику банку відповідно до інцидентів даного ризику;

$NK_i, i = 1 \div n$ - нормалізоване значення i-го показника кількісної оцінки ступеня операційного ризику інформаційної безпеки;

$\alpha_m^*, m = 1 \div 4$ - скорегована характеристика ступеня впливу окремого інциденту на рівень операційного ризику інформаційної безпеки;

$\overline{NK_m}$ - середнє значення за всіма нормалізованими показниками m-го інциденту ризику.

Здійснені під час дослідження розрахунки зведемо до таблиці 1.12.

Таблиця 1.12 – Бінарні характеристики за показниками кількісної оцінки ступеня операційного ризику банку в сфері інформаційної безпеки

№	Значення бінарної характеристики зваженого на характеристику впливу окремого інциденту на рівень показника операційного ризику інформаційної безпеки			
	ризик, пов'язаний з діями працівників та безпекою робочого місця $j=1$	ризик систем і технологій $j=2$	ризик помилки у банківських процесах (ризик взаємовідносин) $j=3$	ризик пов'язаний з зовнішніми чинниками $j=4$
A	1	2	3	4
	I група			
1	$NKbin_{11}$	$NKbin_{12}$	$NKbin_{13}$	$NKbin_{14}$
2	$NKbin_{21}$	$NKbin_{22}$	$NKbin_{23}$	$NKbin_{24}$
…	…	…	…	…
l	$NKbin_{l1}$	$NKbin_{l2}$	$NKbin_{l3}$	$NKbin_{l4}$
	…	…	…	…
	II група			
l+1	$NKbin_{l+11}$	$NKbin_{l+12}$	$NKbin_{l+13}$	$NKbin_{l+14}$
l+2	$NKbin_{l+21}$	$NKbin_{l+22}$	$NKbin_{l+23}$	$NKbin_{l+24}$
…				
k	$NKbin_{k1}$	$NKbin_{k2}$	$NKbin_{k3}$	$NKbin_{k4}$
	…	…	…	…

Продовження таблиці 1.12

	III група			
k+1	$NKbin_{k+11}$	$NKbin_{k+12}$	$NKbin_{k+13}$	$NKbin_{k+14}$
k+2	$NKbin_{k+21}$	$NKbin_{k+22}$	$NKbin_{k+23}$	$NKbin_{k+24}$
…	…	…	…	…
n	$NKbin_{n1}$	$NKbin_{n2}$	$NKbin_{n3}$	$NKbin_{n4}$

Під час *четвертого етапу* визначається сума бінарних показників для певного j-го фактору ризику, що отримали значення «1», тобто експрес-оцінка операційного ризику інформаційної безпеки за j-м фактором ризику (формула 1.19) [30]:

$$EO_j = \sum_{i=1}^{n} NKbin_{ij}\,, \tag{1.19}$$

де EO_j - експрес-оцінка операційного ризику інформаційної безпеки за j-м фактором ризику;

$NKbin_{ij}$ - бінарні характеристики по кожному показнику кількісної оцінки ступеня операційного ризику банку у сфері інформаційної безпеки відповідно до інцидентів даного ризику.

На базі знайденої суми бінарних показників для певного j-го інциденту ризику розраховується загальна сума бінарних показників, що виступає у якості експрес-оцінки операційного ризику банку в сфері інформаційної безпеки (формула 1.20) [30]:

$$EO = \sum_{j=1}^{4}\sum_{i=1}^{n} NKbin_{ij}\,, \tag{1.20}$$

де EO - експрес-оцінка операційного ризику банку в сфері інформаційної безпеки;

$NKbin_{ij}$ - бінарні характеристики певного показника кількісної оцінки ступеня операційного ризику банку в сфері інформаційної безпеки відповідно до інцидентів даного ризику.

На основі визначених сум бінарних показників (EO), що є кількісною експрес-оцінкою ступеня операційного ризику інформаційної безпеки отримується якісна оцінка рівня даного ризику:

- якщо $0 \le EO < 6$, нормальний рівень ризику;
- якщо $6 \le EO < 12$, підвищений рівень ризику;
- якщо $12 \le EO \le 18$, високий рівень ризику.

Щоб розрахувати рівні операційного ризику інформаційної безпеки скористаємось не лише вище наведеною експрес оцінкою, а й імовірнісною оцінкою.

Тобто, на основі імовірнісної оцінки здійснення аналізу якісної характеристики операційного ризику комерційного банку в сфері інформаційної безпеки відбувається шляхом застосування кількісної характеристики її ступеня, що розраховується на базі одержаних бінарних показників та байєсовського (імовірнісного) підходу, що включає коректування поточного рівня операційного ризику інформаційної безпеки враховуючи його значення попереднього періоду та уточнюючих показників поточного періоду. Кількісну характеристику ступеня операційного ризику інформаційної безпеки пропонується отримати як імовірність настання даного виду ризику, тобто імовірність ($p_{OR}(H1)$) виникнення операційного ризику інформаційної безпеки (подія $H1$) за умови існування інформації $OR = (OR_1, OR_2, OR_3, OR_4)$ в розрізі 4-х інцидентів, де $OR_k, k = 1 \div 4$ набувають значення 0, якщо відповідний норматив виконується (імовірність виникнення відповідного фактору ризику знаходиться у граничних значеннях), і 1 – у протилежному випадку. Підґрунтям для визначення складових $OR = (OR_1, OR_2, OR_3, OR_4)$ є імовірності ($p_K(H1j)$) виникнення j-го інциденту операційного ризику інформаційної безпеки (подія

$H1j$) за умови існування інформації $K=(K_1,K_2,...,K_n)$, де $K_k, k=1\div n$ приймають величину 0, якщо певний норматив виконується, і 1 – у протилежному випадку.

Перейдемо до аналізу послідовності визначення імовірності ($p_{OR}(H1)$) виникнення операційного ризику інформаційної безпеки (подія $H1$) за умови існування інформації $OR=(OR_1,OR_2,OR_3,OR_4)$.

Отже, на основі одержаних бінарних показників трьох груп для окремого j-го інциденту ризику відповідно до формули Байєса (база імовірнісного підходу), знайдемо імовірність ($p_K(H1j)$) виникнення j-го інциденту операційного ризику інформаційної безпеки (подія $H1j$) за умови наявності інформації $K=(K_1,K_2,...,K_n)$ наступним чином (формули 1.21-1.22) [30]:

$$p_K(H1j)=\frac{1}{1+e^{\{\lambda_0+L\}}} \tag{1.21}$$

$$L=\sum_{i=1}^{n}\lambda_i NKbin_{ij}$$

$$\lambda_{ij}=\ln\left(\frac{b_{ij}(1-g_{ij})}{g_{ij}(1-b_{ij})}\right), i=1,...,n \tag{1.22}$$

$$\lambda_{0j}=\ln\left(\frac{p(H2j)}{p(H1j)}\right)+\sum_{i=1}^{n}\ln\left(\frac{1-b_{ij}}{1-g_{ij}}\right)$$

де $p_K(H1j)$ – імовірність виникнення j-го інциденту операційного ризику інформаційної безпеки за умови наявності інформації $K=(K_1,K_2,...,K_n)$;

L – інтегральний показник (зважена сума) бінарних характеристик $NKбін_{ij}$ (наявна інформація про стан банку виходячи зі значень аналітичних показників);

$P(H1j)$ – імовірність гіпотези $H1j$;

$H1j$ – висунута гіпотеза, що виникне j-й інциденту операційного ризику інформаційної безпеки;

$P(H2j)$ – імовірність протилежної гіпотези;

$NK = \{NKbin_{ij}\}$ – бінарна компонента множини характеристик діяльності банку;

b_{ij} – імовірність події $NK = \{NKbin_{ij}\}$ для банку у розрізі j-го інциденту операційного ризику інформаційної безпеки,

g_{ij} – імовірність супротивної події.

Щоб отримати кількісну оцінку ступеня операційного ризику інформаційної безпеки за j-м інцидентом спочатку визначимо значення b_{ij} - імовірність події $NKбін_{ij} = 0$, та g_{ij} - імовірність події $NKbin_{ij} = 1$ за всіма n показниками за формулами 1.23 [30]:

$$\begin{aligned} g_{ij} &= \frac{\sum_i NKbin_{ij}}{n}, \\ b_{ij} &= 1 - g_{ij} \end{aligned} \qquad (1.23)$$

Далі, після розрахунку b_{ij} - імовірність події $NKbin_{ij} = 0$, та g_{ij} - імовірність події $NKбін_{ij} = 1$ для кожного інциденту операційного ризику інформаційної безпеки за всіма n показниками визначимо параметри λ_{ij} та λ_{0j} за формулами (11), після чого отримаємо значення L - інтегрального показника (зваженої суми) бінарних характеристик $NK = \{NKbin_{ij}\}$ і підставимо в загальну формулу (10), що відображає розмір оцінки ризику.

На основі отриманої імовірнісної (кількісної) оцінки операційного ризику інформаційної безпеки ($p_K(H1j)$) по певному j-му інциденту знаходиться якісна характеристика рівня ризику:

- якщо $0 \le p_K(H1j) < fsr\left\{\min_s\{p_B(H1)_s\} \div fsr\{p_B(H1)_s\}\right\}$, нормальний рівень ризику (де $fsr\{\ \}$ - середнє значення зазначених показників за сукупністю S банків);

- якщо $fsr\left\{\min_s\{p_B(H1)_s\} \div fsr\{p_B(H1)_s\}\right\} \le p_K(H1j) < fsr\{p_B(H1)_s\}$, підвищений рівень ризику;

- якщо $fsr\{p_B(H1)_s\} \le p_K(H1j) < fsr\left\{fsr\{p_B(H1)_s\} \div \max_s\{p_B(H1)_s\}\right\}$, високий рівень ризику;

- якщо $fsr\left\{fsr\{p_B(H1)_s\} \div \max_s\{p_B(H1)_s\}\right\} \le p_K(H1j) \le 1$, критичний рівень ризику.

Так, використовуючи вище здійснені розрахунки, отримаємо алгоритм знаходження кількісної оцінки ступеня операційного ризику банку в сфері інформаційної безпеки як імовірності виникнення операційного ризику інформаційної безпеки при наявності інформації $B = (p_K(H11), p_K(H12), p_K(H13), p_K(H14))$, що обчислюється на грунті аналітичних показників характеристики діяльності відповідної банківської установи $K = (K_1, K_2, ..., K_n)$ (див. таблицю 1.13):

1. Визначення імовірностей $p_K(H1j)$ виникнення j-го інциденту операційного ризику інформаційної безпеки за умови наявності інформації $K = (K_1, K_2, ..., K_n)$.

2. Розрахунок питомої ваги певного інциденту у загальній структурі операційного ризику інформаційної безпеки. $S(p_K(H1j)) = \dfrac{p_K(H1j)}{\sum_{j=1}^{4} p_K(H1j)} \times 100\%$

3. Знаходження гранично можливого діапазону імовірнісної (кількісної) оцінки операційного ризику інформаційної безпеки за кожним j-м інциденту - $0 \le p_K(H1j) < 0{,}3$, що передбачає нормальний рівень ризику.

Таблиця 1.13 – Показники алгоритму визначення кількісної оцінки ступеня операційного ризику інформаційної безпеки

№	Інциденти операційного ризику інформаційної безпеки			
	ризик, пов'язаний з діями працівників та безпекою робочого місця $j=1$	ризик систем і технологій $j=2$	ризик помилки у банківських процесах (ризик взаємовідносин) $j=3$	ризик пов'язаний з зовнішніми чинниками $j=4$
А	1	2	3	4
Імовірність виникнення j-го інциденту операційного ризику інформаційної безпеки	$p_K(H11)$	$p_K(H12)$	$p_K(H13)$	$p_K(H14)$
Питома вага кожного з інцидентів у загальній структурі операційного ризику інформаційної безпеки	$S(p_K(H1j)) = \frac{p_K(H1j)}{\sum_{j=1}^{4} p_K(H1j)}$ 100%	$S(p_K(H1j)) = \frac{p_K(H1j)}{\sum_{j=1}^{4} p_K(H1j)}$ 100%	$S(p_K(H1j)) = \frac{p_K(H1j)}{\sum_{j=1}^{4} p_K(H1j)}$ 100%	$S(p_K(H1j)) = \frac{p_K(H1j)}{\sum_{j=1}^{4} p_K(H1j)}$ 100%
Гранично допустимий коридор імовірнісної (кількісної) оцінки операційного ризику інформаційної безпеки за кожним j-м інцидентом (за сукупністю S банків)	$0 \le p_K(H1j) < fsr\left\{\min_s\{p_B(H1)_s\} \div fsr\{p_B(H1)_s\}\right\}$			
Бінарні показники за j інцидентами операційного ризику інформаційної безпеки	$NKbin_1$	$NKbin_2$	$NKbin_3$	$NKbin_4$
Імовірність виникнення операційного ризику інформаційної безпеки (кількісна оцінку ступеня операційного ризику)	$p_B(H1)$			

4. Перехід від імовірнісних показників $p_K(H1j)$ до бінарних показників $NKбін_j$ за j інцидентами операційного ризику інформаційної

безпеки: $NKбін_j$ набуває величини «1» у випадку попадання показника $p_K(H1j)$ у гранично допустимі межі або «0» у протилежному випадку.

5. Обчислення g_j - імовірності події $NKбін_j = 1$ ($g_{ij} = \frac{\sum_i NKbin_{ij}}{n}$) та b_j - імовірності події $NKbin_{ij} = 0$ ($b_{ij} = 1 - g_{ij}$) за j інцидентами операційного ризику інформаційної безпеки.

6. Знаходження імовірності появи операційного ризику інформаційної безпеки (кількісної оцінки ступеня операційного ризику інформаційної безпеки) $p_B(H1)$.

7. Визначення якісної оцінки рівня операційного ризику банку в сфері інформаційної безпеки на основі розрахованої кількісної оцінки його ступеня.

На базі отриманих бінарних показників $NKбін_j$ за j інцидентами ризику за формулою Байєса, що є основою імовірнісного підходу, визначимо імовірність ($p_B(H1)$) виникнення операційного ризику інформаційної безпеки (подія $H1$) за умови наявності інформації $B = (p_K(H11), p_K(H12), p_K(H13), p_K(H14))$ наступним чином (формули 1.24-1.25) [30]:

$$p_B(H1) = \frac{1}{1 + e^{\{\lambda_0 + L\}}} \tag{1.24}$$

$$L = \sum_{j=1}^{4} \lambda_j NKbin_j$$

$$\lambda_j = \ln\left(\frac{b_j(1-g_j)}{g_j(1-b_j)}\right), j = 1,...,4 \tag{1.25}$$

$$\lambda_{0j} = \ln\left(\frac{p(H2)}{p(H1)}\right) + \sum_{j=1}^{4} \ln\left(\frac{1-b_j}{1-g_j}\right)$$

де $p_B(H1)$ - імовірність виникнення операційного ризику інформаційної безпеки у випадку наявності інформації $B = (p_K(H11), p_K(H12), p_K(H13), p_K(H14))$;

L - інтегральний показник (зважена сума) бінарних характеристик $NKбін_j$ (наявна інформація щодо стану банку виходячи зі значень аналітичних показників);

$P(H1)$ - імовірність гіпотези $H1$;

$H1$ – висунута гіпотеза щодо виникнення операційного ризику інформаційної безпеки;

$P(H2)$ - імовірність протилежної гіпотези;

$NK = \{NKbin_j\}$ - бінарна компонента множини характеристик діяльності банку;

b_j - імовірність події $NK = \{NKbin_j\}$ для банку у розрізі j-го і операційного ризику інформаційної безпеки,

g_j - імовірність протилежної події.

На основі отриманої імовірнісної (кількісної) оцінки операційного ризику інформаційної безпеки ($p_B(H1)$) розраховується якісна характеристика рівня ризику:

- якщо $0 \le p_B(H1) < fsr\left\{\min_s\{p_B(H1)_s\} \div fsr\{p_B(H1)_s\}\right\}$, нормальний рівень ризику (де $fsr\{\ \}$ - середнє значення зазначених показників за сукупністю s банків);

- якщо $fsr\left\{\min_s\{p_B(H1)_s\} \div fsr\{p_B(H1)_s\}\right\} \le p_B(H1) < fsr\{p_B(H1)_s\}$, підвищений рівень ризику;

- якщо $fsr\{p_B(H1)_s\} \le p_B(H1) < fsr\left\{ fsr\{p_B(H1)_s\} \div \max_s\{p_B(H1)_s\}\right\}$, високий рівень ризику;

- якщо $fsr\left\{ fsr\{p_B(H1)_s\} \div \max_s\{p_B(H1)_s\}\right\} \le p_B(H1) \le 1$, критичний рівень ризику.

Отже, формування якісної системи управління інформаційної безпекою є особливо важливою складовою забезпечення ефективності функціонування банківського сектору. Сучасні тенденції розвитку економічної сфери вимагають від банківських установ бути готовими до існуючих ризиків

інформаційної системи. Неврахування цих ризиків може призвести до значних збитків банків. Ефективність управління операційними ризиками банку в сфері інформаційної безпеки досягається шляхом прийняття обґрунтованих рішень стосовно їх регулювання, основу яких становить кількісна оцінка ступеня цих ризиків. При цьому, запропонований механізм моделювання кількісної оцінки рівня операційного ризику банку в сфері інформаційної безпеки дозволить банківським установам значно знизити ризики інформаційного характеру та ефективно управляти операційними ризиками в напрямку інформаційних активів.

Пункт 1.3.2 цього звіту було виконано із використанням матеріалів проміжного звіту про НДР [11] та публікацій виконавців [18].

1.3.3 Система управління операційними банківськими ризиками у сфері інформаційної безпеки

Як зазначалось в попередньому підрозділі, ризики інформаційної безпеки є невіддільною частиною операційних ризиків банку. Відповідно, управління ними є складовою ризик-менеджменту банку, а, система управління ІБ має мати ризик-орієнтований характер. Це означає, що прийняття управлінських рішень здійснюється на підставі аналізу порівняння поточних ризиків інформаційної безпеки з прийнятними [31].

За результатами дослідження визначено, що управління ІБ банку досить часто розглядається за системним підходом як частина загальної системи управління банком, яка ґрунтується на підході, що враховує ризики інформаційної безпеки як операційні ризики, призначена для розробки, впровадження, функціонування, моніторингу, перегляду, підтримки та вдосконалення інформаційної безпеки [32].

За результатами дослідження вважаємо, що управління ІБ банку структурно являє собою систему, що містить основні підсистеми: методологічну (об'єкти, принципи, цілі та завдання, виконання яких забезпечить належний рівень ІБ банку), функціональну (сукупність інструментарію ідентифікації, оцінки, моніторингу та контролю величини ризиків інформаційної безпеки) та організаційно-управлінську (суб'єкти, через які проводиться реалізація регуляторних впливів, спрямованих на досягнення цілей та завдань забезпечення ІБ банку).

Ризики інформаційної безпеки як об'єкти управління входять в групу операційних ризиків банку, їх елементами є ризики внутрішніх процесів, людського фактора та системи. Як об'єкти управління вони є складними, оскільки виникають внаслідок значної кількості операцій зі значною кількістю контрагентів, на які, у свою чергу, впливає значна кількість різноспрямованих загроз зовнішнього та внутрішнього середовищ. Система управління ІБ банку має забезпечувати захищеність інформаційних активів з урахуванням впливу зовнішніх та внутрішніх загроз, а саме [33]:

– конфіденційність – забезпечення того, що інформація не може бути отримана неавторизованим користувачем і / або процесом;

– цілісність – забезпечення того, що інформація не може бути модифікована неавторизованим користувачем і / або процесом;

– цілісність системи – забезпечення того, що жоден компонент системи не може бути усунений, модифікований або доданий з порушенням політики безпеки;

– доступність – забезпечення такої властивості системи, що користувач і / або процес, який володіє відповідними повноваженнями, може використовувати ресурс відповідно до правил, встановлених політикою безпеки, не очікуючи довше заданого (малого) проміжку часу, тобто коли він знаходиться у вигляді, необхідному користувачу, в місці, необхідному користувачу, і в той час, коли він йому необхідний;

– спостережність – забезпечення такої властивості системи, що дозволяє фіксувати діяльність користувачів та процесів, використання пасивних об’єктів, а також однозначно встановлювати ідентифікатори причетних до певних подій користувачів та процесів з метою запобігання порушення політики безпеки, забезпечення відповідальності за певні дії.

Узагальнивши розробки з цієї тематики та нормативну базу [34], виділимо наступні принципи, яких слід дотримуватись при формуванні системи управління ІБ банку:

- адекватність реальним та потенційним внутрішнім та зовнішнім загрозам ІБ банку;
- комплексність – наявність всіх необхідних засобів (організаційних, методичних, технічних) та способів, спрямованих на захист інформаційних активів та захист всіх інформаційних активів, що визначеними значущими та цінними для банку;
- безперервність та своєчасність заходів захисту від реальних та потенційних загроз ІБ банку;
- висока продуктивність – обробка значних обсягів інформації без зниження швидкодії;
- надійність та відмовостійкість через застосування технологій кластеризації, віртуалізації, балансування навантаження та ін.;
- інформаційне забезпечення через наявність збору, аналізу даних про інциденти та реагування на події безпеки;
- достатність всіх ресурсів, у тому числі фінансових, для сталого розвитку систем ІБ банку.

Організаційно-управлінська підсистема поєднує всіх суб’єктів управління, долучених до процесів забезпечення ІБ банку. При цьому до нього входять як ті суб’єкти управління, що формують загальну систему ІБ, так і ті, через які проводиться регулювання ризиків ІБ як складової ризик-менеджменту.

При цьому слід наголосити на тому, що кожен банк обирає таку модель, що найкращим чином відповідає особливостям його діяльності, характеру та

обсягу банківських, фінансових послуг, рівню розвитку та структурі його інформаційних систем, а також наявним можливостям та потребам у сфері забезпечення ІБ та ризик-менеджменту (рис. 1.38).

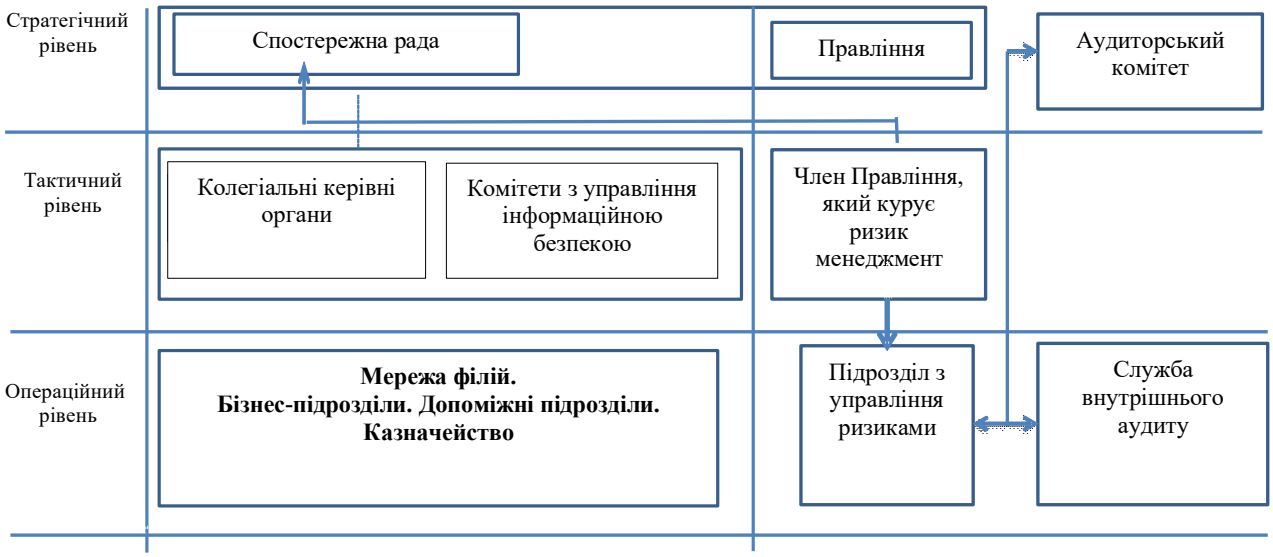


Рисунок 1.38 – Організаційно-управлінська підсистема управління ризиками ІБ банку

На стратегічному рівні повноваження щодо ефективного забезпечення управління ризиками ІБ реалізують спостережна рада та правління. Саме вони визначають основні контури організаційно-управлінської структури забезпечення ІБ, розробляють та затверджують політику та стратегію розвитку ІБ, політику та стратегію управління ризиками ІБ, здійснюють загальний контроль за процесами управління ІБ та ризиками ІБ банку [34, 35].

Правління банку несе відповідальність за безпосередню організацію та реалізацію процесу ризик-менеджменту, в тому числі, за забезпечення виявлення, оцінювання, контроль, та моніторинг ризиків інформаційної безпеки як частини операційних ризиків [35].

Тактичний рівень включає функції управління ризиками ІБ, що виконуються на рівні вищого керівництва та комітетів, тобто схвалення політики управління ризиками, та процесів управління ризиками та створення

адекватних внутрішніх систем та механізмів контролю, так щоб ризик підтримувався у межах допустимих рівнів. При цьому, відповідно до вимог НБУ, банк зобов'язаний сформувати колективний керівний орган з питань впровадження та функціонування системи управління ІБ або наділити цими повноваженнями наявний колективний керівний орган з чітким визначенням завдань, функцій та відповідальності [34]. До його складу мають ввійти голова правління та / або його заступник, що відповідає за інформаційну безпеку; керівники підрозділів – власників критично важливих інформаційних активів та критичних бізнес-процесів, до яких вони відносяться; керівники підрозділу з управління ризиками. Банки України реалізують цю вимогу, у переважній більшості з них створено окремі комітети з управління інформаційною безпекою, що підпорядковуються правлінню, рішення якого є обов'язковими для виконання усіма співробітниками банку. На підрозділ з управління ризиками покладається забезпечення надійного процесу виявлення, оцінки, контролю та моніторингу ризиків ІБ банку [35]. Також на цей підрозділ покладаються функції розробки внутрішньої нормативної бази.

Операційний рівень включає функції управління ризиками ІБ, що здійснюються у підрозділах банку шляхом відповідного контролю, керуючись відповідними операційними процедурами та довідниками, затвердженими вищим керівництвом. Основна роль тут відводиться підрозділам – власникам критично важливих інформаційних активів та критичних бізнес-процесів, до яких вони відносяться. Ці підрозділи зобов'язані впроваджувати політики, процедури та інструментарій з управління ризиками ІБ у свою діяльність, керуючись політикою та стратегією в сфері ІБ, нормативними документами банку у сфері управління ризиками. Вони виконують наступні функції:

- забезпечення функціонування процесів підтримки діяльності у сфері управління ризиками ІБ у межах компетенції підрозділу;
- проведення ідентифікації та формування управлінської звітності про операційні події (інциденти ризиків ІБ);
- дотримання індикаторів якості звітів про операційні події;

- участь у наступному контролі якості даних про операційні події;
- постійний аналіз процесів, продуктів, систем для ідентифікації потенційних ризиків ІБ у межах сфери відповідальності;
- ідентифікація значних ризиків ІБ для сценарного аналізу, в тому числі стрес-тестування;
- участь у сценарному аналізі ризиків ІБ та в їх стрес-тестуванні;
- проведення експертної оцінки ризиків ІБ;
- первинна ідентифікація та оцінка впливу ризиків ІБ при впровадженні нових банківських продуктів, систем, проектів, змін у бізнес-діяльності або організаційній структурі тощо;
- розробка та впровадження ключових індикаторів ризиків ІБ, забезпечення регулярного моніторингу їх динаміки;
- розробка та впровадження заходів з обмеження (контролю) ризиків ІБ;
- підготовка регулярних звітів з ризиків ІБ (збитки, індикатори, сценарії, експозиція до ризику, заходи з обмеження ризику та інш.);
- забезпечення участі працівників підрозділу у регулярних тренінгах з ризиків ІБ;
- підтримка та супроводження впровадження нових ІТ-систем та / або рішень з управління ризиків ІБ на рівні та в межах функцій підрозділу.

Служба внутрішнього аудиту не бере безпосередньої участі в процесі управління ризиками ІБ та ІБ банку, її роль зводиться до оцінки адекватності цих систем цілям та задачам банку в цій сфері [35]. Функціональна підсистема визначається як сукупність інструментарію та дій суб'єктів управління по формуванню політики та стратегії управління ІБ банку, а також ідентифікації, оцінці, моніторингу та контролю величини ризиків ІБ як складової операційних ризиків банку (рис. 1.39).

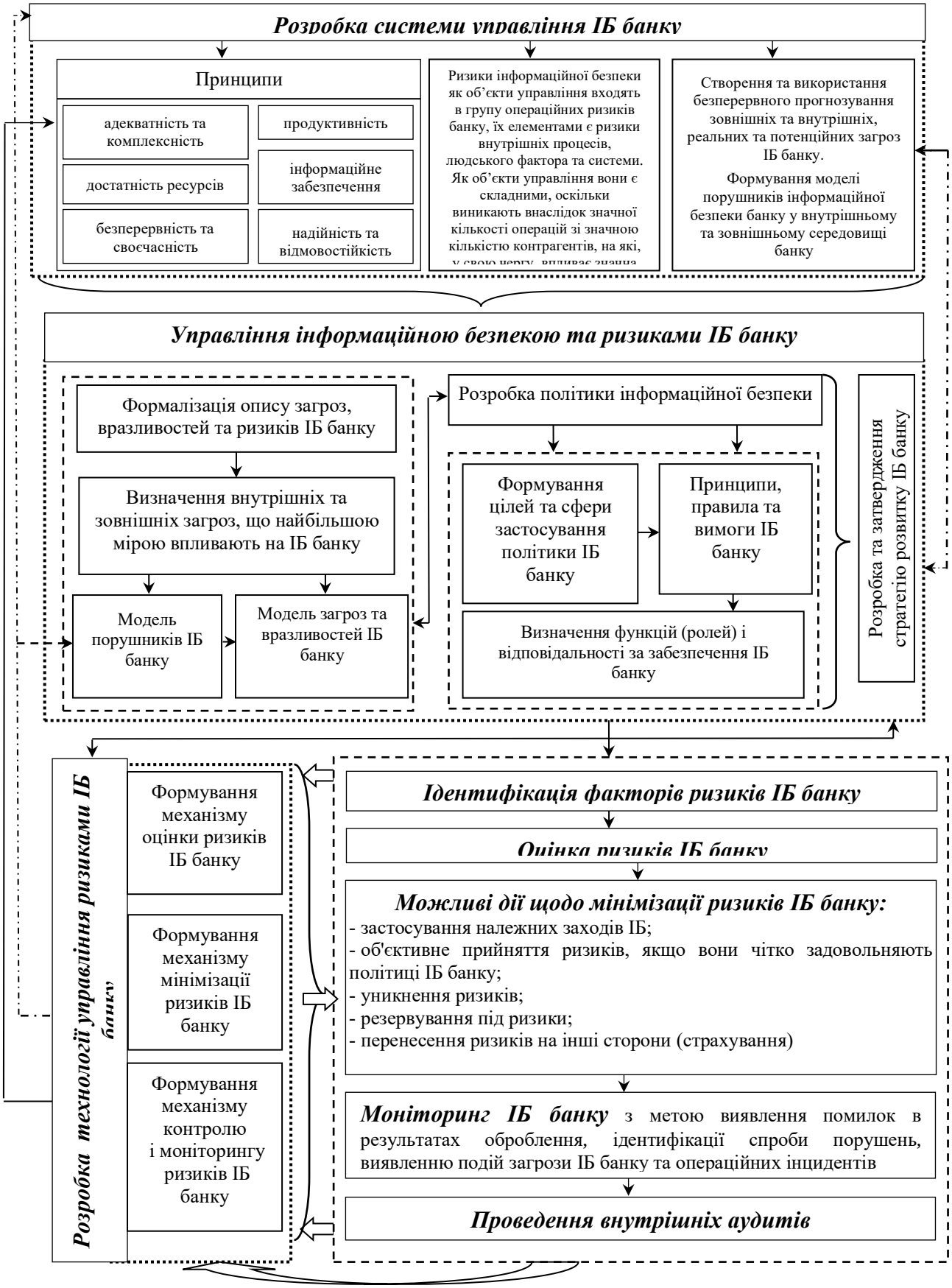


Рисунок 1.39 – Основні функції управління ІБ та ризиками ІБ банку

В основі управління ІБ банку має бути ефективна політика інформаційної безпеки та комплекс заходів, що забезпечують її якісне виконання. Банки України зобов'язані розробити, затвердити в установленому порядку та підтримувати політику ІБ в актуальному стані на основі її перегляду не рідше, ніж один раз на рік [34].

Узагальнивши політики ІБ банків України, нами визначено, що вони включають наступні змістовні розділи: визначення мети політики, сфери її застосування, перелік об'єктів, на які розповсюджується дія ІБ банку, ролі та відповідальність суб'єктів забезпечення ІБ банку, відповідальність працівників банку за інформаційну безпеку, принципи та підходи ІБ банку.

Системним документом, що впливає на забезпечення ІБ, є стратегія її розвитку, що має обов'язково розроблятись та затверджуватись банками. Її зміст має узгоджуватися з політикою ІБ, стратегічними цілями банку, пов'язаними з впровадженням нових бізнес-процесів / банківських продуктів з використанням технологій, що потребують захисту інформації, а також враховувати планування розвитку інфраструктури та заходів ІБ для мінімізації ризиків ІБ [34].

Також банк має ефективно розробляти, впроваджувати та тестувати плани відновлення бізнесу, зокрема розробити та затвердити план забезпечення безперервності діяльності, в якому враховано безперервність функціонування заходів ІБ [34].

Важливим для забезпечення ІБ банку є формування ефективної системи управління ризиками ІБ, що здійснюється за циклом ризик-менеджменту «ідентифікація – оцінка та аналіз – мінімізація – моніторинг та контроль».

Для налагодження здійснення ідентифікації ризиків ІБ банку слід, по-перше, налагодити співпрацю робітників підрозділу з управління ризиками з працівниками підрозділів – власників критично важливих інформаційних активів та критичних бізнес-процесів, по-друге, розробити систему ранньої ідентифікації ризиків, тобто визначення подій, що непрямо впливають на появу ризиків ІБ банку, але є підставою для їх виникнення, по-третє, розробити систему

ідентифікації окремого виду ризику ІБ банку, в тому числі тих, що виникають при аутсорсингу.

Ефективна оцінка ризиків ІБ у грошовому вигляді напряму залежить від правильної їх ідентифікації відповідно до напрямку діяльності банку. Слід зазначити, що використання математико-статистичних моделей, які використовуються для оцінки ринкових, кредитних ризиків та ризиків ліквідності, майже неможливе внаслідок як самої природи ризиків ІБ (різноманітні загрози, що викликають їх появу, та неможливість їх уникнення), так і внаслідок особливостей процесу управління (ці ризики потрібно мінімізувати, а не оптимізувати, отже, інструменти регулювання та контролю є особливими).

Базовою методикою ідентифікації ризиків ІБ є аналіз причинно-наслідкових зв'язків зовнішніх та внутрішніх загроз, реалізація яких може привести до певних відхилень від цільових параметрів ІБ банку та цільового перебігу бізнес-процесу. Наслідком цього стають фінансові втрати, погіршення репутації, втрати транзакцій та клієнтів, санкції наглядових органів та юридична відповідальність (табл. 1.14).

У практичній діяльності банки можуть використовувати підходи до оцінки ризиків ІБ як частини операційних ризиків, що охарактеризовані нижче.

Top-down models (низхідні моделі) розглядають ризики ІБ з точки зору кінцевих результатів діяльності банку, тобто тих наслідків, до яких вони приводять. Як правило, оцінка визначає ті кошти, що банк може втратити у разі настання ризикової події (Exposure Indicators). Для ідентифікації ризиків використовується база даних операційних інцидентів (подій, що призвели до збитків). Ризики об'єднуються в групи та класифікуються.

Bottom-up models – висхідні моделі – при роботі з ними увага акцентується на джерелах, тобто причинах виникнення ризиків ІБ. Ідентифікація ризиків здійснюється шляхом оцінки реакції працівників, процесів, технологій на внутрішні та зовнішні загрози ІБ.

Таблиця 1.14 – Наслідки реалізації ризиків ІБ банку

	Характеристика	Вид	Характеристика	Підвиди
Фінансові втрати	вимірюються у грошовому еквіваленті, безпосередньо впливають на фінансовий результат діяльності банку	Очікувані	сума втрат, що повторюються (виникають із частотою не рідше одного разу на календарний рік) та знаходяться у діапазоні оцінки грошового еквівалента очікуваних фінансових втрат	структуруються за масштабами втрат та визначаються в кожному банку індивідуально
		Неочікувані	максимальні потенційні втрати внаслідок суттєвих недоліків (помилок) системи внутрішнього контролю або надзвичайних зовнішніх подій, що знаходяться у діапазоні оцінки грошового еквівалента неочікуваних фінансових втрат	
Нефінансові втрати	безпосередньо не впливають на фінансовий результат діяльності, але можуть призвести до несприятливих для банку наслідків	Очікувані	значимість очікуваного нефінансового впливу на горизонті одного календарного року	втрата іміджу або репутації банку - втрата транзакцій; - втрата клієнта; - втрата груп клієнтів або портфелю санкції та стягнення
		Неочікувані	максимальний потенційний нефінансовий вплив внаслідок суттєвих недоліків (помилок) системи внутрішнього контролю або надзвичайних зовнішніх подій	

Основним способом є декомпозиція банка та всієї діяльності на кінцеві бізнес-процеси з виділенням критичних для інформаційної безпеки за результатом їх оцінювання за критеріями конфіденційності, цілісності, доступності. Результати висхідної моделі можуть бути використані, наприклад, для проектування та оцінки методів управління ризиками ІБ, виявлення та оцінки ключових факторів ризиків ІБ.

RSCA – самооцінка, що має здійснюватися усіма підрозділами банку з метою самостійного визначення можливих ризиків ІБ. Класичний підхід має на увазі участь в самооцінці керівників, підрозділів, ключових працівників банку.

Скорингові карти використовуються для оцінки ризиків за визначеною групою підрозділів банку, працівників, або регіонів та дозволяють отримати за

допомогою набору питань оцінку ступеню ризику тієї чи іншої події. Оцінка, отримана за допомогою скорингових карт, має суб'єктивний характер, однак, дозволяє визначити ймовірність настання подій ризику ІБ та наочно визначити, які підрозділи банку є їх джерелами. Скорингові карти також можуть бути використані для самооцінки ризику.

Аналіз ключових індикаторів ризику (надалі аналіз КІР) – інструмент оцінки ризиків ІБ, що базується на дослідженні динаміки показників ризику в окремих бізнес-процесах або діяльності банку в цілому, та використовується для моніторингу, контролю та раннього попередження щодо зміни показників ризиків ІБ у бізнес-процесах / діяльності банку. Аналіз КІР застосовується, насамперед, у критичних бізнес-процесах банку з метою моніторингу притаманних певному бізнес-процесу ризиків, що значною мірою створюють загрози ІБ.

Метою застосування аналізу КІР є своєчасний та періодичний контроль показників ризиків ІБ, спрямований на виявлення негативних тенденцій та уникнення випадків їх реалізації у майбутньому. Класифікація ключових індикаторів ризиків ІБ базується на наступних типах:

- синхронні індикатори – показники, що являють дані щодо зафіксованих втрат та включають показники реалізації помилок або нереалізованих втрат (наприклад, сума втрат за успішними шахрайськими операціями з платіжними картками, сума неуспішних шахрайських операцій з платіжними картками);

- казуальні індикатори – показники, пов'язані з первинною причиною події реалізації ризиків ІБ (наприклад, частка часу недоступності інформаційної системи / ресурсу);

- індикатори ефективності контролю – показники поточного моніторингу виконання контролів (наприклад, сума коштів, витрачена при укладанні контрактів з провайдерами).

Граничні значення цих показників розраховуються на основі історичних даних (емпіричний підхід) та / або експертних оцінках співробітників банку.

Залежно від того, у межах яких граничних значень знаходиться показник КІР, характеризується рівень ризиків ІБ у відповідних йому бізнес-процесах.

Сценарний аналіз ризиків ІБ – інструмент оцінки, що досліджує неочікувані, малоймовірні, але потенційно можливі події, реалізація яких може призвести до суттєвих втрат або катастрофічно вплинути на можливість виконання банком притаманних йому функцій.

Розробка сценаріїв ризиків ІБ базується на принципі фокусування на можливому розвитку подій у майбутньому, базуючись на подіях / передумовах, що до поточного моменту не були зафіксовані у банку. Сценарний аналіз ризиків ІБ банку може передбачати застосування наступних сценаріїв: втрата або викрадення комерційної / банківської таємниці співробітниками або третіми особами; порушення фідуціарних зобов'язань перед клієнтами, вимог конфіденційності, конфлікт інтересів; глобальні збої інфраструктури; збої ключових ІТ-систем; помилки в операціях або процесах їх обробки, злам внутрішньої інформаційної чи платіжної системи банку. Сценарний аналіз дає визначення переліку подій, що мають малу ймовірність виникнення, але можуть призвести до значних збитків, а згодом – до банкрутства банку.

Після визначення переліку цих подій кожен банк має провести стрес-тестування та розрахувати максимально можливі збитки, що можуть виникнути унаслідок їх реалізації та розробити необхідні програми управління.

Результати оцінки ризиків ІБ використовуються для прийняття управлінських рішень щодо розподілу ресурсів задля мінімізації виявлених ризиків. Серед виділених ризиків ІБ банку, притаманних цьому бізнес-процесу, мають виділятися критичні ризики, тобто сукупність можливих наслідків реалізації ризиків ІБ, що, серед інших, мають значний вплив на перебіг бізнес-процесу та / або на обсяг / величину ефекту, що виникатиме в результаті реалізації цього ризику в контексті забезпечення ІБ банку.

З метою зменшення рівня ризику ІБ банку та його складових, а саме ймовірності настання, втрат внаслідок реалізації та втрат за вже реалізованими випадками банк має застосовувати відповідні заходи щодо їх мінімізації.

Зважаючи на відсутність ефективної системи оцінки ризиків ІБ, існує досить обмежений інструментарій їх мінімізації.

Найбільш розповсюджений метод управління – створення резервів під ризики. Методом, що отримав розповсюдження в країнах Західної Європи та Північної Америки, є страхування. Крім поширених серед банків полісів майнового страхування та страхування відповідальності, що можуть вважатися факторами, які знижують ризики ІБ, значний інтерес становить поліс BBB (Bankers Blanket Bond) – комплексна програма страхування від злочинів та професійної відповідальності фінансових інститутів. Ця програма може включати три види страхування, покликані забезпечити зниження операційних ризиків банку: страхування BBB; від електронних та комп'ютерних злочинів; професійної відповідальності фінансового інституту.

Основною статтею BBB є страхування від збитків у результаті шахрайства персоналу. Поліс BBB також надає страховий захист від збитків у результаті операцій, здійснених банком на підставі підроблених письмових документів та інструкцій, відшкодуванню також підлягає збиток від операцій з підробленими цінними паперами та фальшивою валютою. Покриття охоплює й «класичні» злочини – такі, як пограбування банку, крадіжка цінного майна з його приміщень, а також в процесі інкасації, а також пошкодження і загибель цінного майна з будь-якої причини.

Поліс страхування від електронних та комп'ютерних злочинів, що придбаний як доповнення до стандартного BBB, забезпечує захист від збитків у результаті несанкціонованого проникнення в електронні та комп'ютерні системи банку та зміни даних, що знаходяться в них; дії комп'ютерного вірусу; здійснення операцій за шахрайськими інструкціями, одержаними за електронними каналами зв'язку (наприклад, SWIFT); операціями з бездокументарними цінними паперами; зламу комп'ютерних систем клієнта, здійсненого з комп'ютерів банку (наприклад, неблагонадійними співробітниками); загибелі та пошкодження електронних даних та їх носіїв.

Третім елементом у системі комплексного страхування банків, не пов'язаним з криміналом, але таким, що значно збільшує загальний ступінь захисту, є поліс страхування професійної відповідальності (Professional Indemnity Policy) співробітників банку за недбалості й ненавмисні помилки, допущені в процесі виконання ними професійних обов'язків перед клієнтами.

Таким чином, цей комплекс страхових продуктів надає найповніший захист діяльності банку, причому комплексність полягає ще й у тому, що під покриття, за взаємною угодою, підпадає не тільки головна компанія, але і вся система філій банку, причому нові підрозділи автоматично включаються в застраховану систему з подальшою доплатою премії страхувальникам.

Найбільш складним етапом в управлінні ризиками ІБ є формування ефективної системи контролю, оскільки важко оцінити ефективність оцінки, а, тим більше, управління, завдяки їх багатовекторності та невизначеності навіть після настання ризикової події. Доцільним є використання наступних елементів контролю та моніторингу управління ризиками ІБ:

- здійснення контролю за виконанням встановлених правил та процедур діяльності банку за допомогою використання принципу багатосторонньої відповідальності за здійснення операцій;

- використання програм-менеджерів та програм підтримки прийняття рішень при здійсненні операцій в інформаційній системі банку, що дозволить оптимальним чином розподілити обов'язки, права та відповідальність між користувачами інформаційної системи, розробити зручний інтерфейс для програм, що призначені для відстеження здійснення несанкціонованих операцій як з внутрішніх, так і зовнішніх терміналів;

- визначення критеріїв ефективності застосування різноманітних програм страхування за допомогою порівняння сум страхових тарифів із сумами отриманих страхових відшкодувань унаслідок настання страхових подій.

Чинним законодавством регулюються, здебільшого, превентивні інструменти мінімізації ризиків ІБ банку, а не подальшого контролю за дотриманням визначених правил та процедур, тому банкам знадобиться

міжнародний досвід, щоб сформувати цілісну систему управління ІБ в цілому, та ризиками ІБ, зокрема.

Пункт 1.3.3 цього звіту було виконано із використанням матеріалів проміжного звіту про НДР [11] та публікацій виконавців [18].

1.4 Розробка комплексу превентивних заходів до попередження настання ситуацій, які класифікуються як кіберзагроза або шахрайство

1.4.1 Розробка моделі впливу макроекономічних факторів на формування схильності до шахрайства в банківській сфері

Виникнення шахрайства здійснюється в умовах складної взаємодії комплексу чинників економічного, політичного та соціального характеру. Стан макроекономічного рівня країни дозволяє сформувати передумови виникнення шахрайства. Всі фактори впливають на систему і визначають її поведінку. За даних умов, вирішено оцінити вплив макроекономічних факторів на формування схильності до шахрайства. Виділимо ситуації, в яких можуть формуватися вплив на шахрайство, що дозволить розробити основні гіпотези:

– якщо в країні мінімальна заробітна плата є низькою, тоді у населення країни зростає схильність до шахрайських операцій;

– в країні в якій велика кількість населення має дохід нижче валового доходу схильність до здійснення шахрайських операцій зростаю;

– коли в країні йде поширення корупційної складової, яка впливає і сильно заважає ефективному державному управлінню, можемо припустити, що схильність до здійснення шахрайських операцій буде збільшуватися;

– в країні в якій держава не в змозі контролювати цілісність території, та не в змозі впливати на демографічну, соціальну та політичну ситуацію в країні можливе виникнення шахрайства;

– коли суспільство не має право вибору на бажану роботу, виробництво товарів, різних витрат та інвестицій, тоді в населення виникає схильність до шахрайства більше ніж в суспільстві, яке має вільні економічні права;

– країни із низькою купівельною спроможністю населення характеризуються вищою ймовірністю виникнення шахрайських операцій;

– в тому випадку, коли держава намагається створювати умови для благополуччя людей, то можемо допустити, що ймовірність виникнення шахрайства буде на низькому рівні;

– в країні в якій рівень безпечності проживання є на високому рівні, то виникнення шахрайства буде не низькому рівні;

– висока схильність до виникнення шахрайства буде в країнах, в яких буде збільшуватися рівень цін на товари та послуги, які купує населення для невиробничого споживання, а купівельна спроможність населення буде залишатися на низькому рівні;

– можемо допустити, що рівень шахрайства в країні буде змінюватися, коли буде зростати загальна кількість населення, та в залежності від розподілу чоловіків та жінок проживаючих в даній країні;

– якщо держава створює умови для процвітання країни, то ймовірність шахрайських операцій буде на низькому рівні.

Побудова моделі передбачає використання макроекономічних показників окремої країни, які будуть вказувати на схильність до шахрайства населення країни: індекс бідності, індекс споживчих цін, рівень злочинності, ВВП на душу населення, кількість чоловіків та жінок в країні та інші.

Вибір цих факторів обумовлений тим, що різні макроекономічні дії в країні спричиняють формування в населенні схильності до здійснення шахрайства. Зміни в економічному, соціальному та політичному становищі країни, спричиняють виникненню шахрайських операцій. Виникнення шахрайства здійснюється в умовах складної взаємодії комплексу чинників економічного, політичного та соціального характеру. Всі фактори впливають на систему і визначають її поведінку. Виходячи з даних ситуацій розроблено концептуальну

модель оцінки впливу макроекономічних факторів на формування схильності до шахрайства в банківській сфері (рисунок 1.40).

Рисунок 1.40 – Концептуальна модель оцінки впливу макроекономічних факторів на формування схильності до шахрайства

В процесі підготовки до побудови математичної моделі впливу макроекономічних показників на формування схильності до шахрайства в якості вхідних даних було використано різні макроекономічні показники декількох

країн «Х», за останні 26 років. Інформація містить 18 вхідних змінних, виключаючи цільову змінну. Змінні представлені в таблиці 1.15.

Таблиця 1.15 – Опис вхідних змінних

Ім'я змінної	Економічний зміст	Роль	Тип	Допустимі значення
(Y)	Збитки від шахрайських операцій	цільова	nominal	>=0
(X_1)	Мінімальна заробітна плата	вхідна	nominal	>0
(X_2)	Показник сприйняття корупції	вхідна	interval	[0;100]
(X_3)	Індекс економічної свободи	вхідна	interval	[0;100]
(X_4)	Індекс цивільної свободи	вхідна	interval	[0;10]
(X_5)	Індекс процвітання	вхідна	interval	[0;100]
(X_6)	Індекс політичних прав	вхідна	interval	[0;100]
(X_7)	Індекс мира	вхідна	interval	[0;5]
(X_8)	Індекс споживчих цін	вхідна	nominal	>=0
(X_9)	Рівень бідності	вхідна	nominal	>=0
(X_{10})	Населення	вхідна	nominal	
(X_{11})	Рівень інфляції	вхідна	nominal	>=0
(X_{12})	ВВП на душу населення	вхідна	nominal	>=0
(X_{13})	Кількість жінок	вхідна	nominal	>=0
(X_{14})	Кількість чоловіків	вхідна	nominal	>=0
(X_{15})	Фіксовані телефонні абонементи	вхідна	nominal	>=0
(X_{16})	Кількість безпечних інтернет серверів	вхідна	nominal	>=0
(X_{17})	Індекс щастя	вхідна	interval	[0;100]
(X_{18})	Рівень злочинності	вхідна	nominal	>=0
(X_{19})	Індекс людського розвитку	вхідна	interval	[0;1]
(X_{20})	Індекс недієздатності держави+	вхідна	nominal	[0;100]

Вибірка даних складається 26 спостережень, взятих з шести країн: Україна та Великобританія, США, Канада, Росія та Австралія.

Змінна Y показує збитки від шахрайських операцій в банківській сфері даної країни.

Змінна X_1 показує розмір заробітної плати за просту, некваліфіковану працю, нижче якого не може встановлюватися оплата за виконану роботу.

Змінна X_2 вказує на рівень корупції в країн, відображає поширення корупційної складової в державному секторі. У рейтингу відображено сприйняття корупції від 100 (немає корупції) до 0 (сильна корупція).

Змінна X_3 відображає рівень економічної свободи в країні, тобто характеризує рівень втручання держави в економічний сектор. В економіко вільних країнах особи мають право у виборі роботи, виробництві товарів та послуг, витратах та інвестиційних діях за допомогою підтримки з боку держави. Базується на 10 індексів, та вимірюється від 0 (мінімальна свобода) до 100 (максимальна свобода).

Змінна X_4 відображає рівень громадської свободи в країні, тобто показує відсутність примусових обмежень. Базується на великій кількості показників з різних сфер, а саме верховенство закону, безпеку, пересування, релігія, громадянське суспільство, розмір уряду, інформація, право власності, свобода торгівлі на міжнародному рівні, регулювання кредиту, праці та бізнесу. Показник розраховується від 0(максимальна свобода) до 10 (мінімальна свобода)

Змінна X_5 показує оцінку світового балансу і благополуччя. Індекс складається з багатої кількості показників, які об’єднані в дев’ять категорій, які показують різні аспекти життя населення та параметри суспільного благополуччя. Рейтинг вимірюється від 0 (низький рівень) до 100 (високий рівень).

Змінна X_6 показує забезпечення країни правової середи, яка базується на принципах верховенства права.

Змінна X_7 показує рівень надійності проживання в країні. Показник враховує як внутрішні фактори, а саме рівень насильства в країні, та рівень злочинності, так і зовнішні – міжнародні відношення країни. Вимірюється від 0 (безпечні для проживання) до 5 (небезпечні для проживання).

Змінна X_8 показує зміну в часі загального рівня цін на товари та послуги в країні.

Змінна X_9 відображає долю населення сімейний дохід якої нижче абсолютного рівня.

Змінна X_{10} показує загальну кількість людей проживаючих у даній країні.

Змінна X_{11} відображає знецінення грошей.

Змінна X_{12} відображає рівень економічного розвитку.

Змінна X_{14} та X_{13} показує кількість чоловіків і жінок проживаючих в країні.

Змінна X_{15} відображає кількість фіксованих телефонних абонентів.

Змінна X_{16} показує кількість безпечних інтернет серверів.

Змінна X_{17} відображає стан захисту довкілля, та добробут населення. Вимірюється шляхом порівняння рівня життя в країнах світу за допомогою ВВП на душу населення або за ІРЛП.

Змінна X_{18} показує наскільки кримінальна активність в країні.

Змінна X_{19} відображає оцінку прогресу людського розвитку у трьох сферах, а саме довготривале та здорове життя населення, доступу до знань, гідний рівень життя суспільства.

Змінна X_{20} характеризує спроможність держави контролювати цілісність території, та за допомогою інструментів впливати на демографічну, соціальну та політичну ситуацію в країні. Країни в яких високий рівень злочинності, корупційної складової, також де багато біженців або іммігрантів, то їх економіка буде мати чисельні проблеми, та мати низький рівень недієздатності держави.

Для виявлення значимості кожного фактору та збільшення точності результатів використовується рівняння стандартизованої множинної регресії [36]. Стандартизоване рівняння регресії показує на скільки зміниться результати за умови, що значення відповідної змінної зміниться на одну одиницю при незмінному середньому рівні інших факторів.

Стандартизоване рівняння регресіє буде будуватися до трьох складових: економічної, політичної та соціальної.

Рівняння моделі для економічної сфери наведено в наступній формулі:

$$t_{y(\text{e})} = \beta_1 \cdot t_{x3} + \beta_2 \cdot t_{x12} + \beta_2 \cdot t_{x11} + \beta_2 \cdot t_{x8} + \beta_2 \cdot t_{x9} + \beta_2 \cdot t_{x1} + \\ + \beta_2 \cdot t_{x17} + \varepsilon, \qquad (1.26)$$

де t_{x1} – стандартизована змінна, яка показує мінімальну заробітну плату населення країни;

t_{x3} – стандартизована змінна, яка показує індекс економічної свободи;

t_{x8} – стандартизована змінна, яка показує рівень споживчих цін;

t_{x9} – стандартизована змінна, яка показує рівень бідності населення;

t_{x11} – стандартизована змінна, яка показує рівень інфляції;

t_{x12} – стандартизована змінна, яка показує ВВП на душу населення;

t_{x17} – стандартизована змінна, яка показує індекс щастя.

Рівняння моделі для політичної сфери наведено в наступній формулі:

$$t_{y(\text{п})} = \beta_1 \cdot t_{x18} + \beta_2 \cdot t_{x3} + \beta_2 \cdot t_{x2} + \beta_2 \cdot t_{x4} + \beta_2 \cdot t_{x7} + \beta_2 \cdot t_{x20} + \varepsilon, \qquad (1.27)$$

де t_{x2} – стандартизована змінна, яка показує рівень сприйняття корупції;

t_{x3} – стандартизована змінна, яка показує індекс політичних прав;

t_{x4} – стандартизована змінна, яка показує індекс цивільної свободи;

t_{x7} – стандартизована змінна, яка показує індекс миру;

t_{x18} – стандартизована змінна, яка показує рівень злочинності;

t_{x20} – стандартизована змінна, яка показує індекс недієздатності держави.

Рівняння моделі для соціальної сфери наведено в наступній формулі:

$$t_{y(\text{с})} = \beta_1 \cdot t_{x4} + \beta_2 \cdot t_{x5} + \beta_2 \cdot t_{x7} + \beta_2 \cdot t_{x9} + \beta_2 \cdot t_{x10} + \beta_2 \cdot t_{x13} + \qquad (1.28)$$
$$+\beta_1 \cdot t_{x14} + \beta_2 \cdot t_{x15} + \beta_2 \cdot t_{x16} + \beta_2 \cdot t_{x17} + \beta_2 \cdot t_{x19} + \varepsilon,$$

де t_{x4} – стандартизована змінна, яка показує індекс цивільної свободи;

t_{x5} – стандартизована змінна, яка показує індекс процвітання;

t_{x7} – стандартизована змінна, яка показує індекс миру;

t_{x9} – стандартизована змінна, яка показує рівень бідності;

t_{x10} – стандартизована змінна, яка показує населення країни;

t_{x13} – стандартизована змінна, яка показує кількість чоловіків, які проживають в країні;

t_{x14} – стандартизована змінна, яка показує кількість жінок, які проживають в країні;

t_{x15} – стандартизована змінна, яка показує кількість фіксованих телефонних абонентів;

t_{x16} – стандартизована змінна, яка показує кількість безпечних інтернет серверів;

t_{x17} – стандартизована змінна, яка показує індекс щастя;

t_{x19} – стандартизована змінна, яка показує індекс людського розвитку.

Модель регресії в стандартному масштабі припускає, що всі значення перетворюються в стандартизовані значення за формулою:

$$t_j = \frac{xi - \bar{x}\imath}{\sigma xi} \tag{1.29}$$

де xi значення в xi спостереженні:

$$t_y = \frac{y - \bar{y}}{\sigma y} \tag{1.30}$$

Для яких середні значення дорівнює нулю, а середнє квадратичне відхилення одиниці.

Для відбору найбільш значущих факторі було використано покрокову або гребеневу регресію. Гребенева регресія має найбільш точні результати, вона штучним способом занижує коефіцієнт кореляції, для розрахунку найбільш стійких оцінок коефіцієнтів регресії.

Всі змінні задані як нормовані стандартизовані коефіцієнти регресії, тому їх можна порівняти між собою. Також при порівняні факторів можна їх ранжувати між собою за впливом на результат [36].

Алгоритм визначення ступеня переваги кожної альтернативи за допомогою метрики Мінковського:

1. формування матриці значень часткових критеріїв альтернатив;
2. розділення значень на стимулятори та дестимулятори;
3. визначення стандартних значень часткових критеріїв для стимуляторів та дестимуляторів;
4. формування матриці значень часткових критеріїв альтернатив;
5. визначення ваги кожного показника;
6. визначення ступеня переваги кожної альтернативи.

Створення функції корисності $F(x_i)$ для кожної альтернативи відбувається за допомогою згортання векторного критерія f в скалярний через різні типи згортки [37]:

– адитивної:

$$F(x_i) = \sum_{j=1}^{n} \omega_j \cdot x_{ij} \tag{1.31}$$

– мультиплікативної:

$$F(x_i) = \prod_{j=1}^{n} x_{ij}^{\omega_j} \tag{1.32}$$

Які вважаються найпоширенішими [38] для формування класичного виду адитивно-мультиплікативної згортки.

Недоліки методів згортки:

– на адекватність впливає розподіл альтернатив у вибірці критеріїв [38];

– недостане значення одного критерію може компенсуватися значенням іншого критерія [39];

– часткові функції корисності повинні бути односпрямовані [40].

Нормування часткових критеріїв до єдиного значення зводиться за допомогою часткового критерію, максимального значення x_{maxj}.

Під час формування функції корисності треба брати до уваги, що одна частина змінних повинна бути максимізована, а інша мінімізована [41]. Тому необхідно критерії поділити на:

- стимулятори:

$$f_j(x) \to max, \qquad j = \overline{1,k}, x \epsilon S \tag{1.33}$$

- дестимулятори:

$$f_j(x) \to min, \qquad j = \overline{1,k}, x \epsilon D \tag{1.34}$$

де S та D – множина критеріїв.

Нормування стимуляторів проводиться за формулою 1.35:

$$x'_{ij} = \frac{x_{ij}}{x_{maxj}} \tag{1.35}$$

Нормування дестимуляторів проводиться за наступною формулою 1.36:

$$x'_{ij} = \frac{x_{ij}}{x_{minj}} \tag{1.36}$$

Метрикою являється числова функція яка знаходить відстань між векторами. Метрики для векторів повинні задовольняти наступні аксіоми:

$$\rho(y,z) \geq 0 \ ,\rho(y,z) = 0, y \Leftrightarrow z; \tag{1.37}$$

$$\rho(y,z) = \rho(z,y); \tag{1.38}$$

$$\rho(y,z) \le \rho(w,y) + \rho(y,z). \tag{1.39}$$

Метрика Мінковського має наступний вигляд:

$$\rho(y,z) = (\sum_{i=1}^{n} a_i^s \cdot |y_i - z_i|^r)^{1/r} \tag{1.40}$$

Функція корисності матиме вигляд:

$$F(x_i) = 1 - \sqrt[n]{\sum_{j=1}^{k} \omega_j \cdot \left|1 - \frac{x_{ij}}{x_{maxj}}\right|^n + \sum_{j=k+1}^{n} \omega_j \cdot \left|1 - \frac{x_{minj}}{x_{ij}}\right|^n} \tag{1.41}$$

Функція корисності отримана з припущення, що для критеріального простору R^n показник простору $r = n$.

Вплив макроекономічних факторів на формування схильності до шахрайства можна визначити за низкою параметрів, які характеризують макроекономічний стан країни. Модель схильності до шахрайства побудована на основі моделі оцінки рівня економічного, соціального та політичного розвитку Кузьменко О. В. [42-44]

Алгоритм моделі наступний:

1. формується база дослідження соціальних, економічних та політичних факторів окремої країни, які впливають на формування схильності до шахрайства в банківській сфері;

2. виявлення аномальних часових рядів з метою усунення аномальних значень;

3. відбираються фактори;

4. нормалізуються індикатори соціального, економічного та політичного стану країни;

5. будується модель схильності до шахрайства.

Будується трикутника, сторонами якого є економічні, соціальні і політичні показники країни (рис. 1.41).

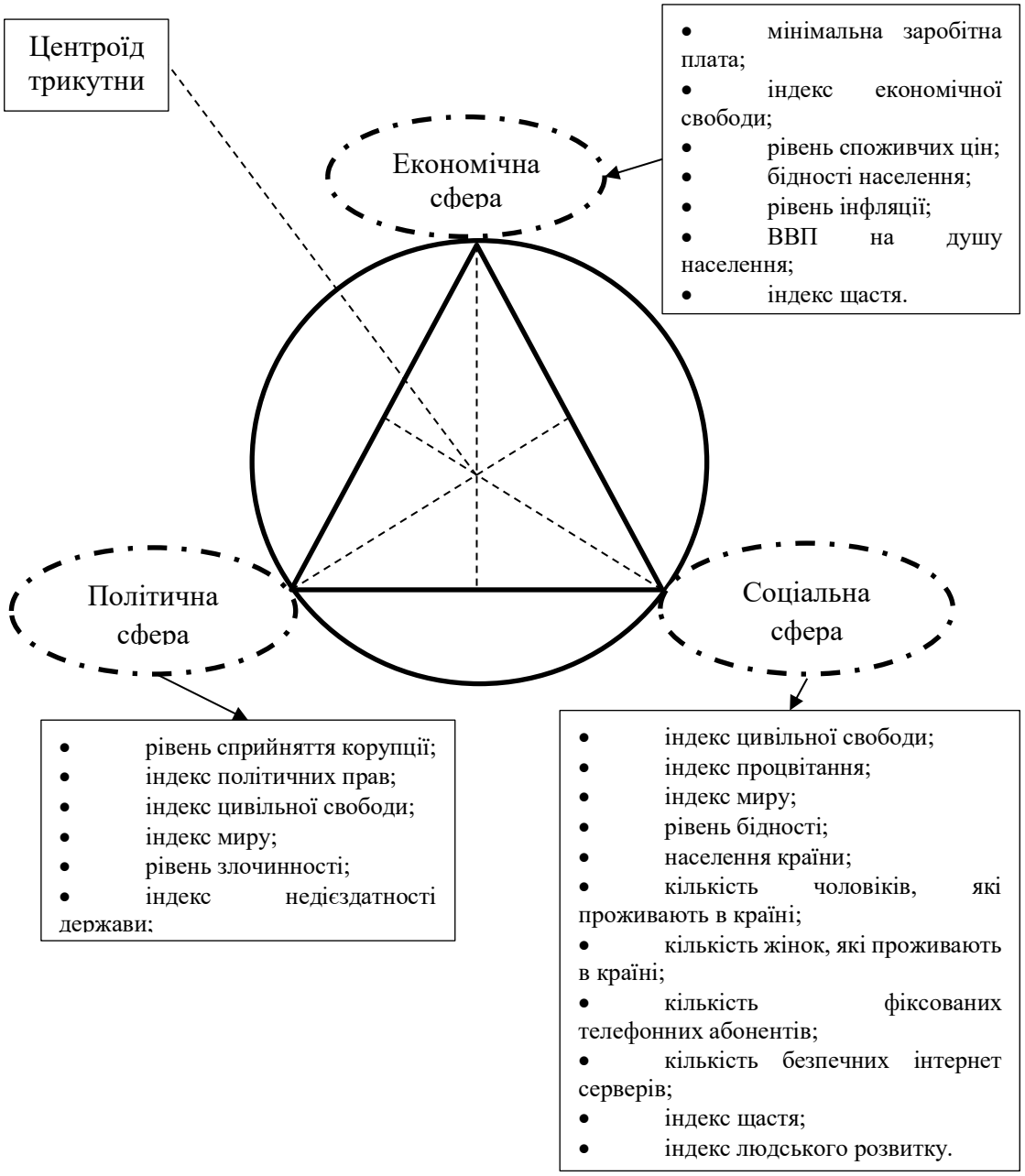


Рисунок 1.41 – Трикутник

Метою моделі є визначення центроїди трикутника, що показує на те, що не має схильності до шахрайства в країні, який можна описати за радіусом описаного кола.

$$R_t = \frac{n_{et} \cdot n_{st} \cdot}{\sqrt{\left(n_{et} + n_{st} + n_{pt}\right) \cdot \left(-n_{et} + n_{st} + n_{pt}\right) \cdot \left(n_{et} + n_{st} - n_{pt}\right) \cdot}} \quad (1.42)$$

$$\frac{\cdot\, n_{pt}}{\sqrt{\cdot \left(n_{et} - n_{st} + n_{pt}\right)}}$$

де R_t – радіус описаного кола навколо трикутника, в даний період часу;

n_{et}, n_{st}, n_{pt} – нормалізовані показники економічного, політичного та соціального стану країни.

Для того щоб визначити високу схильність до шахрайства в країни, необхідно визначити кути трикутника, які наведені в формулах 1.43-1.45:

$$\sin \alpha_{et} = \frac{n_{et}}{2 \cdot R_t}; \quad (1.43)$$

$$\sin \alpha_{st} = \frac{n_{st}}{2 \cdot R_t}; \quad (1.44)$$

$$\sin \alpha_{pt} = \frac{n_{pt}}{2 \cdot R_t}, \quad (1.45)$$

де R_t – радіус описаного кола навколо трикутника в даний момент часу;

n_{et}, n_{st}, n_{pt} – нормалізовані показники економічного, політичного та соціального стану країни.

$\alpha_{et}, \alpha_{st}, \alpha_{pt}$ – кути трикутника.

Якщо сума кутів трикутника дорівнює 180 градусів, то схильність до шахрайства відсутня. Якщо трикутник гострокутний, центроїда лежить в середині трикутника, то схильність до шахрайства є низькою. Коли трикутник

тупокутний, центроїда лежить поза трикутником, то схильність до шахрайства є високою [42-43].

Реалізацію моделі проведемо в програмному забезпечені STATISTICA. На рисунку 1.42 представлено результати регресійної моделі для економічного стану.

Regression Summary for Dependent Variable: Var2 (Spreadsheet1)
R= ,64316972 R?= ,41366728 Adjusted R?= ,33718910
F(3,23)=5,4090 p<,00577 Std.Error of estimate: 159,63

N=27	b*	Std.Err. of b*	b	Std.Err. of b	t(23)	p-value
Intercept			-32,7792	406,6830	-0,08060	0,936456
X1	-1,14328	0,731329	-1,7587	1,1250	-1,56329	0,013164
X3	0,33419	0,198695	13,8946	8,2612	1,68191	0,010612
X12	0,42679	0,693717	0,0750	0,1220	0,61522	0,044445

Рисунок 1.42 – Результати регресійної моделі для економічного стану

До політичних: рівень злочинності, індекс політичних прав, показник сприйняття корупції, індекс громадської свободи, індекс миру.

Результати проведення регресійного аналізу наведені на рисунку 1.43.

Regression Summary for Dependent Variable: Var2 (Spreadsheet1)
R= ,65042858 R?= ,42305733 Adjusted R?= ,28569003
F(5,21)=3,0798 p<,03070 Std.Error of estimate: 165,71

N=27	b*	Std.Err. of b*	b	Std.Err. of b	t(21)	p-value
Intercept			-974,156	1134,253	-0,85885	0,400119
X20	0,491920	0,207956	41,900	17,713	2,36550	0,027705
X18	-0,742159	0,257014	-2,147	0,744	-2,88762	0,008808
X4	0,569129	0,247494	148,576	64,611	2,29957	0,031831
X2	-0,598645	0,260075	-495,963	215,466	-2,30182	0,031682

Рисунок 1.43 – Результати регресійної моделі для політичного стану

До соціального стану відносяться: індекс щастя, кількість чоловіків проживаючих в країні, кількість жінок проживаючих в країні, бідність, глобальний індекс мира, індекс процвітання, індекс громадської свободи, кількість фіксованих телефонних абонентів, кількість безпечних інтернет серверів.

Результати регресійної моделі для соціального стану наведені на рисунку 1.44.

Regression Summary for Dependent Variable: Var2 (Spreadsheet1)
R= ,87894621 R?= ,77254644 Adjusted R?= ,65212984
F(9,17)=6,4156 p<,00053 Std.Error of estimate: 115,64

N=27	b*	Std.Err. of b*	b	Std.Err. of b	t(17)	p-value
Intercept			44284,6	12421,41	3,56519	0,002382
X4	-0,58430	0,253133	-152,5	66,08	-2,30826	0,033824
X5	-0,71391	0,297518	-24,0	10,00	-2,39956	0,028152
X7	0,63482	0,279128	189,6	83,37	2,27428	0,036195
X10	-3,68972	1,282741	-0,0	0,00	-2,87644	0,010472
X17	0,72491	0,302118	20,6	8,59	2,39944	0,028159
X19	-4,14769	1,135206	-38546,9	10550,13	-3,65369	0,001966

Рисунок 1.44 – Результати регресійної моделі для соціального стану

В результаті проведення первинного аналізу були отримані найбільш вагомі змінні:

— економічні

$$F_{\text{e}} = b_{i1} \cdot X_1 + b_{i2} \cdot X_3 + b_{i3} \cdot X_{12}, \qquad (1.46)$$

де X_1 – стандартизована змінна, яка показує мінімальну заробітну плату населення країни;

X_3 – стандартизована змінна, яка показує індекс економічної свободи;

X_{12} – стандартизована змінна, яка показує ВВП на душу населення;

— соціальні

$$F_i = b_{i1} \cdot X_4 + b_{i2} \cdot X_5 + b_{i2} \cdot X_7 + b_{i2} \cdot X_{10} + b_{i2} \cdot X_{17} + \quad (1.47)$$
$$+ b_{i2} \cdot X_{19},$$

де X_4 – стандартизована змінна, яка показує індекс цивільної свободи;

X_5 – стандартизована змінна, яка показує індекс процвітання;

X_7 – стандартизована змінна, яка показує індекс миру;

X_{10} – стандартизована змінна, яка показує населення країни;

X_{17} – стандартизована змінна, яка показує індекс щастя;

X_{19} – стандартизована змінна, яка показує індекс людського розвитку.

— політичні

$$F_i = b_{i1} \cdot X_2 + b_{i2} \cdot X_4 + b_{i3} \cdot X_{18} + b_{i4} \cdot X_{20} \quad (1.48)$$

де X_2 – рівень сприйняття корупції;

X_4 – індекс цивільної свободи;

X_{18} – рівень злочинності;

X_{20} –індекс недієздатності держави;

Визначивши вхідні показники моделі, винесемо їх до табличного редактора Microsoft Office Excel, на наступному кроці визначимо до якої групи належать показники: стимулятори, дестимулятори чи номінатори. З огляду на показники, які розглядаються в даному дослідженні їх було поділено на стимулятори та дестимулятори (рис. 1.45).

С	С	С	Д	С	Д	Д	С	С	Д	С	С	С	С
Мінімальна заробітня плата	Індекс економічної свободи	ВВП на душу населення	Рівень злочинності	Індекс людської свободи	Рівень сприйняття крупції	Індекс мира	Індекс недієздатності держави	Індекс щастя	Індекс працевлаштування	Індекс людського розвитку	Населення	Фіксовані телефонні абоненти	Кількість інтернет серверів
0,0175029	0,661328	0,369676	0,9623	0,75	0,77217	1	0,9229692	0,5157	0,9948	0,915107	0,9966	0,557348	0,0069
0,0198366	0,7182939	0,351853	0,8121	0,75	0,84411	0,93	0,9216783	0,6377	0,982	0,918115	0,9994	0,575091	0,0069
0,0256709	0,7665287	0,312215	0,7235	1	0,89814	0,8692	0,9203911	0,7422	0,9695	0,921123	1	0,593495	0,0069
0,0326721	0,8066452	0,25116	0,682	1	0,92956	0,8158	0,9191074	0,8289	0,9573	0,924131	0,9951	0,612133	0,0069
0,042007	0,7150538	0,232267	0,6079	1	0,93781	0,7686	0,9178273	0,8981	0,9454	0,927139	0,9872	0,630726	0,0069
0,0735123	0,7275986	0,216568	0,6321	1	0,92628	0,7266	0,9165508	0,9497	0,9339	0,930147	0,9785	0,701305	0,0069
0,084014	0,7795699	0,24598	0,6623	1	0,90079	0,6889	0,9152778	0,9837	0,9226	0,933155	0,9696	0,71413	0,0069
0,0326721	0,7240143	0,207275	0,6774	1	0,86768	0,6549	0,9140083	1	0,9115	0,936163	0,961	0,736002	0,007
0,0373396	0,7831541	0,15777	0,6984	1	0,83248	0,6242	0,9127424	0,9987	0,9008	0,939171	0,952	0,764521	0,0068
0,0490082	0,8566308	0,157755	0,6872	1	0,79945	0,5962	0,9114799	0,9798	0,8903	0,942179	0,9424	0,790552	0,0071
0,0665111	0,8691756	0,193745	0,7583	1	0,77163	0,5706	0,910221	0,9433	0,88	0,945187	0,933	0,809722	0,0065
0,0793466	0,8637993	0,218247	0,8475	1	0,75129	0,5471	0,9089655	0,8892	0,87	0,948195	0,9238	0,822145	0,0077
0,0980163	0,9157706	0,260198	0,689	1	0,74037	0,5254	0,9077135	0,8175	0,8601	0,951203	0,9163	0,843106	0,0053
0,1295216	0,9623656	0,339317	0,7393	0,75	0,74107	0,5055	0,9064649	0,7282	0,8506	0,954211	0,9094	0,92146	0,0101
0,1831972	1	0,453808	0,7934	0,5	0,75656	0,4869	0,9052198	0,6212	0,8412	0,957219	0,9028	0,885385	0,0118
0,2415403	0,9749104	0,571509	0,9108	0,5	0,78571	0,4697	0,9039781	0,5613	0,832	0,966578	0,8967	0,940825	0,0166
0,3127188	0,9229391	0,761495	0,9559	0,5	0,81481	0,4537	0,9229692	0,3264	1	0,975936	0,8913	0,979433	0,0252
0,3990665	0,9139785	0,965586	1	0,5	0,88	0,9068	0,930791	0,9603	1	0,981283	0,8865	1	0,0377
0,285881	0,874552	0,631677	0,8878	0,5	1	0,8453	0,9454806	0,9628	0,9135	0,973262	0,8826	0,988572	0,0526
0,3302217	0,8315412	0,735819	0,7721	0,75	0,91667	0,8469	0,9482014	0,9401	0,9223	0,981283	0,8791	0,982126	0,1157
0,386231	0,8207885	0,885858	0,7501	0,75	0,95652	0,8914	0,9550725	0,9219	0,95	0,987968	0,8759	0,962359	0,1544
0,4422404	0,8261649	0,956748	0,8727	0,75	0,84615	0,8798	0,9806548	0,9497	0,9794	0,994652	0,8738	0,924509	0,2042
0,4784131	0,8297491	1	0,6923	0,75	0,88	0,8181	1	0,9381	0,9794	0,997326	0,8718	0,897859	0,2297
0,3383897	0,8835125	0,770441	0,7375	0,75	0,84615	0,7191	0,9806548	0,9502	0,9314	1	0,8676	0,793897	0,3933
0,2333722	0,8405018	0,527249	0,6904	0,75	0,81481	0,6436	0,8636959	0,9411	0,8879	0,993316	0,8654	0,691595	0,564
0,2240373	0,874552	0,542403	0,6585	0,75	0,75862	0,557	0,8728477	0,9338	0,8879	0,993316	0,8625	0,641368	0,777
0,2952159	0,8620072	0,65509	0,7448	0,75	0,75862	0,5881	0,8905405	0,9628	0,8482	0,993316	0,8592	0,31343	1

Рисунок 1.45 – Відносна нормалізація показників

Як видно з рисунку 1.45 завдання нормалізації виконано, усі показники приведені до єдиної основи, після цього можна перейти до наступного кроку. Далі визначимо ступень переваги кожної альтернативи за допомогою метрики Мінковського (рис. 1.46).

Метрика Мінковського		
Економічна	Політична	Соціальна
0,0535802	0,68150172	0,73647462
0,0552463	0,81287614	0,88182469
0,0698245	0,7957357	0,84559122
0,0955816	0,85706261	0,88897206
0,1221872	0,8969307	0,88900184
0,1665603	0,91191599	0,86281978
0,1631256	0,90377516	0,83193537
0,1190126	0,8833921	0,80423817
0,1391655	0,85959981	0,78157075
0,1489172	0,83586505	0,76281681
0,1555458	0,81233079	0,74463736
0,1621333	0,78713557	0,72281972
0,166821	0,75724269	0,69132603
0,1756622	0,81994286	0,70836821
0,2028575	0,72283791	0,89010549
0,2390048	0,75467115	0,78361699
0,2832209	0,75481729	0,52684652
0,3597781	0,5826089	0,55852346
0,2789759	0,5717486	0,55729164
0,3118076	0,80163749	0,72245655
0,3562654	0,79673929	0,71500233
0,4128268	0,82255058	0,713902
0,45105	0,80945869	0,73035537
0,3119445	0,822491	0,76480454
0,2463158	0,87337931	0,80956853
0,2294402	0,9441095	0,96289712
0,2853289	0,91839714	0,8356133

Рисунок 1.46 – Метрика Мінковського

На наступному етапі будуємо модель стабільності соціальних, економічних та політичних факторів окремої країни, які впливають на формування схильності до шахрайства в банківській сфері (рис. 1.47).

радиус	синус е	синус п	синус с
1,54355	0,01736	0,22076	0,23857
0,56676	0,04874	0,71712	0,77795
0,58607	0,05957	0,67888	0,72141
0,46362	0,10308	0,92432	0,95874
0,44847	0,13623	0,99999	0,99115
0,46602	0,17871	0,97842	0,92574
0,48464	0,1683	0,93242	0,85831
0,56515	0,10529	0,78156	0,71153
0,49618	0,14024	0,86623	0,7876
0,45968	0,16198	0,90918	0,82972
0,43368	0,17933	0,93655	0,8585
0,41287	0,19635	0,95325	0,87536
0,39604	0,21061	0,95601	0,8728
0,49532	0,17732	0,82768	0,71505
0,71069	0,14272	0,50855	0,62623
0,39205	0,30482	0,96247	0,99939
0,53615	0,26412	0,70392	0,49132
0,30116	0,59733	0,96729	0,9273
0,29164	0,47829	0,98024	0,95546
0,40136	0,38844	0,99864	0,9
0,39838	0,44714	0,99998	0,89739
0,41128	0,50188	0,99998	0,8679
0,40787	0,55293	0,99229	0,89532
0,41128	0,37924	0,99993	0,9298
0,43972	0,28008	0,99312	0,92056
0,48181	0,2381	0,97975	0,99925
0,46336	0,30789	0,99101	0,90168

Рисунок 1.47 – Модель схильності до шахрайства на формування якої впливають соціальні, економічні та політичні фактори окремої країни

Зобразимо графічно динаміку значень радіуса кола описаного навколо трикутника для: України, США, Великобританії, Канади та Росії (рис. 1.48)

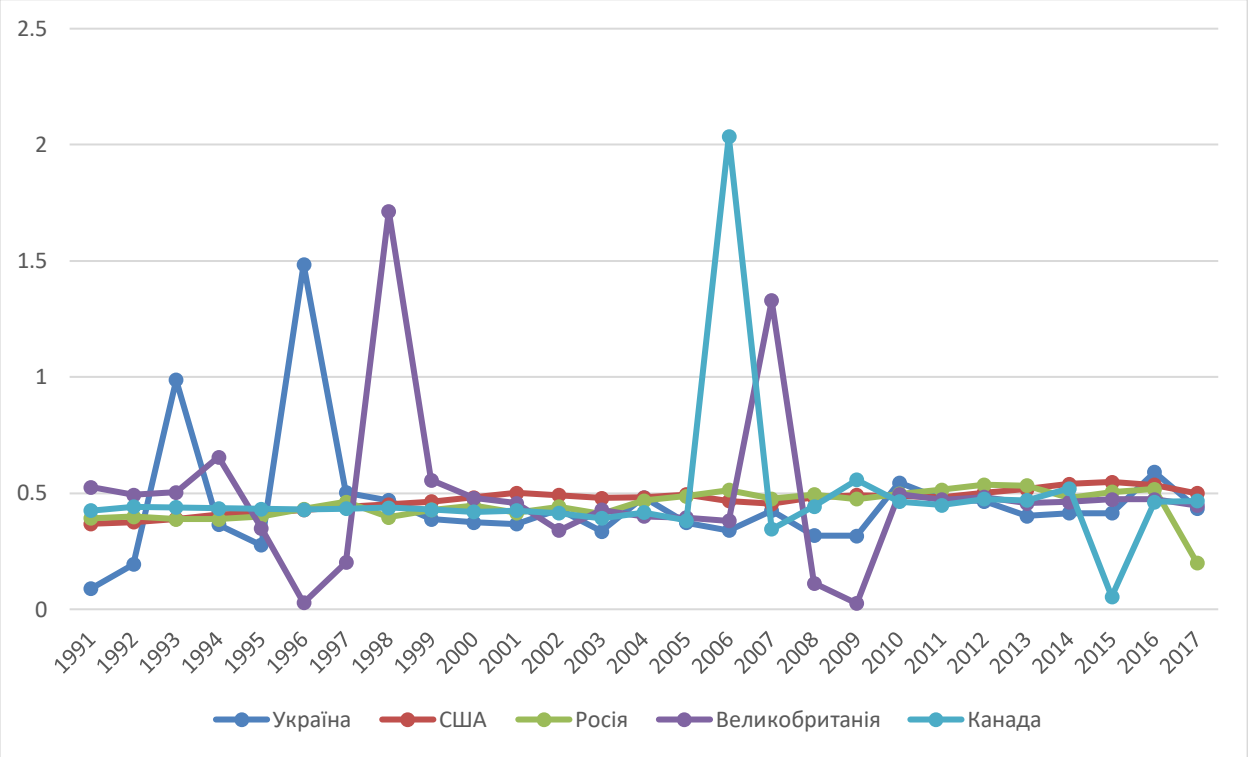


Рисунок 1.48 – Діаграма динаміки значень радіуса кола описаного навколо трикутника політичної та економічної ситуації України, США, Великобританії, Канади та Росії

На основі даних, які наведених на рисунку 1.48, можна зазначити, що схильність до формування шахрайства в країн буде залежить від значення радіуса кола, описаного навколо трикутника. При зростанні значень радіусу зростає відстань від центра до кожної вершини трикутника, тому ситуація в країні буде характеризуватися збільшенням шахрайства. Якщо центроїд знаходиться ближче до вершин трикутника економічних, політичних та соціальних складових, тим менше схильність до шахрайства в країні. Проаналізуючи криву значень радіуса країн (рис. 1.48), можна зробити висновок, найменший показник схильності до шахрайства є у США, потім Канада та Росія. А найбільш схильним до шахрайства є Великобританія та Україна.

Досліджується сума кутів трикутника рисунок 1.49.

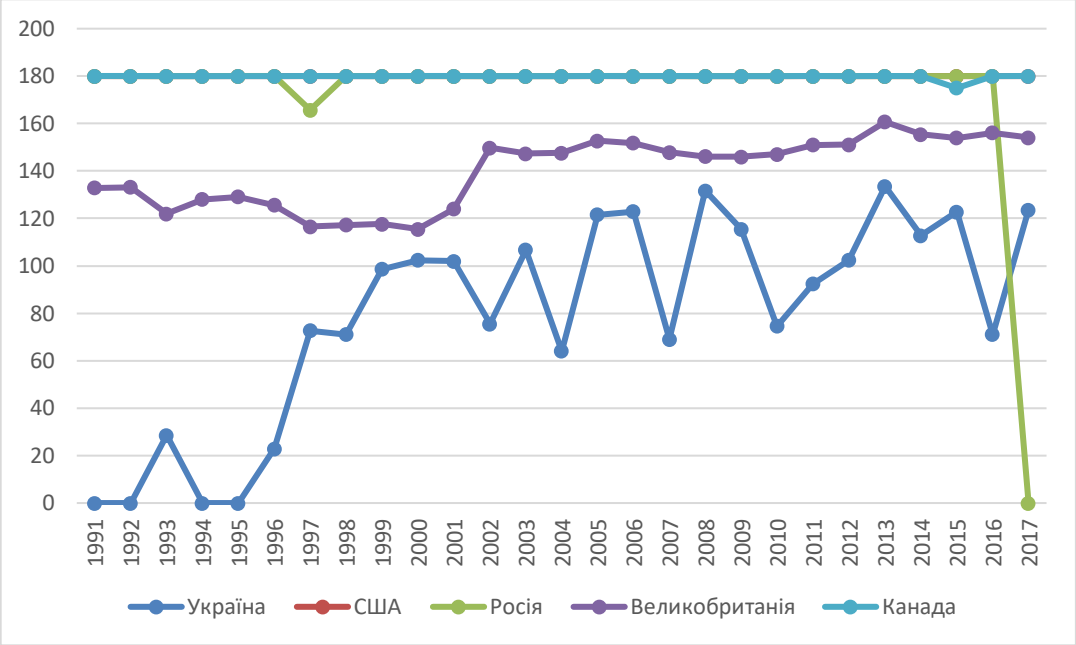


Рисунок 1.49 – Діаграма динаміки схильності до шахрайства в України, США, Великобританії, Канади та Росії

Таким чином, дослідження показників Росії, США та Канади протягом 26-ти років демонструють, що в країні не висока схильність до шахрайства, а в Великобританії та України висока схильність до шахрайства.

Карта світу із зазначеним схильності до шахрайства по країнам графічно наведено на рисунку 1.50. Як бачимо з рисунку Росія, Канада та США мають низьку схильність до шахрайства, а Україна та Великобританія мають високу схильність до шахрайства.

Пункт 1.4.1 даного звіту було виконано із використанням матеріалів проміжного звіту про НДР [11], публікацій виконавців [18, 45, 46], магістерської дипломної роботи [47].

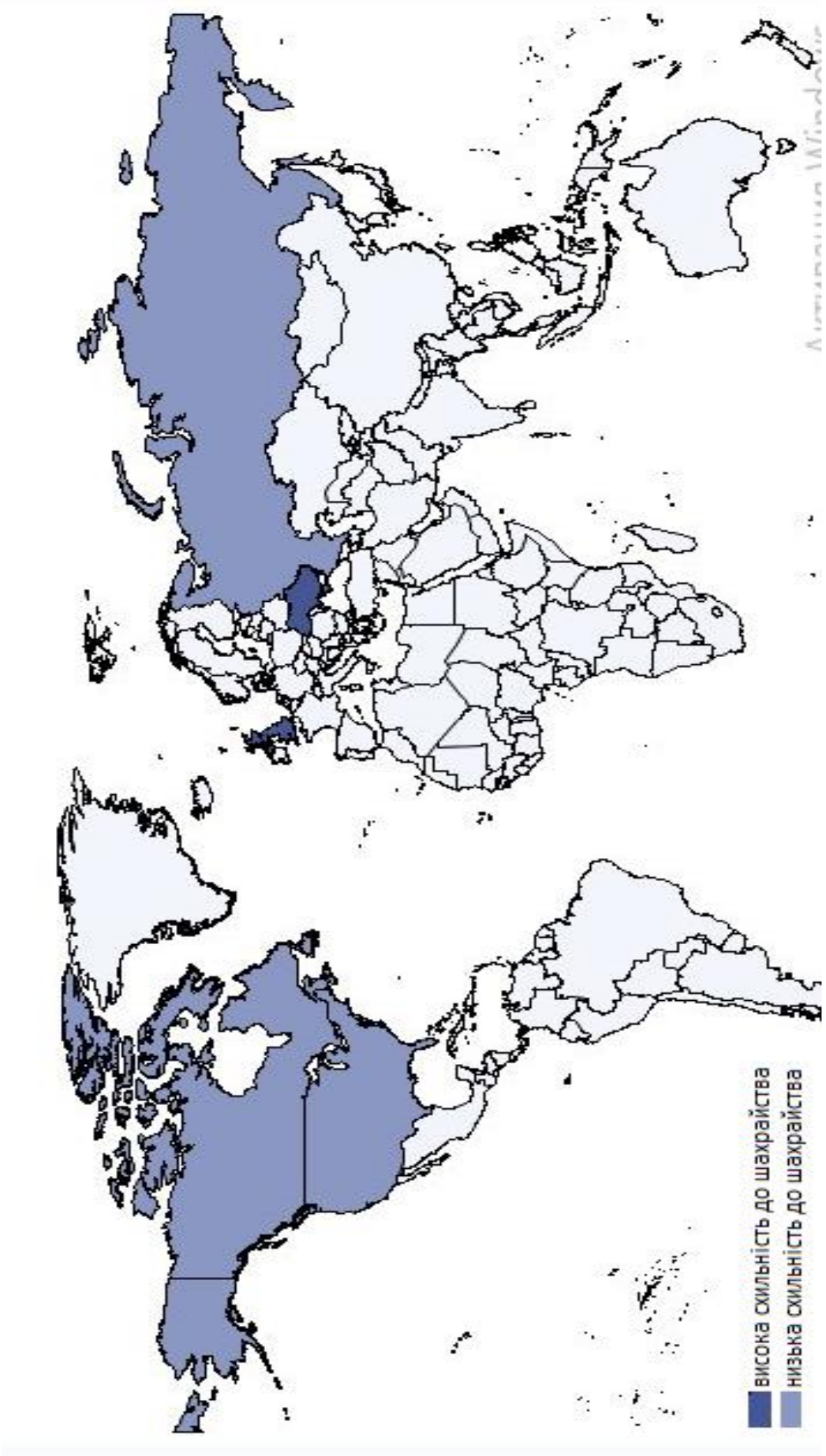


Рисунок 1.50 – Рівень впливу шахрайства по країнам

1.4.2 Розробка гравітаційної моделі оцінки привабливості країни для легалізації кримінальних доходів та фінансування тероризму

Для проведення дослідження було сформовано набір даних по 215 країнам світу за 2017 рік. Набір даних представляє собою статистичну інформацію, яку було отримано з офіційних сайтів світових організацій. Так, авторами було узято 8 показників: з офіційного сайту Світового банку – Gross Domestic Product per capita (GDP), Claims on the central government (CCG), Internally displaced persons, new displacement associated with conflict and violence (number of cases) (IDP); по даним The Organisation for Economic Co-operation and Development - Automatic Exchange of Information (AEOI); з сайту організації Transparency International – Corruption Perceptions Index (CPI); з матеріалів досліджень Institute for economics & peace – Global Terrorism Index (GTI); із звітності, представленої на сайті The Legatum Institute – Legatum Prosperity Index (LPI); з розрахунків Happy Planet Index – Happy Planet Index (HPI).

Вибір перелічених показників обґрунтовано, виходячи із гіпотез, які було висунуто авторами дослідження, тобто:

1) GDP per capita країни показує рівень її економічного добробуту, платоспроможності населення. Збільшення значення даного показника говорить про збільшення обсягів виробництва товарів та послуг, формування умов в країні, сприятливих для інших країн, які намагаються легалізувати кошти, отримані незаконним шляхом, що сприяє зниженню рівня ризику. Даний показник виступає в якості фактора-дестимулятора;

2) Automatic Exchange of Information характеризує процес обміну фінансовою інформацією між банками та податковими органами. Якщо країни не залучені до даної системи, відповідно для країн, які намагаються легалізувати кошти, знижується ризик легалізації. В протилежному випадку, приєднання країни до цієї системи підвищує рівень безпеки інформації, її надійності. Для країн, що легалізують кошти, ризик легалізації відповідно підвищується,

оскільки для них фоормується несприятливе середовище. Даний фактор виступає стимулятором в моделі;

3) Claims on the central government свідчить про рівень довіри до центрального уряду в частині його фінансових зобов'язань. Країни з високим рівнем довіри формують сприятливі умови для легалізації кримінальних доходів, відповідно для країн, що легалізують, даний фактор ймовірно свідчиме про зниження ризику легалізації. В моделі показник є дестимулятором;

4) Internally displaced persons, new displacement associated with conflict and violence – фактор-стимулятор, який свідчить про нестабільність в країні, підвищений рівень небезпеки для розміщення фінансових ресурсів. З позиції осіб, які легалізують кримінальні доходи, воєнні конфлікти, випадки насилля, які призводять до переміщення осіб, створюють умови, несприятливі для легалізації. Тобто підвищення рівня даного показника буде говорити про підвищений рівень для легалізації коштів іншою країною;

5) Corruption Perceptions Index є фактором-дестимулятором в моделі, оскільки відображає ефективність роботи правоохоронних органів щодо виявлення фактів корупції. В країнах із високим значенням даного показника створюються умови, сприятливі для розміщення фінансових потоків. Вони є привабливими для країн, що легалізують кошти, оскільки ризики легалізації для них зменшуються;

6) Global Terrorism Index показує рівень терористичної активності в країнах світу. Вибір даного показника обумовлюється збільшення випадків терористичних актів, що впливає на безпеку країну в цілому. Країни, що легалізують кошти, не приваблюють країни з високим рівнем тероризму, оскільки існує підвищений ризик втрати грошових ресурсів. Даний показник виступає фактором-стимулятором;

7) Happy Planet Index характеризує рівень добробуту населення країни з позиції не його фінансового стану, а з позиції задоволеністю життям, рівня екологічної безпеки, стану медицини і т.п. Країни, в яких проживає щасливе населення, на думку авторів дослідження, є найбільш привабливими для країн,

що легалізують кошти, оскільки визивають більше довіри за рахунок стабільності життя. Фактор виступає дестимулятором, оскільки ризик легалізації із збільшенням значення показника знижується;

8) Legatum Prosperity Index – показник добробуту країни, який відображає різні параметри: економіку, управління, освіту, здоров'я, безпеку, екологію тощо. Для дослідження ми беремо різницю між добробутом країни, яка легалізує кошти, та країни, в якій кошти будуть відмиватися. Чим більше різниця між добробутом країн, тим кращі умови для легалізації. Показник є дестимулятором, але оскільки в моделі він використовується у знаменнику, то його треба враховувати, як стимулятор.

Після формування набору даних, його було проаналізовано на предмет відсутності значень показників для певних країн. Тому дані було очищено від таких спостережень. В результаті для моделювання було обрано дані 105 країн.

Далі було проведено аналіз даних на мультиколінеарність. Результати парних коефіцієнтів кореляції представлені в таблиці 1.16:

Таблиця 1.16 – Міжфакторна кореляція для показників оцінки ризику легалізації

	GDP	AEOI	CCG	IDP	CPI	GTI	HPI	LPI
GDP	1							
AEOI	0,1117	1						
CCG	-0,1205	0,2822	1					
IDP	0,0331	-0,2546	-0,1138	1				
CPI	-0,0885	0,6125	0,1225	-0,2408	1			
GTI	0,0821	-0,1059	0,0103	0,4787	-0,2662	1		
HPI	-0,0112	0,5845	0,1587	-0,2125	0,7181	-0,2123	1	
LPI	-0,0069	0,6576	0,1549	-0,3379	0,8973	-0,3665	0,8372	1

Результати міжфакторної кореляції свідчать про існування між окремими факторами залежності, що для моделювання не є прийнятним. Але цю залежність можна пояснити наступним чином:

1) такий показник, як Automatic Exchange of Information, корелює із Corruption Perceptions Index, Happy Planet Index та Legatum Prosperity Index. Наявність зв’язку обумовлена або випадковістю, або тим, що країни з високим рівнем життя є обов’язковими учасниками даної системи;

2) зв'язок між Happy Planet Index та Legatum Prosperity Index обумовлений тим, що дані показники характеризують схожі за змістом аспекти – щастя та добробут. Оскільки рівень добробуту буде у знаменнику моделі, то буде враховуватися не його лінійний зв'язок, а нелінійний, тому залишимо його у моделі;

3) зв'язок між Corruption Perceptions Index, Happy Planet Index та Legatum Prosperity Index є значним, що обумовлено також тим, що у країн із високими показниками щастя та добробуту є можливості та інструменти протидії з корупцією.

Оскільки для запропонованої методики не будується регресійна модель та не оцінюються параметри, для яких це призводить до нестійкості, то наявність міжфакторної кореляції не впливатиме на загальний результат.

Для оцінки економічної безпеки країн світу стосовно ризику легалізації кримінальних доходів та фінансування тероризму пропонуємо методику, в основі якої знаходиться гравітаційне моделювання. Це дозволить визначити можливості легалізації фінансових ресурсів однією країною в іншій та визначити рівень безпеки.

На першому етапі необхідно провести нормалізацію даних. Це пов’язано з тим, що показники, які ми використовуємо для побудови моделі, мають різну розмірність. Тому їх треба привести до вигляду від 0 до 1. Також треба врахувати той факт, що дані показники впливають по різному на ризик легалізації кримінальних доходів. Тобто, збільшення значення показника призводить до покращення ситуації, тобто зменшення значення ризику, і навпаки. Відповідно,

ми маємо справу із стимулятором. Якщо зміни значення показника призводять до погіршення обставин, тобто із збільшенням показника ризик збільшується, і навпаки, то мова йде про дестимулятор. Для нормалізації використаємо абсолютну нормалізацію, що дозволить нам здійснити її як для стимуляторів, так й дестимуляторів (формула 1.49):

$$x_{ij}^{+} = \frac{x_{ij}}{x_{max_j}}, x_{ij}^{-} = \frac{x_{min_j}}{x_{ij}}, \tag{1.49}$$

де x_{ij}^{+}, x_{ij}^{-} – нормалізоване значення *j*-го показника характеристики рівня ризику легалізації кримінальних доходів та фінансування тероризму, як для стимуляторів (+), так й для дестимуляторів (-), для *i-оїї* розглянутої країни;

x_{ij} – початкове (емпірічне) значення *j*-го показника характеристики рівня ризику легалізації для *i-оїї* країни;

x_{min_j} – мінімальна величина *j*-го показника характеристики визначення рівня ризику легалізації для всіх країн дослідження;

x_{max_j} – максимальна величина *j*-го показника характеристики визначення рівня ризику легалізації для всіх країн дослідження.

Значення показника “Claims on central government”, який використовується для моделювання, є як від’ємними, так й додатними. Відповідно, застосування абсолютної нормалізації до даного показника не дозволить нам отримати його значення від 0 до 1. Оскільки показник виступає дестимулятором, то для нього застосовуємо нормалізацію Севіджа, що дозволить уникнути даної проблеми, за наступною формулою 1.50:

$$x_{ij}^{-} = \frac{x_{max_j} - x_{ij}}{x_{max_j} - x_{min_{ij}}}. \tag{1.50}$$

На другому етапі методики розрахунку визначаємо вагові коефіцієнти для обраних показників. З цією метою проводиться експертне опитування фахівців, які є компетентними з питань банківських ризиків, економічної безпеки, науковців, які працюють над проблемами легалізації коштів. Для роботи з експертами використовується метод аналіз ієрархії в частині отримання вагових коефіцієнтів.

Експертам пропонується заповнити матрицю, представлену у вигляді таблиці 1.17:

Таблиця 1.17 – Матриця попарного порівняння факторів, що заповнюється експертами

	GDP	AEOI	CCG	IDP	CPI	GTI	HPI
GDP	1	a_{12}	a_{13}	a_{14}	a_{15}	a_{16}	a_{17}
AEOI	$1/a_{12}$	1	a_{23}	a_{24}	a_{25}	a_{26}	a_{27}
CCG	$1/a_{13}$	$1/a_{23}$	1	a_{34}	a_{35}	a_{36}	a_{37}
IDP	$1/a_{14}$	$1/a_{24}$	$1/a_{34}$	1	a_{45}	a_{46}	a_{47}
CPI	$1/a_{15}$	$1/a_{25}$	$1/a_{35}$	$1/a_{45}$	1	a_{56}	a_{57}
GTI	$1/a_{16}$	$1/a_{26}$	$1/a_{36}$	$1/a_{46}$	$1/a_{56}$	1	a_{67}
HPI	$1/a_{17}$	$1/a_{27}$	$1/a_{37}$	$1/a_{47}$	$1/a_{57}$	$1/a_{67}$	1

Матриця заповнюється шляхом попарного порівняння критеріїв за важливістю по шкалі, представленій у таблиці 1.18:

В процесі заповнення матриці, якщо елемент і важливіше елементу j, то на перетині рядку і та стовпчика j в клітинку (i; j) ставиться ціле число, якщо навпаки, то ставиться обернене число, тобто дріб. В клітинку (j; i) на перетині рядка j та стовпчика і ставиться обернене до цілого числа, або ціле, що є оберненим до дробу.

Таблиця 1.18 – Шкала, за якою заповнюється матриця попарного порівняння

Відносна оцінка важливості критерія	Якісна оцінка	Пояснення
1	Однаково важливий	Обидва елементи вносять однаковий вклад у досягнення кінцевої цілі
3	Не набагато важливий	Існують вербальні висловлювання відносно пріоритету одного елемента щодо іншого, але ці висловлювання досить непереконливі
5	Суттєво важливіший	Існують достатньо переконливі доведення та логічні критерії, що один з елементів є більш важливим (вагомішим)
7	Значно важливіший	Існує переконливе доведення великої значущості одного елемента в порівнянні з іншим
9	Абсолютно важливіший	Усвідомлення пріоритету одного елемента щодо іншого максимально підтверджується
2; 4; 6; 8	Проміжні оцінки між двома сусідніми судженнями	Потрібен певний компроміс
$\frac{1}{\nu}; \nu = 1, ..., 9$	Обернені значення ненульових оцінок	Протилежні оцінки та судження щодо пріоритету одного елементу у відношенні до іншого
0	Непорівняльність	Немає сенсу в порівнюванні елементів

Після цього в кожній матриці, в якій експерт поставив свої оцінки, для кожного фактору у рядку матриці знаходимо ваговий коефіцієнт за формулою 1.51:

$$\omega_i^k = \frac{\sqrt[n]{\prod_{j=1}^{n} a_{ij}^k}}{\sum_{i=1}^{n} \sqrt[n]{\prod_{j=1}^{n} a_{ij}^k}}, \quad (1.51)$$

де ω_i^k – ваговий коефіцієнт для кожного фактору і, що оцінюється k-им експертом;

a_{ij}^k– оцінка, яку ставить k-ий експерт і-ому фактору;

n – кількість факторів, які підлягають оцінці.

Перед визначенням узагальненої оцінки для вагового коефіцієнту необхідно перевірити узгодженість експертів за допомогою коефіцієнта конкордації та парної рангової кореляції за формулами:

$$K_{кон} = \frac{\sum_{j=1}^{n} d_j^2}{\frac{1}{12}\left[m^2(n^3 - n) - m\sum_{i=1}^{m} T_i \right]}; \quad (1.52)$$

де

$$d_j = S_j - \frac{\sum_{j=1}^{n} S_j}{n}; \quad (1.53)$$

$$S_j = \sum_{i=1}^{m} R_{ij}; \quad (1.54)$$

m – кількість експертів, які прийняли участь в дослідженні;

n – кількість факторів дослідження;

R_{ij} – ранг оцінки і-им експертом j-ого фактору;

$$T_i = \sum_{l=1}^{L} (t_l^3 - t_l); \quad (1.55)$$

L – кількість груп зв’язаних (однакових) рангів;

t_l – кількість зв’язаних рангів в кожній групі.

Коефіцієнт парної рангової кореляції між оцінками 2-ох експертів:

$$P_{\alpha\beta} = 1 - \frac{\sum_{j=1}^{n} \psi_j^2}{\frac{1}{6} \times (n^3 - n) - \frac{1}{12}(T_\alpha + T_\beta)}; \quad (1.56)$$

де ψ_j – різниця по модулю величин рангів оцінок j-ого фактору, поставлених експертами α і β;

$$\psi_j = \left| R_{\alpha j} - R_{\beta j} \right|; \tag{1.57}$$

T_α, T_β – показники зв’язаних рангів оцінок експертів α і β, що визначаються аналогічно, як і для коефіцієнта конкордації.

Для перевірки статистичної значущості коефіцієнта конкордації застосовується критерій Пірсона, який розраховується за формулою:

$$\chi_p^2 = \frac{\sum_{j=1}^{n} d^2}{\frac{1}{12}\left[mn \times (n+1) - \frac{1}{n-1}\sum_{i=1}^{m} T_i \right]}. \tag{1.58}$$

Якщо коефіцієнт конкордації буде наближатися до 1, критерій Пірсона покаже його статистичну значущість, значення коефіцієнта парної рангової кореляції покажуть сильний зв'язок між результатами експертного опитування, тобто значення буде від 0,7 до 1, - тільки за цих умов ми можемо зробити про узгодженість між експертами. Якщо думки експертів не узгоджені, то необхідно обрати тих експертів, думки яких слабко корелюють з іншими, та результати їх опитування виключити з розгляду.

Після визначення узгодженості експертів визначається середньоарифметичне значення вагових коефіцієнтів, як:

$$\omega_j = \frac{\sum_{i=1}^{m} \omega_i}{m}. \tag{1.59}$$

Сума отриманих значень вагових коефіцієнтів повинна дорівнювати 1.

Після знаходження вагових коефіцієнтів на третьому етапі визначається інтегральний показник кількісної оцінки рейтингу певної країни щодо характеристики визначення рівня ризику легалізації кримінальних доходів та фінансування тероризму за допомогою метрики Мінковського, який дозволяє

враховувати вплив факторів на основі їх позицій, як стимуляторів, так і дестимуляторів (формула 1.60):

$$IRA_i = 1 - \sqrt{\sum_{j=1}^{k} \omega_j \left|1 - x_{ij}^{+}\right|^2 + \sum_{j=k+1}^{n} \omega_j \left|1 - x_{ij}^{-}\right|^2}; \quad (1.60)$$

де IRA_i – інтегральна рейтингова оцінка характеристики рівня ризику легалізації для *i-oї* країни;

ω_j – вагові коефіцієнти для *j*-го показника.

З урахуванням того, що для оцінки ризику легалізації кримінальних доходів та фінансування тероризму було обрано 7 факторів, формула для визначення інтегрального показника матиме наступний вигляд (формула 1.61):

$$IRA(x_i) = 1 - \sqrt{\omega_1(1-x_1^-)^2 + \omega_3(1-x_3^-)^2 + \omega_5(1-x_5^-)^2 + \omega_7(1-x_7^-)^2 + \omega_2(1-x_2^+)^2 + \omega_4(1-x_4^+)^2 + \omega_6(1-x_6^+)^2} \quad (1.61)$$

де x_1^- - це нормалізоване значення GDP per capita, як фактора-дестимулятора;

x_2^+ - це нормалізоване значення Automatic Exchange of Information, як фактора-стимулятора;

x_3^- - це нормалізоване значення Claims on the central government per capita, як фактора-дестимулятора;

x_4^+ - це нормалізоване значення Internally displaced persons, new displacement associated with conflict and violence, як фактора-стимулятора;

x_5^- - це нормалізоване значення Corruption Perceptions Index per capita, як фактора-дестимулятора;

x_6^+ - це нормалізоване значення Global Terrorism Index per capita, як фактора-стимулятора;

x_7^- - це нормалізоване значення Happy Planet Index, як фактора-дестимулятора.

Отримане значення інтегрального показника буде варіюватися в межах від 0 до 1.

Наступним четвертим етапом буде побудова гравітаційної моделі ризику легалізації. З цією метою проведемо аналогію між законом гравітаційного тяжіння та гравітаційної сили в суспільних явищах. Тобто,

$$M_{ij} = k\frac{p_i p_j}{d_{ij}^2}, \tag{1.62}$$

де M_{ij} – показник взаємодії між об'єктами і та j;

k – коефіцієнт відповідності;

p – деяка значимість об'єкта;

d_{ij}^2 – відстань між об'єктами.

Дану аналогію було розглянуто у праці Walter Isard "Location Theory and Trade Theory: Short-Run Analysis" (1954) для міжнародної торгівлі у міжнародній економіці.

Ризик легалізації ідентифікується наступним чином: окрема країна «притягує» ризикові операції в інші країни з силою, що прямо пропорційна рейтинговій оцінці характеристики рівня ризику легалізації розглянутої країни, а також обернено пропорційна квадрату величини Prosperity Index у процесі здійснення ризикових операцій (формула 1.63):

$$SVA_k = \frac{IRA_k \cdot IRA_r}{d_{kr}^2}, \tag{1.63}$$

де SVA_k – кількісна оцінка величини (сили) взаємодії між певною розглянутою країною та k-ю країною в розрізі ризику легалізації;

IRA_k – інтегральна рейтингова оцінка характеристики рівня ризику легалізації *k*-ї країни, яка передає ризик у цесію;

IRA_r – інтегральна рейтингова оцінка характеристики рівня ризику легалізації *r*-ї країни, яка приймає ризик легалізації;

d_{kr} – величина, яка представляє собою нормалізовану різницю між добробутом *k*-ї та *r*-ї країни, яка визначається, як (формула 1.64):

$$d_{kr} = |LPI_k - LPI_r|,^+ \tag{1.64}$$

де PI_k – значення Legatum Prosperity Index для країни k;

PI_r – значення Legatum Prosperity Index для країни r.

Для знаходження різниці між добробутом країн використаємо природню нормалізацію, оскільки даний фактор є стимулятором для нашої моделі (формула 1.65):

$$x_{ij}^+ = \frac{x_{ij} - x_{min_j}}{x_{max_j} - x_{min_{ij}}}. \tag{1.65}$$

На основі розрахованих значень кількісної оцінки величини (сили) взаємодії між країнами в розрізі ризику легалізації будується матриця, яка дозволить оцінити взаємодію між різними країнами світу.

Але при побудові даної матриці необхідно значення знов нормалізувати, оскільки кількісна оцінка ризику повинна бути від 0 до 1. Для цього використовуємо нормалізацію Харрінгтона, яка дозволить нам врахувати розкид в отриманих значеннях, тобто:

$$SVA'_k = \exp(-\exp(-SVA_k)). \tag{1.66}$$

Отримане значення буде знаходитися в межах від 0 до 1 та свідчиме: якщо значення наближається до 0, то країна, яка легалізує кошти буде мати

підвищений рівень легалізації; якщо значення наближається до 1, то країна матиме низький рівень легалізації.

Розрахунки проводилися із використанням MS Excel. На першому етапі методики проведено нормалізацію факторів-стимуляторів та дестимуляторів. На другому етапі – отримано результати експертного опитування важливості факторів. Було залучено 7 експертів-фахівців з питань банківської справи, економічної безпеки, наукових дослідників, які займаються проблематикою відмивання коштів. Узгодженість думок експертів було оцінено за коефіцієнтом конкордації, який отримано рівним 0,8076. Його значення наближається до 1, що свідчить про високий рівень узгодженості між експертами. Статистичну значущість даного коефіцієнта підтверджує критерій Пірсона. Отримане значення критерію дорівнює 33,9184, що перевищує табличне значення, рівне 12,5916.

Узгодженість між думками експертів підтверджують розраховані значення коефіцієнту парної рангової кореляції, результати яких представлені в таблиці 1.19:

Таблиця 1.19 – Матриця парної рангової кореляції узгодженості думок між експертами

	1	2	3	4	5	6	7
1	-	0,6071	0,8571	0,7857	0,9643	0,9643	0,5714
2		-	0,7500	0,8929	0,6786	0,5714	0,6786
3			-	0,8571	0,8214	0,8929	0,8571
4				-	0,8571	0,7500	0,7857
5					-	0,9286	0,6071
6						-	0,6071
7						-	-

Значення парної рангової кореляції є позитивними та варіюються в межах від 0,5714 до 0,9643, що свідчить про середній та високий рівень узгодженості між експертами. За результатами оцінки узгодженості експертів, приймаємо отримані значення, як достовірні.

В результаті опитування розраховано усереднену оцінку факторів та отримано ваги, які використовуємо в моделі (таблиця 1.20).

Таблиця 1.20 – Вагові коефіцієнти для факторів моделі

Фактори	Ваги
GDP per capita (current LCU)	0,08664
Automatic Exchange of Information	0,29812
Claims on central government (annual growth as % of broad money)	0,08766
Internally displaced persons, new displacement associated with conflict and violence (number of cases)	0,10479
Corruption Perceptions Index	0,19534
Global Terrorism Index	0,19627
Happy Planet Index	0,03118
SUM	1,0000

За результатами отриманих вагів видно, що найбільшу вагу має фактор Automatic Exchange of Information, Corruption Perceptions Index and Global Terrorism Index. Тобто дані фактори чинять найбільший вплив на оцінку ризику легалізації кримінальних доходів. Розраховані ваги дозволили авторам розрахувати інтегрований показник оцінки ризику та знайти кількісну оцінку величини (сили) взаємодії між певною розглянутою країною та *k*-ю країною в розрізі ризику легалізації.

Для проведення аналізу авторами було обрано три країни – Україну, Польщу та Германію. В таблиці 1.21 представлено результати для України – 10 країн, які є найбільш привабливими для легалізації коштів з боку України, де ризик легалізації найнижчий, та 10 країн, легалізація коштів в яких з боку України буде супроводжуватися високим ризиком. На рисунку 1.51 представлена карта привабливості легалізації доходів для України в різних країнах світу.

Таблиця 1.21 – Топ країн, привабливих та непривабливих для легалізації коштів з боку України

№	Країни, непривабливі для легалізації	SVA_k'	№	Країни, привабливі для легалізації	SVA_k'
1	Lesotho	1,0000	95	Canada	0,4234
2	Algeria	1,0000	96	United Kingdom	0,4228
3	Burkina Faso	1,0000	97	Ireland	0,4227
4	Tanzania	1,0000	98	Sweden	0,4219
5	Azerbaijan	1,0000	99	Netherlands	0,4189
6	Lebanon	1,0000	100	Denmark	0,4167
7	Tajikistan	1,0000	101	Finland	0,4142
8	Senegal	1,0000	102	Iceland	0,4125
9	India	1,0000	103	Switzerland	0,4105
10	Kenya	1,0000	104	New Zealand	0,4065

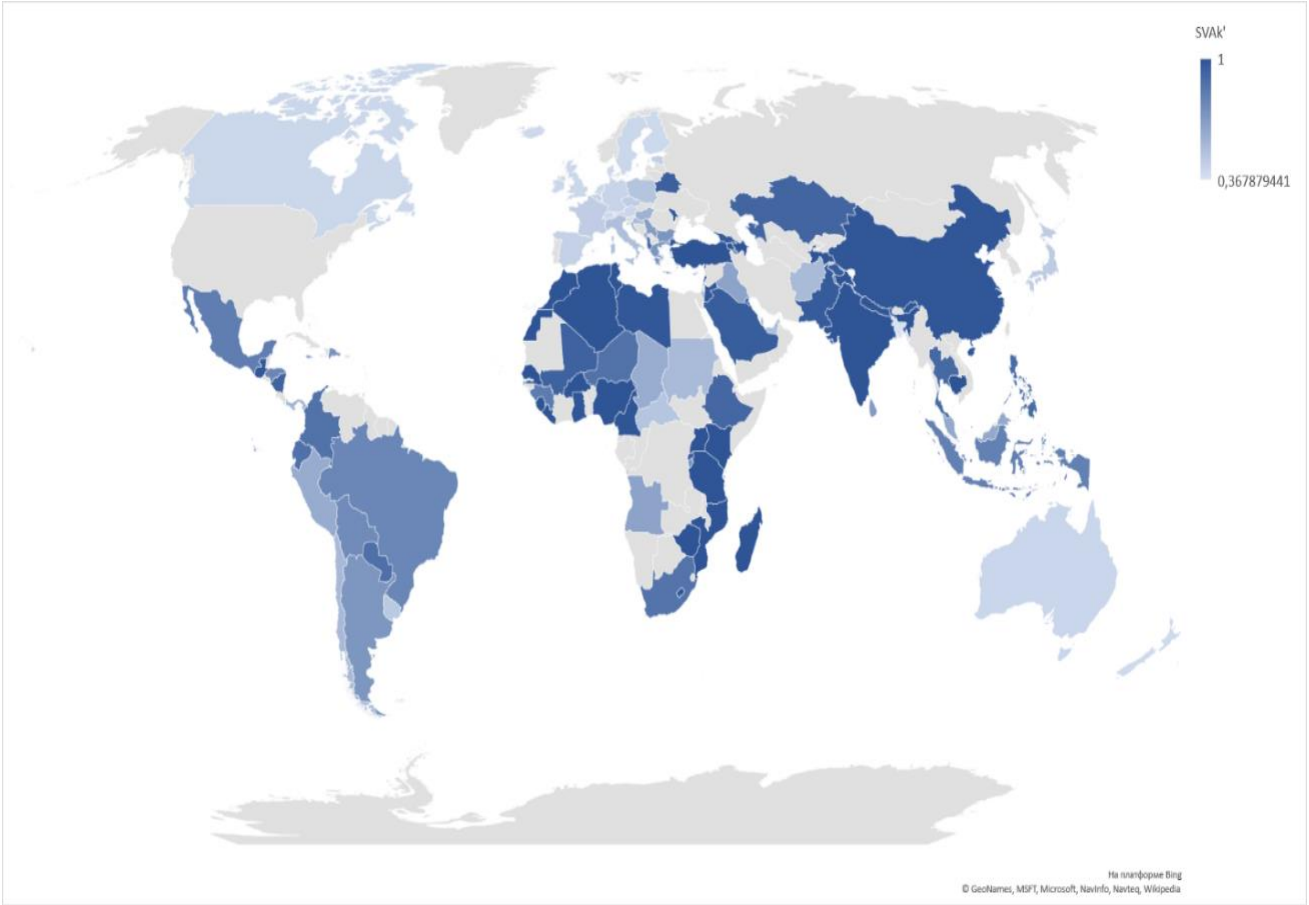


Рисунок 1.51 – Карта привабливості легалізації доходів для України в різних країнах світу

Дані таблиці 1.21 показують, що найбільш ризиковими країнами для легалізації доходів з боку України є Canada, United Kingdom, Ireland, Sweden,

Netherlands, Denmark, Finland, Iceland, Switzerland and New Zealand, які відносяться до країн з високим рівнем добробуту, протидії корупції, тощо. Завдяки своєму високому рівню розвитку вони приваблюють можливостями для легалізації коштів. Але вони також впроваджують високі стандарти захисту та протидії легалізації коштів для збереження економічної безпеки країни.

Такі країни, як Lesotho, Algeria, Burkina Faso, Tanzania, Azerbaijan, тощо у економічному розвитку та добробуті не випереджають Україну. Відповідно ризик легалізації коштів в цих країнах для неї зменшується. Така картина спостерігається й для інших країн з низькими показниками економічного розвитку та добробуту, що можна прослідкувати на рисунку 1.51. Але ці країни не є привабливими для відмивання коштів, оскільки мають низькі показники добробуту, високі показники корупції, мають воєнні конфлікти, тощо. Відповідно, ризик для країни, що легалізує, буде значним.

Українським державним установам, таким як Національна комісія, що здійснює державне регулювання у сфері ринків фінансових послуг, Державна служба фінансового моніторингу, Національний банк України, що здійснюють регулювання питань щодо руху фінансових потоків за межі України, доцільно посилити напрямки відслідковування операцій, які будуть здійснюватися в країни з високим ризиком легалізації доходів. Це можливо за рахунок встановлення певних обмежень та розширення інформації стосовно джерел доходів суб’єктів господарювання.

В таблиці 1.22 наведено результати розрахунків за запропонованою методикою для Польщі – 10 країн, де ризик легалізації найнижчий, та 10 країн, легалізація коштів в яких буде супроводжуватися високим ризиком з боку Польщі.

На рисунку 1.52 представлена карта привабливості легалізації доходів для Польщі в різних країнах світу.

Таблиця 1.22 – Топ країн, привабливих та непривабливих для легалізації коштів з боку Польщі

№	Країни, непривабливі для легалізації	SVA_k'	№	Країни, привабливі для легалізації	SVA_k'
1	United Arab Emirates	1,0000	95	Mali	0,4281
2	Chile	1,0000	96	Guinea	0,4271
3	Cyprus	1,0000	97	Lesotho	0,4254
4	Italy	1,0000	98	Iraq	0,4211
5	Uruguay	1,0000	99	Chad	0,4188
6	Croatia	1,0000	100	Burundi	0,4149
7	Panama	1,0000	101	Angola	0,4142
8	Malaysia	1,0000	102	Afghanistan	0,4081
9	Hungary	1,0000	103	Sudan	0,4042
10	Estonia	0,9997	104	Central African Republic	0,4004

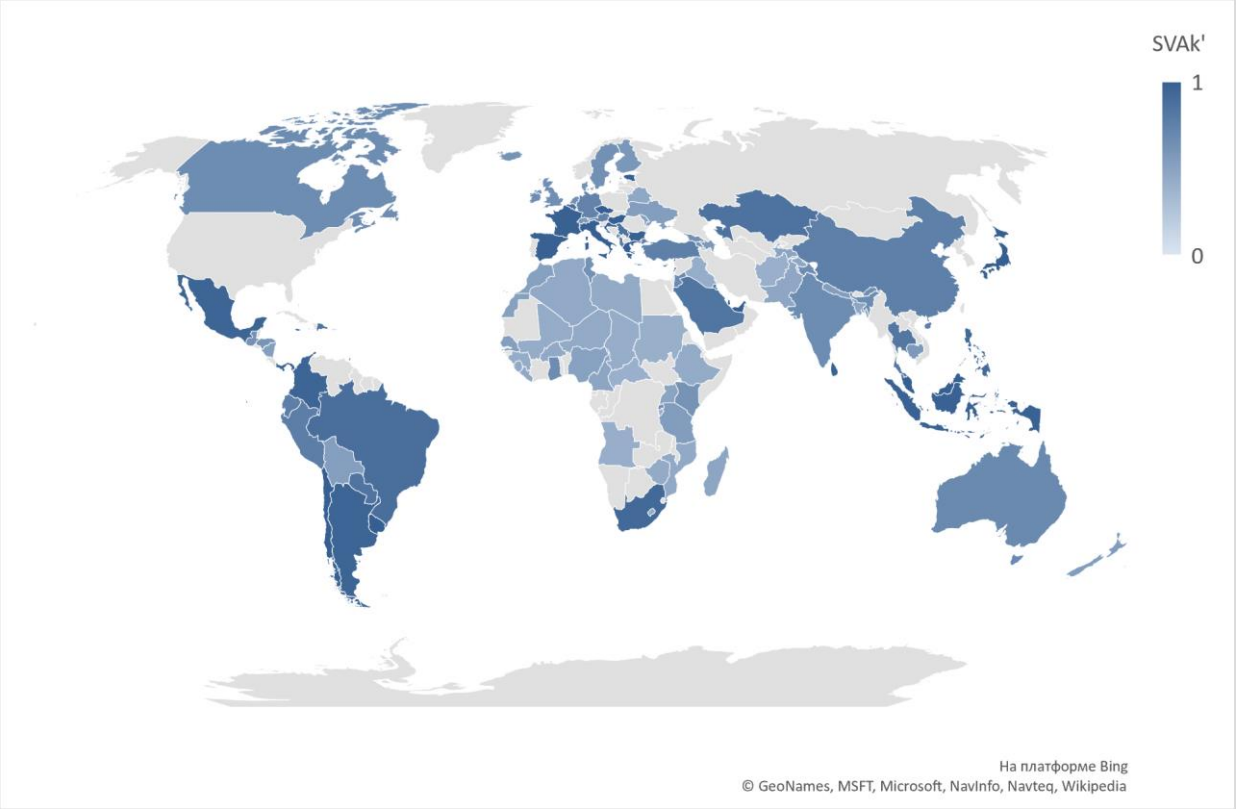


Рисунок 1.52 – Карта привабливості легалізації доходів для Польщі в різних країнах світу

Дані таблиці 1.22 показують, що найбільш ризиковими країнами для легалізації доходів для Польщі є Mali, Guinea, Lesotho, Iraq, Chad, Burundi, Angola, Afghanistan, Sudan, Central African Republic, які відносяться до країн з низьким рівнем добробуту, протидії корупції, рівнем щастя, тощо. Це

пояснюються не тільки великою різницею між економічним розвитком даних країн та Польщі, але також тим, що країни із низьким рівнем розвитку та високим рівнем тероризму, наявністю воєнних конфліктів, генеруватимуть високий ризик для відмивання коштів, що призведе до їх втрати.

Такі країни, як United Arab Emirates, Chile, Cyprus, Italy, Uruguay, Croatia, Panama, Malaysia, Hungary, Estonia, тощо генерують для Польщі низький рівень відмивання кримінальних доходів. Така картина спостерігається й для інших країн, які мають схожі із Польщею показники економічного розвитку, що можна прослідкувати на рисунку 1.52. Низький рівень ризику свідчить, що ці країни формують для Польщі умови, які є сприятливими для легалізації.

В таблиці 1.23 наведено результати розрахунків кількісної оцінки величини (сили) взаємодії між Германією та 10 країнами, де ризик легалізації найнижчий, та 10 країнами, де ризик легалізації найвищий.

На рисунку 1.53 представлена карта привабливості легалізації доходів для Германії в різних країнах світу.

Таблиця 1.23 – Топ країн, привабливих та непривабливих для легалізації коштів з боку Германії

№	Країни, непривабливі для легалізації	SVA_k'	№	Країни, привабливі для легалізації	SVA_k'
1	Canada	1,0000	95	Chad	0,4306
2	Ireland	1,0000	96	Zimbabwe	0,4298
3	Iceland	1,0000	97	Belarus	0,4292
4	Austria	1,0000	98	Mali	0,4283
5	Netherlands	1,0000	99	Angola	0,4214
6	Denmark	1,0000	100	Burundi	0,4195
7	United Kingdom	1,0000	101	Afghanistan	0,4186
8	Switzerland	1,0000	102	Lesotho	0,4150
9	Sweden	1,0000	103	Sudan	0,4125
10	Belgium	1,0000	104	Central African Republic	0,4101

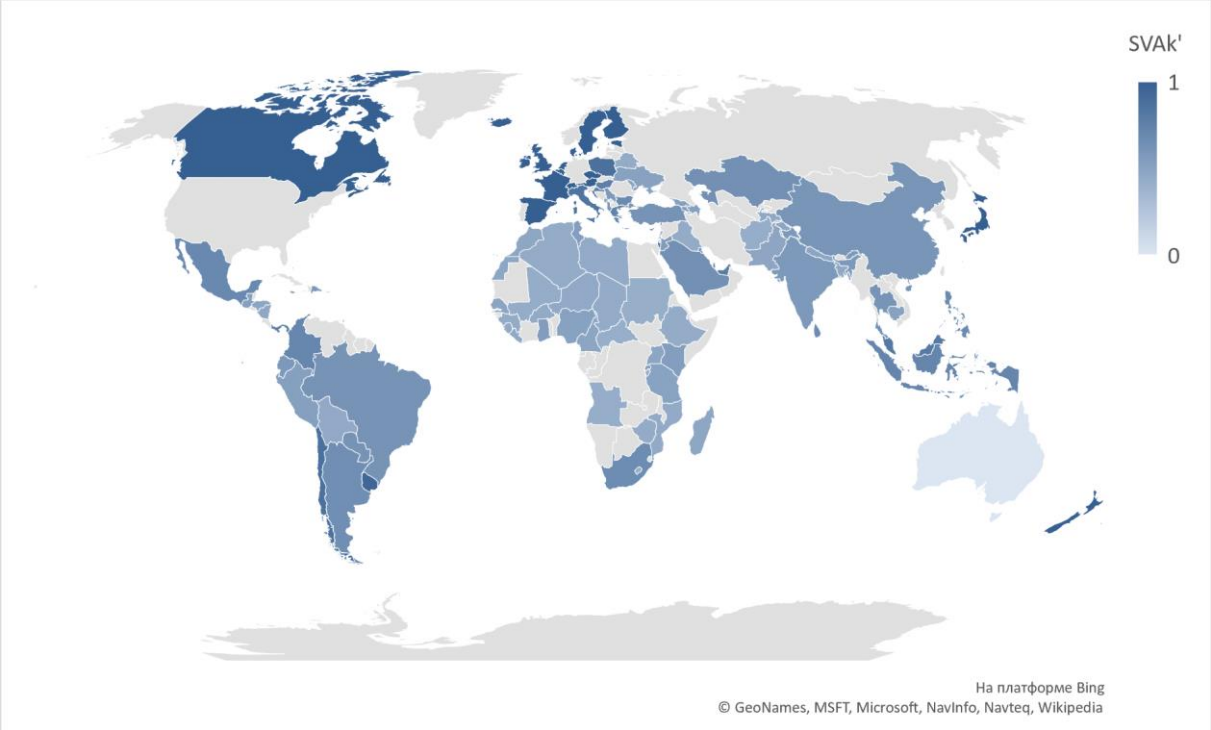


Рисунок 1.53 – Карта привабливості легалізації доходів для Германії в різних країнах світу

Такі країни, як Canada, Ireland, Iceland, Austria, Netherlands, Denmark, United Kingdom, Switzerland, Sweden, Belgium, для країн з високим рівнем економічного розвитку та економічної безпеки, як Германія, генерують низький ризик легалізації, що обумовлено схожістю рівнів добробуту. Але оскільки в даних країнах діють підвищені стандарти захисту від припливу кримінальних доходів, то для Германії зменшуються можливості легалізації доходів саме в цих країнах.

Навпаки, у таких країнах, як Chad, Zimbabwe, Belarus, Mali, Angola, Burundi, Afghanistan та інші, які представлені в таблиці 1.23 та на рисунку 1.53, ризик легалізації кримінальних доходів для Германії підвищується. Ступінь привабливості для легалізації доходів у таких країн низька, оскільки для них характерні не високі показники економічного розвитку та нестабільне політичне становище. Але у разі існування таких можливостей, Deutche Bundesbank може розробити стратегію блокування легалізації доходів саме для країн цієї групи, що

сприятиме забороні виведення грошей з країни та втрати їх через відведення у тінь.

Такий процес, як легалізація кримінальних доходів та фінансування тероризму, для будь-яких країн світу, як правило, носить несприятливий характер, особливо для економічної безпеки країни. По-перше, цей процес сприяє зростанню тіньового сектору в економіці, оскільки частина доходів скривається. По-друге, бюджет держави втрачає значні кошти, оскільки з таких доходів, як кримінальні, не сплачуються податки. По-третє, легалізація кримінальних доходів сприяє створенню та розповсюдженню шахрайських схем щодо фінансових потоків. По-четверте, збільшується відтік інвестицій та знижується привабливість бізнесу. По-п’яте, збільшуються витрати держави на боротьбу із фінансовою злочинністю. Все це призводить до підриву устоїв економічної безпеки країни, може впливати на появу та збільшення терористичних загроз для суспільства, що врешті-решт може призвести також й до порушення соціальної безпеки в країні.

Запропонована методика покликана сприяти зменшенню ризиків для держави з боку легалізації кримінальних доходів та фінансування тероризму. Її застосування на рівні державних структур дозволить сформувати інформаційну базу для прийняття управлінських рішень щодо підвищення рівня економічної безпеки країни, оскільки це надає можливості концентрувати увагу саме на тих країнах, з якими ризик легалізації є підвищеним. Впровадження даної методики сприятиме розробці нових інструментів моніторингу, аналізу, оцінки та прогнозування фінансових операцій, здійснення яких можливе за межами країни. Так, це дозволить створити механізм взаємодії з іншими країнами в плані визначення обсягів фінансових операцій, цільових видів діяльності, джерел походження ресурсів, тощо. В свою чергу, це потребуватиме удосконалення законодавчої бази для фінансово-кредитних установ, суб’єктів господарювання, а також осіб, що придбають нерухомість, акції закордоном, або є пов’язаними з іншими посередниками.

Інформація, яка є результатом запропонованої методики, слугує підґрунтям для удосконалення стандартів економічної політики країни з боку посилення економічної безпеки та розвитку партнерських відносин з іншими країнами. Це можливе за рахунок розвитку нових інформаційних технологій щодо збору та обміну інформацією не тільки в середині країни стосовно фінансових потоків, але й по всьому світу, за рахунок залучення нових учасників. Так, застосування The Automatic Exchange of Information дозволяє вирішувати питання ухилення від сплати податків, але при обміні інформацією не розкривається інформація щодо руху коштів на рахунках для дотримання банківської таємниці. В частині даного обміну можна впровадити електронну ідентифікацію джерел доходів та характеру операцій, що дозволить не порушуючи банківську таємницю позначати операції із сумнівними джерелами доходу та повідомляти про спробу їх здійснення у правоохоронні органи. Подібну ідентифікацію доцільно впроваджувати на рівні банків, як обов'язковий елемент звітності банківських установ перед державою.

Запропоновану методику планується удосконалити в частині визначення найбільш ризикованих видів економічної діяльності країн, які є привабливими для легалізації доходів. Також дослідження буде спрямоване на інтеграцію показників методики з показниками інших сфер безпеки країни – політичною, соціальною, економічною. В подальшому планується впровадити запропоновану методику в діяльність Національної комісії, що здійснює державне регулювання у сфері ринків фінансових послуг, Державної служби фінансового моніторингу та Національного банку України.

Пункт 1.4.2 даного звіту було виконано із використанням матеріалів проміжного звіту про НДР [11], публікацій виконавців [48].

1.4.3 Розробка прототипу автоматизованого модулю процесу виявлення шахрайських операцій з банківськими картками

Шахрайські операції з банківськими картками – це те, що може загальмувати розвиток онлайн-бізнесу. Якщо товаром або послугою скористався шахрай, втрачається і товар, і гроші. Дуже просто купити товар на сайті, ввівши при оплаті номер карти й інші цифри, які надруковані на ній. Але при цьому карта буде чужа – введені дані можна сфотографувати або підглянути, роздобути за допомогою технологічних махінацій з банкоматами або через слабо захищені сайти інших інтернет-магазинів. Після виконання шахрайської операції справжній власник картки обов'язкового напише заяву в банк про повернення списаної без його відома суми. У разі проходження несанкціонованої операції по банківській карті через інтернет-магазин банк-емітент за дорученням власника картки опротестує транзакцію і онлайн-крамниця буде зобов'язана відшкодувати всю вартість покупки.

Одним з кроків створення ефективної інформаційної системи є її попереднє моделювання. Відтворення моделі дозволяє отримати загальний вигляд даних інформаційної системи. Цей загальний вигляд системи, яким користуються всі учасники (всі підсистеми), є механізмом, що дозволяє системно підійти до проекту. Бізнес-процес відображає організаційну структуру системи і моделювання може дозволити організації належним чином керувати своїм робочим процесом. Моделювання бізнес-процесів може систематично відображати потоки ділової активності, що дозволяє проводити відповідний аналіз та моделювання. Моделювання бізнес-процесів визнаються як інструмент, який може допомогти організації ефективно працювати і легко знаходити проблемні зони. Більше того, він дозволяє перетворити або модернізувати бізнес-процеси. Таким чином, чим краще буде моделювання бізнес-процесів, тим більше можна покращити продуктивність та конкурентоспроможність організації.

Під час попереднього дослідження (перша ітерація) вибираються найважливіші дані з урахуванням обсягу та частоти процесів. Важливо визначити підмножину інформації, що дозволить добре сформулювати модель даних та всі підсистеми.

Система виявлення шахрайських операцій складається з наступних складових (підсистем):

– Fraud Predictor Service – сервіс виявлення шахрайських операцій за допомогою перевірки за різними фільтрами;

– Transactions Log – база даних транзакцій банківських карт;

– SMS API Service – сервіс верифікації за допомогою повідомлення на мобільний телефон.

Крім того система містить клієнтські веб-додатки як, наприклад, веб-додаток для відображення транзакцій, котрі система визначила шахрайськими.

Взаємодію компонентів як єдиної системи, що пропонується, продемонстровано на діаграмі послідовності на рисунку 1.54.

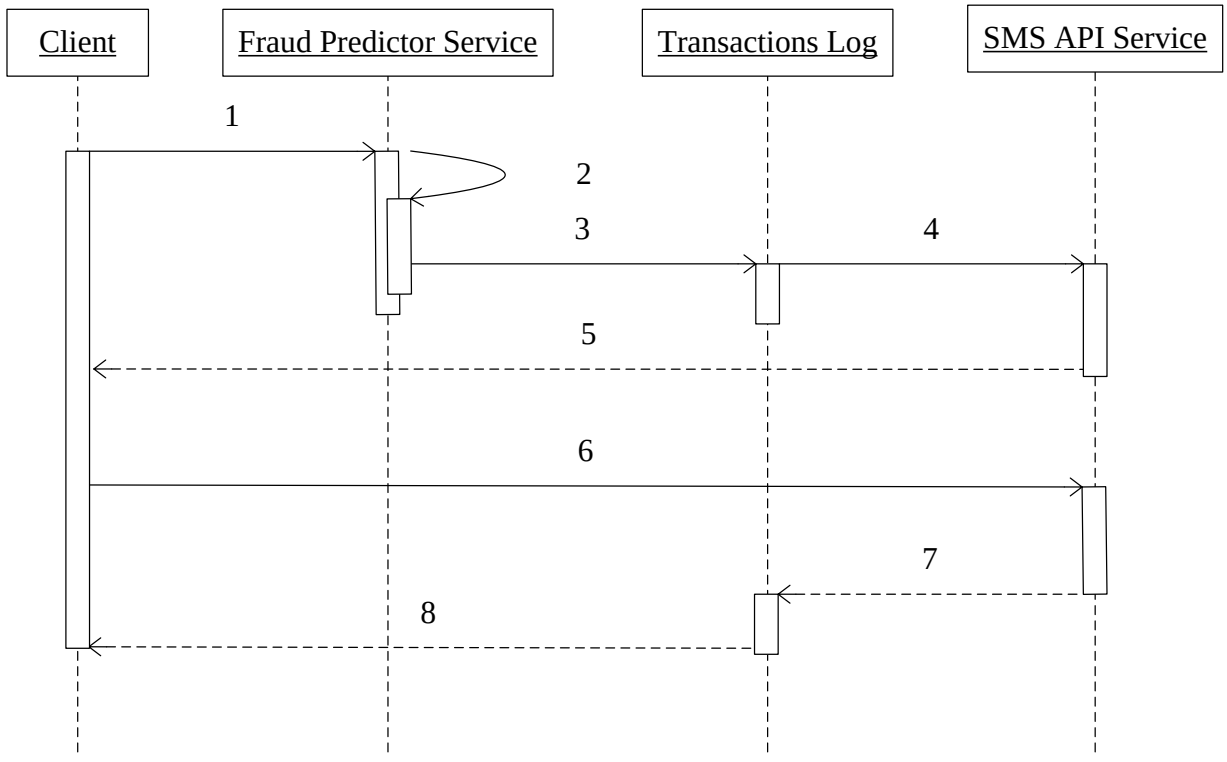


Рисунок 1.54 – Діаграма послідовності системи

Прокоментуємо подану діаграму поетапно:

– Крок 1. Відправка запиту з боку клієнта до системи.

– Крок 2. Робота сервісу виявлення шахрайських операцій та повернення результату – чи буде платіж шахрайським.

– Крок 3. Збереження даних.

– Крок 4. Виклик вікна додаткової верифікації.

– Крок 5. Повернення результату клієнту.

– Крок 6. Введення коду, отриманого у повідомлені.

– Крок 7. Зміна інформації про транзакцію.

– Крок 8. Повернення результату клієнту.

Кроки 4-8 відбуваються тільки у випадку шахрайського платежу.

Перед розробкою автоматизованої системи необхідно розглянути її з точки зору бізнес-процесів, побудувавши бізнес-моделі. Вони являють собою формалізований (графічний, табличний, текстовий, символьний) опис бізнес-процесів, що відображає реально існуючу або передбачувану діяльність [49].

Для моделювання та опису бізнес-процесів прийнято використовувати спеціалізовані системи управління бізнес процесами – BMP (Business Process Management) системи, які використовують наступні нотації моделювання:

– BPMN (Business Process Model and Notation) – нотація моделювання бізнес процесів, яка забезпечує високий рівень наочного зображення процесу. Вони розробляються як стандартні блок-схеми.

– BPEL (Business Process Execution Language) – це спеціальна XML-мова виконання бізнес-процесів. Вона подає окремий бізнес-процес у вигляді послідовності веб-сервісів.

– DFD (Data Flow Diagramming) – опис потоків даних. Відображення інформаційних потоків, які відбуваються протягом робіт. Також дану нотацію застосовують для опису документообігу.

– IDEF0 (Business Process Modeling) – методологія для опису бізнес-процесів, чиї моделі використовуються для опису робіт процесу. В нотації

враховуються не тільки входи і виходи, а й управління та механізми, тобто дозволяє описувати керування процесами організації.

– IDEF3 – нотація, що зосереджена на описі потоків робіт (Work Flow Modelling). Стандарт IDEF3 наближений до стандартних блок-схем, але включає в себе орієнтованість на алгоритмічність методу побудови схем бізнес-процесів.

– XPDL (XML Process Definition Language) – формат обміну даними між BPM-системами. Використовується в основному як стандарт виконання експорту-імпорту описів бізнес-процесів [50].

Для опису бізнес-моделі нашої системи будемо використовувати нотації IDEF0 та IDEF3.

На рисунку 1.55 зображено контекстну діаграму процесу виявлення шахрайських операцій. Після неї наведемо пояснення до кожного елементу, що присутній на діаграмі (таблиця 1.24).

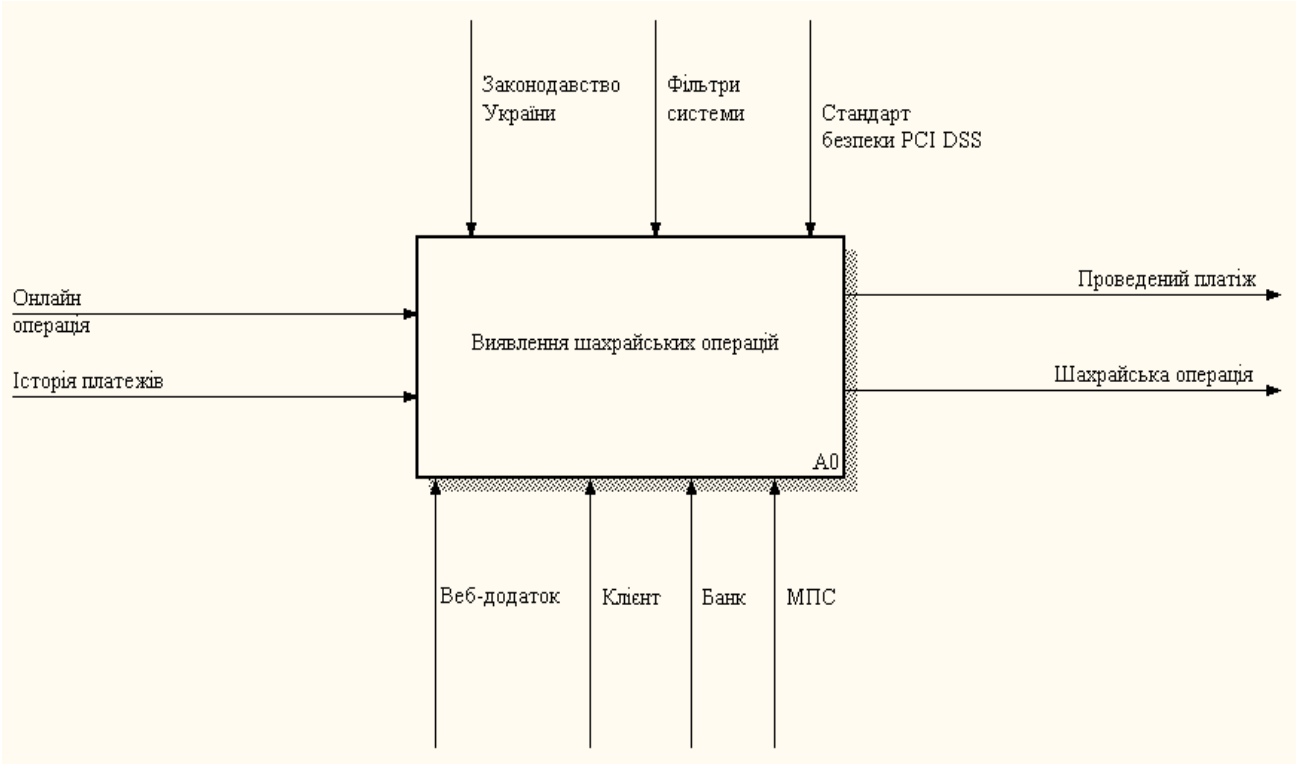


Рисунок 1.55 – Контекстна діаграма «Виявлення шахрайських операцій»

Таблиця 1.24 – Опис основних елементів контекстної діаграми

Назва стрілки	Опис	Тип
Онлайн операція	Операція купівлі товару в інтернет-магазині за допомогою банківської картки	Input
Історія платежів	Попередні операції в Інтернеті	Input
Законодавство України	Закони України, що регулюють процес проведення онлайн-платежів та взаємодію його учасників	Control
Фільтри системи	Критерії, яким повинні відповідати нешахрайські операції	Control
Стандарт безпеки PCI DSS	Стандарт безпеки даних індустрії банківських платіжних карток	Control
МПС	Міжнародна платіжна система	Mechanism
Веб-додаток	Форми для зв’язку з клієнтом	Mechanism
Банк	Банк, який випустив банківську картку клієнту	Mechanism
Клієнт	Особа, яка проводить платіж в мережі Інтернет	Mechanism
Проведений платіж	Успішно проведена транзакція клієнта	Output
Шахрайська операція	Виявлена шахрайська операція	Output

Контекстна діаграма не дає детального та повного розуміння суті процесу. Тому наступним кроком є декомпозиція контекстної діаграми, тобто розбиття на частини (підпроцеси), щоб глибше розібрати даний процес виявлення шахрайських операцій (рисунок 1.56).

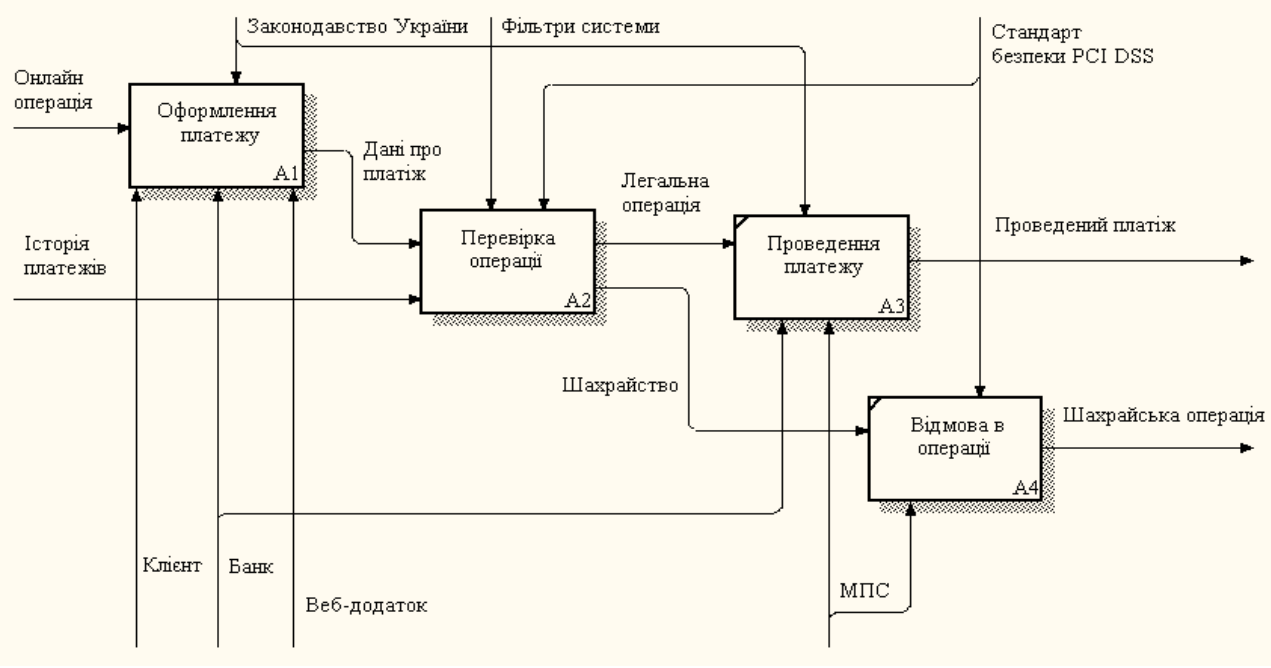


Рисунок 1.56 – Декомпозиція контекстної діаграми

Для поданого рисунка необхідно навести опис робіт (таблиця 1.25).

Таблиця 1.25 – Опис робіт діаграми-декомпозиції

Функціональний блок	Опис	Тип
Оформлення платежу	Заповнення форми купівлі товару в Інтернеті	WORKING
Перевірка операції	Моніторинг операції та аналіз її на можливість шахрайства	WORKING
Проведення платежу	Підтвердження транзакції купівлі	WORKING
Відмова в операції	Операцію визнано шахрайською, транзакція відхилена	WORKING

За аналогією до контекстної діаграми наведемо опис зв’язків між роботами діаграми-декомпозиції контекстної діаграми, де буде вказано назва стрілки, її джерело, призначення, один із чотирьох можливих типів (табл. 1.26).

Таблиця 1.26 – Опис зв’зків між роботами діаграми-декомпозиції

Назва стрілки	Джерело	Тип	Призначення	Тип
Онлайн операція	Контекстна діаграма		Оформлення платежу	Input
Історія платежів	Контекстна діаграма		Перевірка операції	Input
Законодавство України	Контекстна діаграма		Оформлення платежу, проведення платежу	Control
Фільтри системи	Контекстна діаграма		Перевірка операції	Control
Стандарт безпеки	Контекстна діаграма		Перевірка операції, відмова в операції	Control
Клієнт	Контекстна діаграма		Оформлення платежу	Mechanism
Банк	Контекстна діаграма		Оформлення платежу, проведення платежу	Mechanism
Веб-додаток	Контекстна діаграма		Оформлення платежу	Mechanism
МПС	Контекстна діаграма		Проведення платежу, відмова в операції	Mechanism
Дані про платіж	Оформлення платежу	Output	Перевірка операції	Input
Легальна операція	Перевірка операції	Output	Проведення платежу	Input
Шахрайство	Перевірка операції	Output	Відмова в операції	Input
Шахрайська операція	Відмова в операції	Output	{Border}	Output
Проведений платіж	Проведення платежу	Output	{Border}	Output

Для кращого розуміння процесів потрібно дослідити підпроцеси «оформлення платежу» та «перевірка операції» (рисунок 1.57), де зображено 3

роботи, які складають процес оформлення платежу. Необхідно навести їх опис у вигляді таблиці 1.27. Також потрібно продемонструвати зв’язків між ними, описавши їх в таблиці 1.28. Зв’язки об’єднують не тільки роботи в цій діаграмі-декомпозиції, а й в батьківській.

Таблиця 1.27 – Опис робіт діаграми-декомпозиції

Функціональний блок	Опис	Тип
Заповнення банківських реквізитів	Процес введення клієнтом даних банківської картки	WORKING
Заповнення адреси доставки	Процес введення регіону та місту, куди відправляти товар	WORKING
Визначення місцезнаходження	Пошук міста, в якому знаходиться клієнт, за допомогою IP-адреси	WORKING

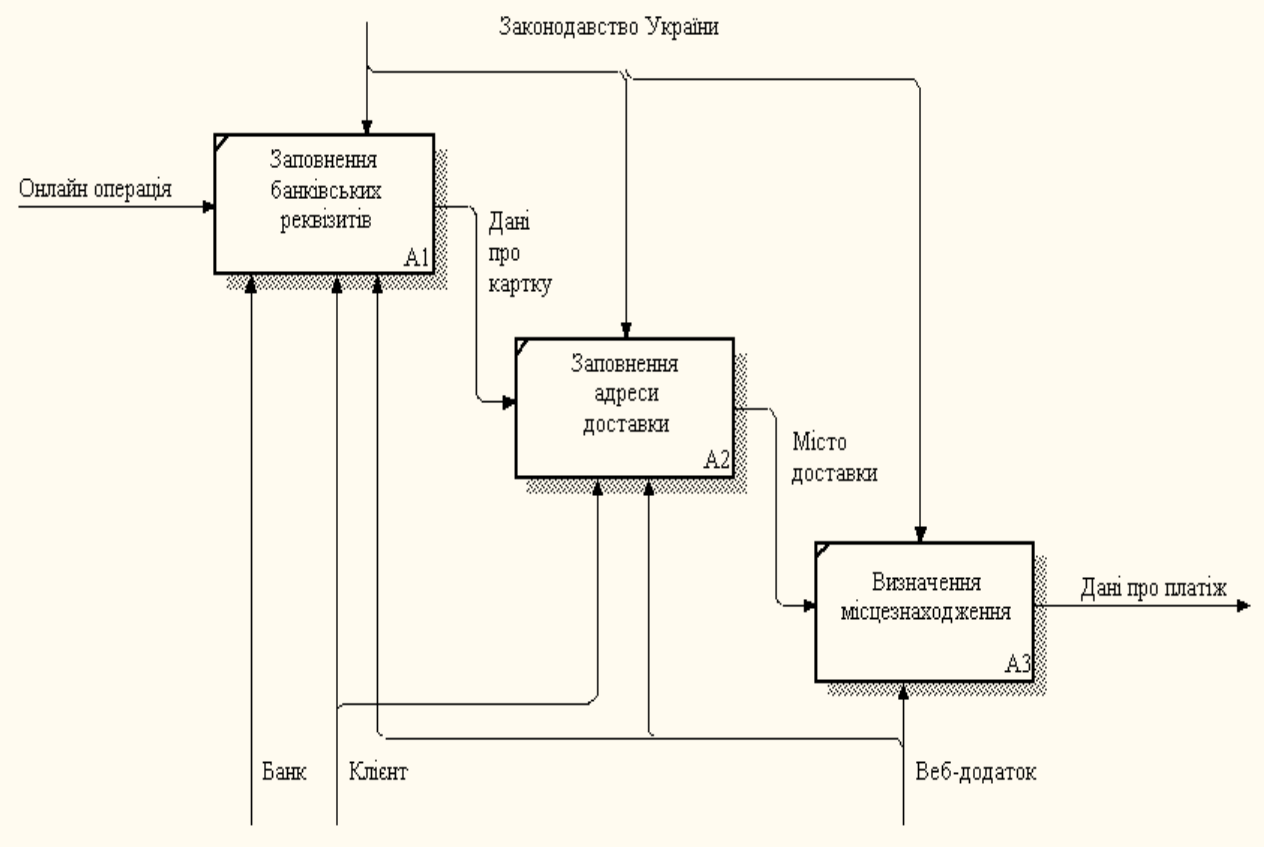


Рисунок 1.57 – Діаграма-декомпозиція процесу «оформлення платежу»

Таблиця 1.28 – Опис зв’зків між роботами діаграми-декомпозиції

Назва стрілки	Джерело	Тип	Призначення	Тип
Онлайн операція	Контекстна діаграма		Заповнення банківських реквізитів	Input
Законодавство України	Контекстна діаграма		Заповнення банківських реквізитів, заповнення адреси доставки, визначення місцезнаходження	Control
Банк	Контекстна діаграма		Заповнення банківських реквізитів	Mechanism
Клієнт	Контекстна діаграма		Заповнення банківських реквізитів, заповнення адреси доставки	Mechanism
Веб-додаток	Контекстна діаграма		Заповнення банківських реквізитів, заповнення адреси доставки, визначення місцезнаходження	Mechanism
Дані про картку	Заповнення банківських реквізитів	Output	Заповнення адреси доставки	Input
Місце доставки	Заповнення адреси доставки	Output	Визначення місцезнаходження	Input
Дані про платіж	Визначення місцезнаходження	Output	Перевірка операції, відмова в операції	Output

Для декомпозиції другого підпроцесу скористаємося нотацією IDEF3. Вона краще підходить для опису процесів на глибоку рівні декомпозиції, тому що зображує послідовність виконання процесів як деякий алгоритм.

Як і в IDEF0, основною одиницею опису IDEF3-моделі є діаграма. На діаграмі зображуються одиниці роботи (UnitOfWork), які є центральними компонентами моделі. Істотною відмінністю IDEF3 від IDEF0 є наявність перехресть. Вони бувають перехрестями злиття (Fan-in Junction) та перехрестя розгалуження (Fan-out Junction).

IDEF3 діаграму перевірки операцій наведено на рисунку 1.58. Детальний опис поданої діаграми наведемо в наступній таблиці 1.29.

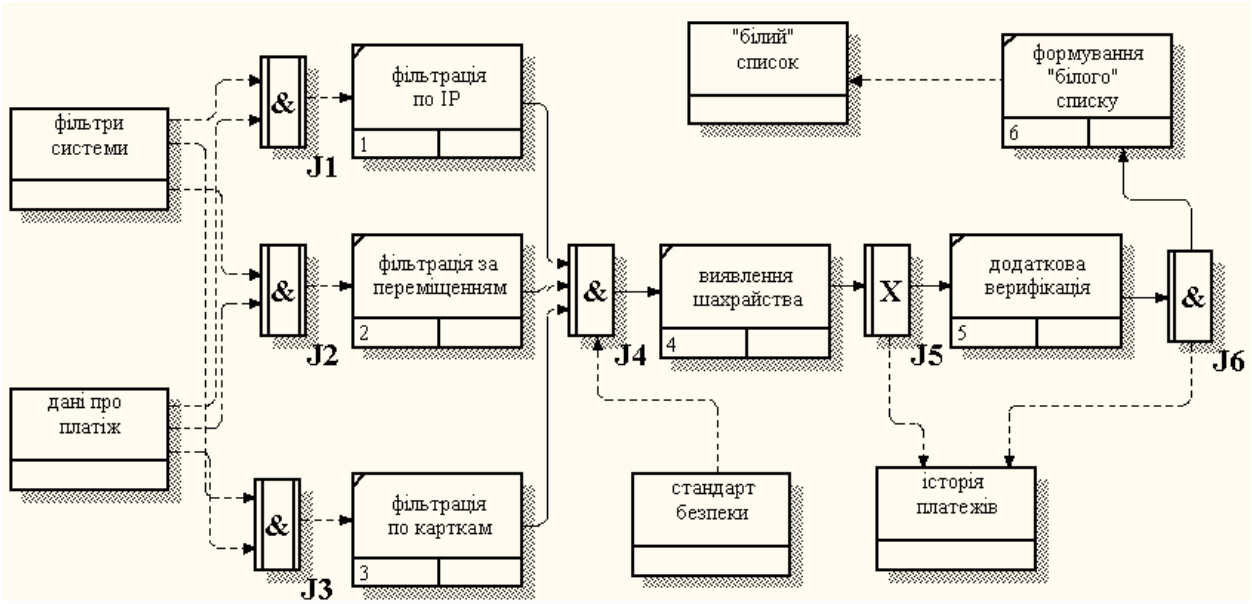


Рисунок 1.58 – IDEF3 діаграма системи виявлення шахрайства

В нотації IDEF3 продемонстровано 6 робіт зв’язаних між собою перехрестями: асинхронної, синхронної кон’юнкції та виключної диз’юнкції. Роботи між собою поєднуються стрілками пріоритету, а із зовнішніми об’єктами – стрілками відношення.

Таблиця 1.29 – Опис робіт діаграми

Функціональний блок	Опис	Тип
Фільтрація по IP	Процес порівняння поточного місця знаходження та адреси доставки	WORKING
Фільтрація за переміщенням	Процес аналізу швидкості переміщення клієнта	WORKING
Фільтрування по картках	Розрахунок унікальних банківських карт	WORKING
Виявлення шахрайства	Узагальнення результатів роботи фільтрів	WORKING
Додаткова верифікації	Підтвердження достовірності особи	WORKING
Формування «білого» списку	Процес верифікації банківських карт та IP-адрес	WORKING
Дані про платіж	Інформація про місце знаходження клієнта, адреса замовлення, минулі платежі	DATABASE
«Білий» список	Карти, платежі за якими не потребують підтвердження	DATABASE
Фільтри системи	Фільтри для виявлення шахрайства	DATABASE
Історія платежів	Список всіх транзакцій по окремій картці	DATABASE
Стандарт безпеки	Вимоги забезпечення безпеки даних банківських карт	DATABASE

Реалізація автоматизованого модулю передбачає також створення інформаційного забезпечення. В даному випадку воно буде у вигляді реляційної бази даних. База даних буде зберігати тільки необхідну інформацію, яка пов’язана із перевіркою платежу на шахрайство. Інформаційне забезпечення стосовно перевірки банківської картки на вірність терміну дієї та CVV2 буде знаходитися у відповідного банку.

Усю інформацію, з якою працює автоматизований модуль можна виокремити у три групи:

- інформація, яку вводить клієнт;
- інформація, яка зберігається у системі (історія транзакцій);
- інформація, що виводиться співробітнику банка.

Для зберігання поданої інформації необхідно створити наступні сутності:

- «clients» – інформація про клієнтів;
- «cards» – інформація про банківські карти;
- «transactions» – інформація про всі транзакції;
- «frauds» – інформація про транзакції, які позначили шахрайськими;
- «location» – довідник місцезнаходження від IP-адреси;
- «location_ua» – довідник місцезнаходження в Україні від IP-адреси.

В результаті створення бази даних, було отримані наступні таблиці з відповідними структурами (таблиця 1.30 – 1.35).

Таблиця 1.30 – Структура таблиці «clients»

№	Назва атрибута	Тип даних	Обмеження	Призначення атрибута
1	clientID	int(11)	AUTO_INCREMENT	Первинний ключ
2	fname	varchar(100)	NOT NULL	Ім’я клієнта
3	sname	varchar(100)	NOT NULL	Прізвище клієнта
4	patronymic	varchar(100)	NOT NULL	По-батькові клієнта
5	telephone	varchar(12)	NOT NULL	Номер телефона

Таблиця 1.31 – Структура таблиці «transactions»

№	Назва атрибута	Тип даних	Обмеження	Призначення атрибута
1	transactionID	int(11)	AUTO_INCREMENT	Первинний ключ
2	cardID	varchar(16)	FOREIGN KEY, NOT NULL	Зовнішній ключ, номер банківської картки
3	time	datetime	NOT NULL, CURRENT_ TIMESTAMP	Дата та час транзакції
4	region	varchar(128)	NOT NULL	Регіон доставки
5	ort	varchar(128)	NOT NULL	Місто доставки
6	ip	int(10)	NOT NULL, UNSIGNED	IP-адреса транзакції
7	fraud	boolean	NOT NULL, DEFAULT=0	Виявлено шахрайство

Таблиця 1.32 – Структура таблиці «location»

№	Назва атрибута	Тип даних	Обмеження	Призначення атрибута
1	ip_from	int(10)	UNSIGNED	Початок діапазону IP-адреси
2	ip_to	int(10)	UNSIGNED	Кінець діапазону IP-адреси
3	country_code	char(2)	-	Код країни
4	country_name	varchar(64)	-	Назва країни
5	region_name	varchar(128)	-	Назва регіону
6	city_name	varchar(128)	-	Назва міста
7	latitude	double	-	Географічна широта
8	longitude	double	-	Географічна довгота
9	zip_code	varchar(30)	-	Поштовий індекс

Таблиця 1.33 – Структура таблиці «frauds»

№	Назва атрибута	Тип даних	Обмеження	Призначення атрибута
1	fraudID	int(11)	AUTO_INCREMENT	Первинний ключ
2	transactionID	int(11)	FOREIGN KEY, NOT NULL	Зовнішній ключ
3	code	int(11)	NOT NULL	Код підтвердження клієнта
4	reason	varchar(128)	NOT NULL	Причина виявлення шахрайства

Таблиця 1.34 – Структура таблиці «cards»

№	Назва атрибута	Тип даних	Обмеження	Призначення атрибута
1	cardID	varchar(16)	NOT NULL	Первинний ключ, номер банківської картки
2	clientID	int(11)	FOREIGN KEY, NOT NULL	Зовнішній ключ

Таблиця 1.35 – Структура таблиці «location_ua»

№	Назва атрибута	Тип даних	Обмеження	Призначення атрибута
1	ip_from	int(10)	UNSIGNED	Початок діапазону IP-адреси
2	ip_to	int(10)	NOT NULL	Кінець діапазону IP-адреси
3	region_name	varchar(128)	NOT NULL	Назва регіону
4	city_name	varchar(128)	NOT NULL	Назва міста
5	latitude	double	NOT NULL	Географічна широта
	longitude	double		Географічна довгота

Відношення між таблицями були встановлені наступні:

- «clients» – «cards» – відношення один до багатьох;
- «cards» – «transactions» – відношення один до багатьох;
- «transactions» – «frauds» – відношення один до одного.

Схематичне зображення всіх сутностей з атрибутами та зв’язків між ними прийнято подавати у вигляді схеми база даних або моделі сутність-зв’зок. Програмне забезпечення Open Server забезпечує таку можливість у спеціальному вікні «Дизайн» (рисунок 1.59).

Зв’зок між сутностями location та location_ua на рівні бази даних не передбачений, тому що вони являють собою довідники місцезнаходження без первинного ключа. В них немає атрибуту, з яким можна поєднати сутність transactions, так як шукана ip-адреса повинна знаходитись в діапазоні, а не дорівнювати певному значенню. Сценарій створення бази даних, усіх таблиць з атрибутами та зв’язків між ними наведено в Додатку А.

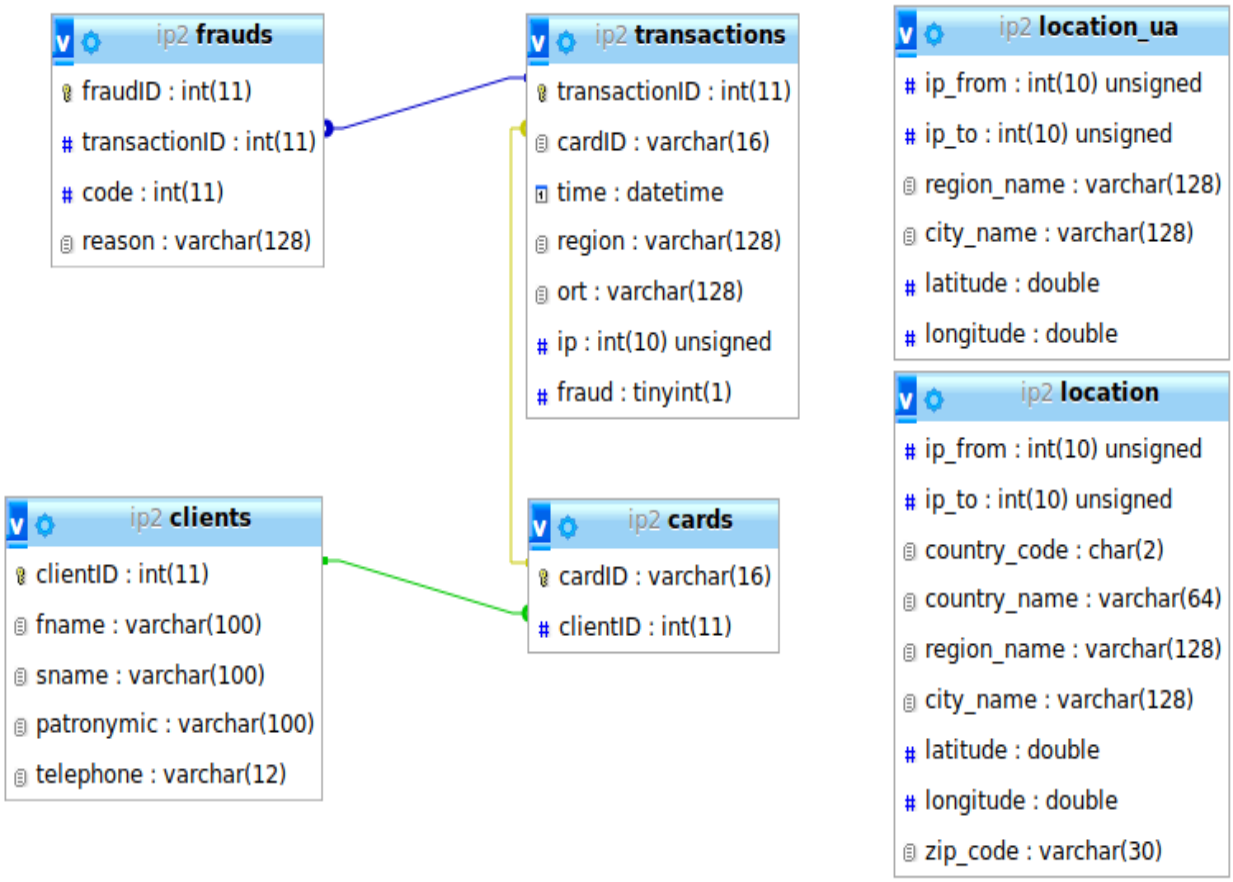


Рисунок 1.59 – Схема бази даних автоматизованого модуля виявлення шахрайських операцій з картками

Логіка будь-якого додатку полягає в його функціональних можливостях та алгоритмічному забезпеченні. Головна ідея цього модулю – це виокремлення шахрайських операцій та робота з ними. Враховуючи це, найголовнішим є аналіз онлайн-платежу за різними параметрами і винесення результат за кожним компонентом системи. Внутрішня система аналізу складається з трьох компонент (фільтрів), перевірку через які повинен пройти платіж. На кожному етапі система повертає результат, чи є операція шахрайською. Роботу даних фільтрів можна зобразити у вигляді блок-схем (рисунок 1.60-1.63).

Логіка алгоритму, продемонстрованого на рисунку 1.60, полягає у підрахунку кількості банківських карт. При виконані операції з певної IP-адреси, програма визначає зі скількох інших банківських карт виконувалися онлайн-

операції за останню добу. Якщо унікальних карт буде більше двох, то операція вважається шахрайською.

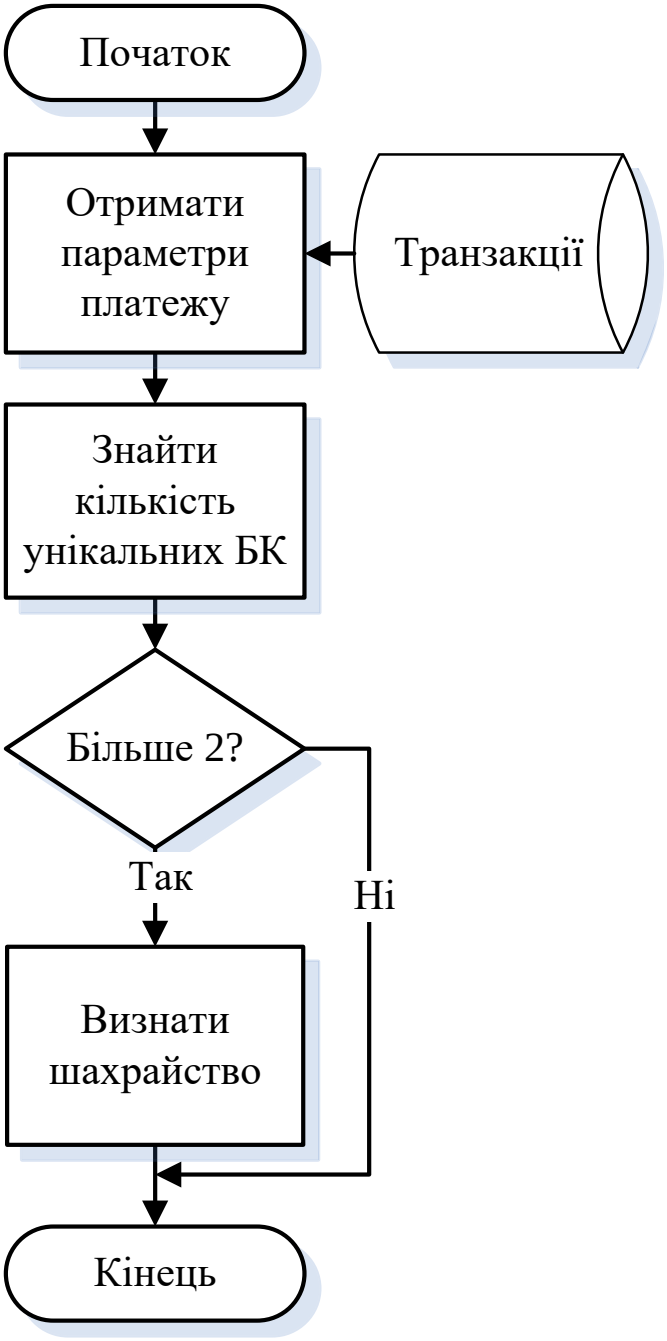


Рисунок 1.60 – Блок-схема алгоритму фільтрування за кількістю карт

Рисунок 1.61 демонструє алгоритм, за яким відбувається аналіз переміщення клієнта. Розраховується швидкість, з якою клієнт подолав відстань за час з моменту останньої операції і порівнюється з критичним значенням у 50

км/год. Якщо швидкість клієнта була більшою, то це є підозрілим і операція вважається шахрайською.

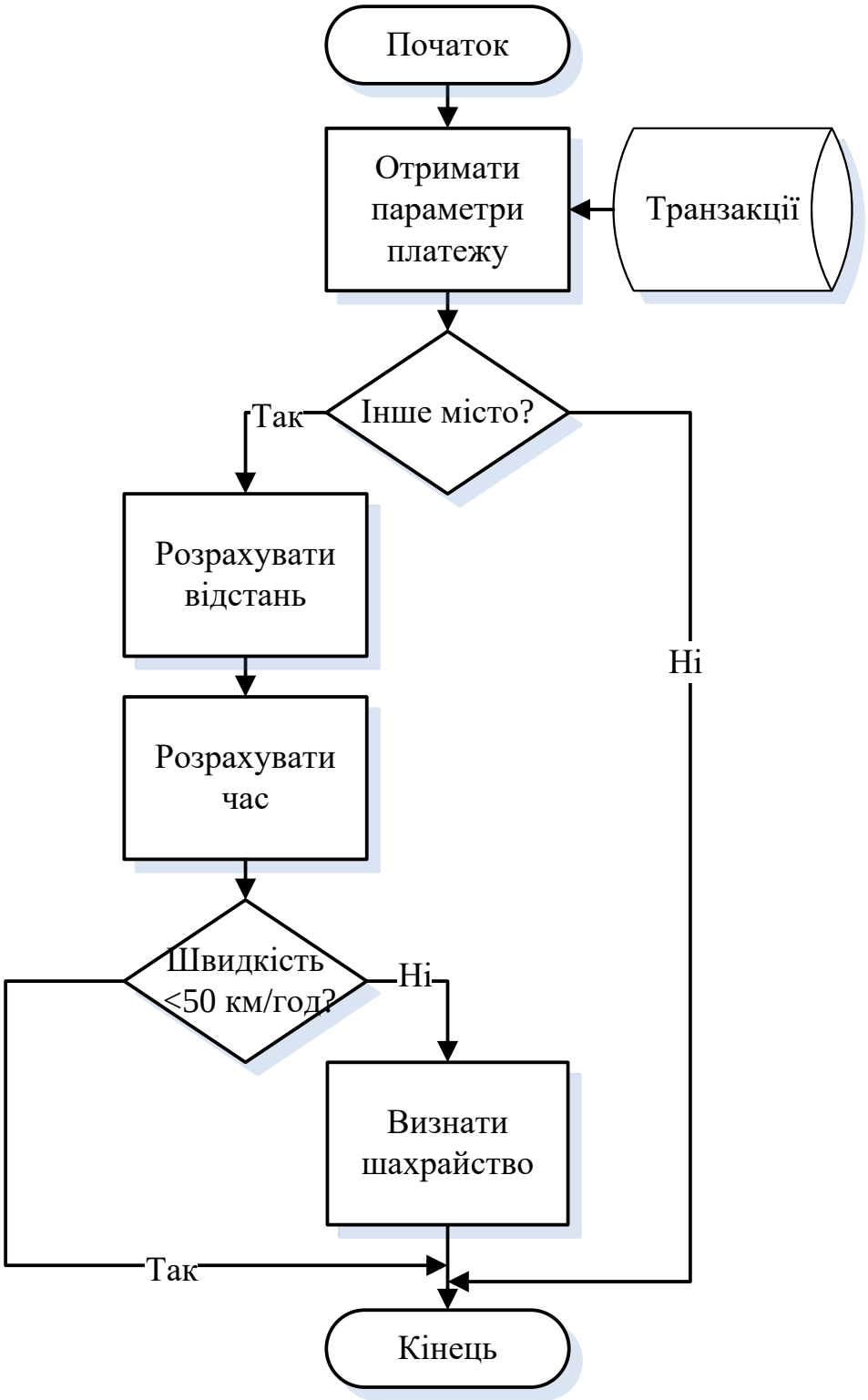


Рисунок 1.61 – Блок-схема алгоритму фільтрування за швидкістю переміщення клієнта

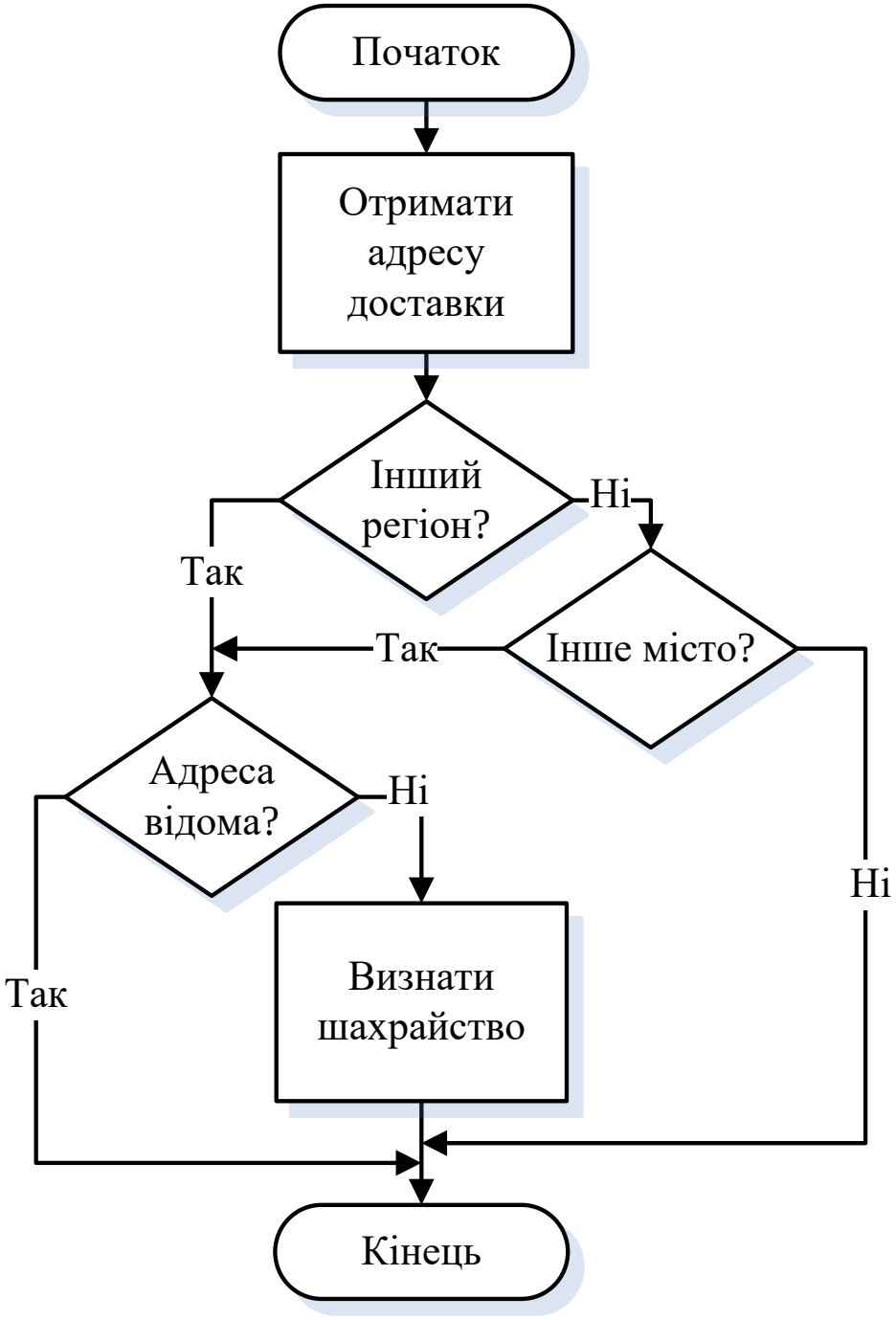


Рисунок 1.61 – Блок-схема алгоритму фільтрування за місцем знаходження та доставки

Робота даного фільтру (рисунок 1.61) полягає у порівнянні поточного регіону та міста, яке визначається за IP-адресом та місто, в яке замовлено доставку товару. У випадку різних значень додатково перевіряється, чи куплялися товари раніше на ту адресу. Якщо дана адреса вже була збережена у транзакціях клієнта, то операція не вважається шахрайською.

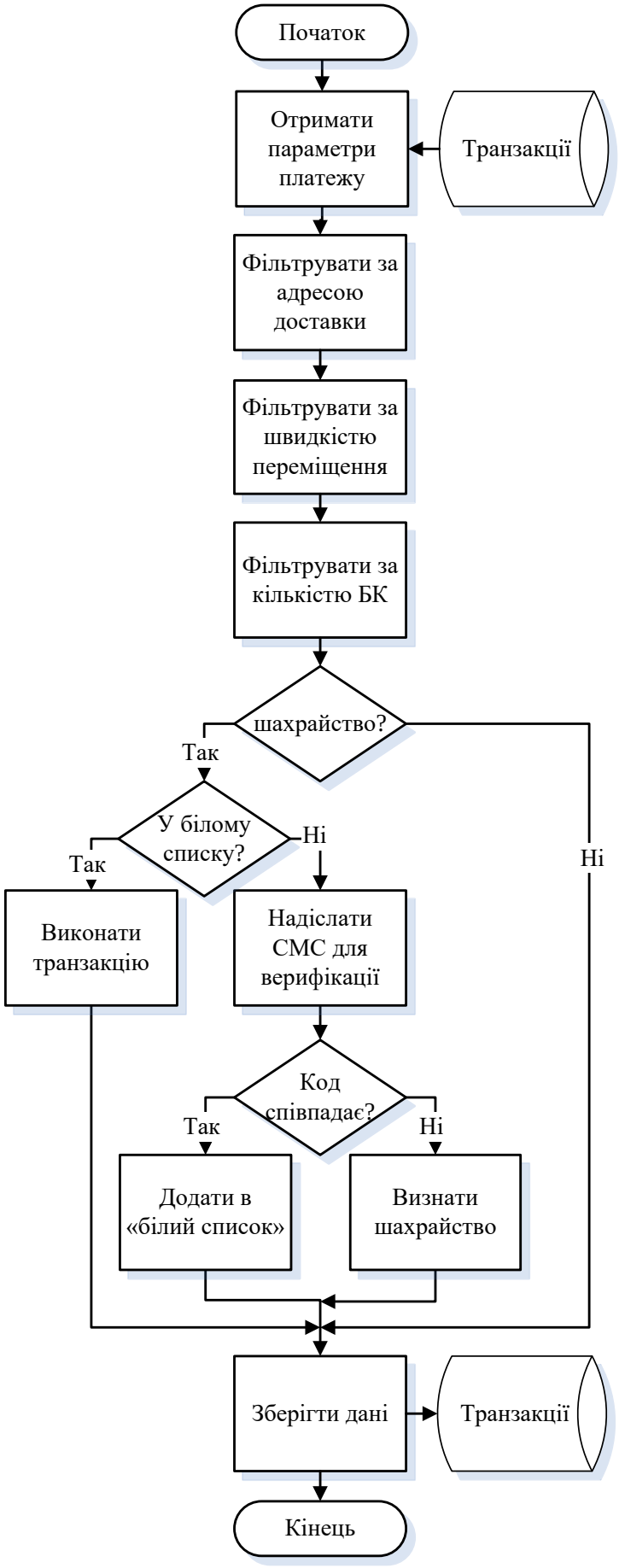


Рисунок 1.62 – Загальний вигляд алгоритму модулю виявлення шахрайства

На рисунку 1.62 зображено весь алгоритм за яким виконується процес виявлення шахрайських операцій – фільтрування платежу за 3 критеріями, верифікація у випадку необхідності та зберігання результатів в базі даних.

Автоматична система починається з форми онлайн-платежу, яку заповнює клієнт. Після цього методом POST дані відправляються до системи з фільтрами для виявлення шахрайських операцій. Кожен фільтр зберігає причину класифікації платежу як шахрайського, якщо вона є.

Для наочності наведемо частину програмного коду (Лістинг 1.1), який відповідає за аналіз часу та місцем знаходження клієнта між платежами:

Лістинг 1.1 – Фільтрація платежу за швидкістю переміщення клієнта

```
$time_dif = (strtotime("now")-strtotime($res['time'']))/3600;
$result = mysqli_fetch_assoc(mysqli_query($link,$sql));
$lat1 = $res['latitude'];
$long1 = $res['longitude'];
$lat2 = $result['latitude'];
$long2 = $result['longitude'];
$dist = calculateTheDistance($lat1, $long1, $lat2, $long2)/1000;
if($time_dif < $dist/50) {
    $fraudrisk=1;
    $fraud[] = "ошибка во времени";
}
```

Перший рядок розраховує скільки годин пройшло з моменту останнього платежу. Другий рядок повертає географічні координати поточного місцезнаходження. У рядках 3-4 записується у змінні координати місцезнаходження у момент останнього платежу, у рядках 4-6 – поточного місця. У 7 рядку викликається власна функція calculateTheDistance, яка розраховує відстань між містами у кілометрах. У 8 рядку перевіряється, чи достатньо було часу для проходження розрахованої відстані при швидкості у 50 кілометрів за годину. Якщо часу недостатньо, то записується, що платіж шахрайський (рядок 10) і його причину (рядок 11).

Як зазначено на рисунку 1.62, після виконання аналізу за допомогою 3 фільтрів, повертається результат про те, чи є операція шахрайською. Якщо

система класифікує її такою, то перевіряється достовірність клієнта – звіряються дані платежу з «білим списком» та відправляється клієнту СМС з кодом. Після введення отриманого коду у форму, платіж підтверджується і клієнт повертається до початкової сторінки оформлення платежу. Для зменшення надмірного відправлення СМС клієнтам з метою додаткової верифікації створюється «білий список». Він являє собою перелік унікальних банківських карт та IP-адрес, операції за якими спочатку були виявлені як шахрайські, але потім пройшли верифікацію. Він формується динамічно запитом до бази даних. Тому при повторному проведені платежу протягом 3 годин не потрібно буде заново підтверджувати особистість.

Після виконання алгоритму інформація зберігається в базі даних. Операції які позначені, або були позначені як шахрайські виводяться в додаток, який використовує співробітник банку.

Програмний код алгоритмічного забезпечення наведено в Додатку Б. У лістингу Б.1 продемонстровано програмний код, який виконує процес аналізу операції. В лістингу Б.2 записана функція, яка розраховує відстань між містами. Код з лістингу Б.3 використовується для збереження результатів.

Автоматизований модуль буде мати 2 частини, призначені для різних користувачів. Перша частина створена для клієнтів електронної комерції, які хочуть здійснити платіж за допомогою кредитної картки. У своєму браузері клієнт буде бачити форму, в якій йому необхідно заповнити дані про банківську картку та адресу доставки товару (рисунок 1.63). Всі поля, окрім квартири є обов’язковими для заповнення. Поля область та місто доставки є вибірковими, при цьому назва міст динамічно змінюються зі зміною області.

Після натискання кнопки виконується алгоритмічна частина додатку, в якій перевіряється чи є даний платіж шахрайським. Якщо у системи немає зауважень до цього платежу, то транзакція передається на виконання у платіжну систему, а клієнт повертається на початкову сторінку магазину електронної комерції.

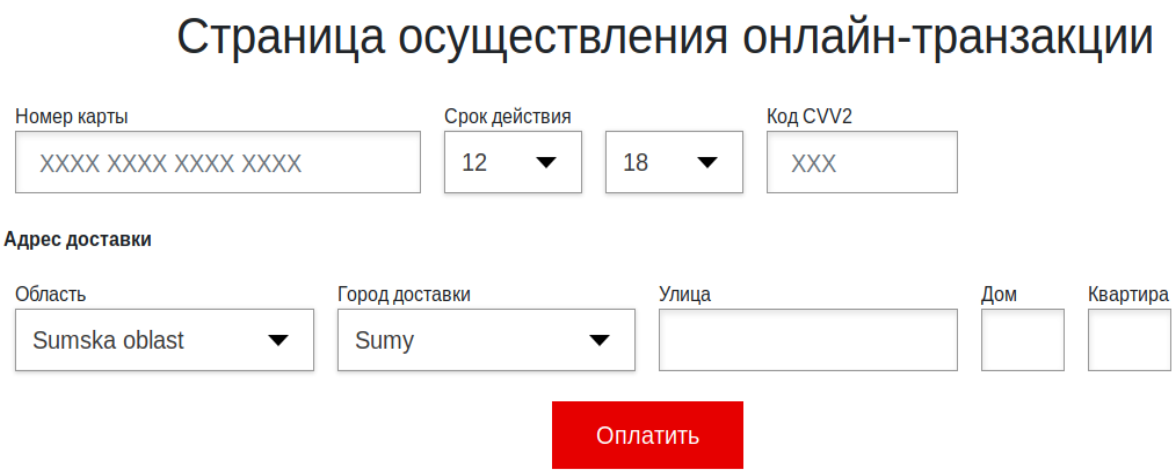


Рисунок 1.63 – Вікно здійснення онлайн-платежу

У випадку виявлення шахрайства виконання транзакції призупиняється і виконується запит до SMS API Service. На мобільний телефон клієнта приходить повідомлення із кодом (рисунок 1.64), який необхідно ввести у форму (рисунок 1.65). Після введення вірного коду платіж перестає вважатися шахрайським, транзакція виконуються і клієнт повертається на початкову сторінку. Код запиту до API для верифікації наведено в лістингу 4.2.

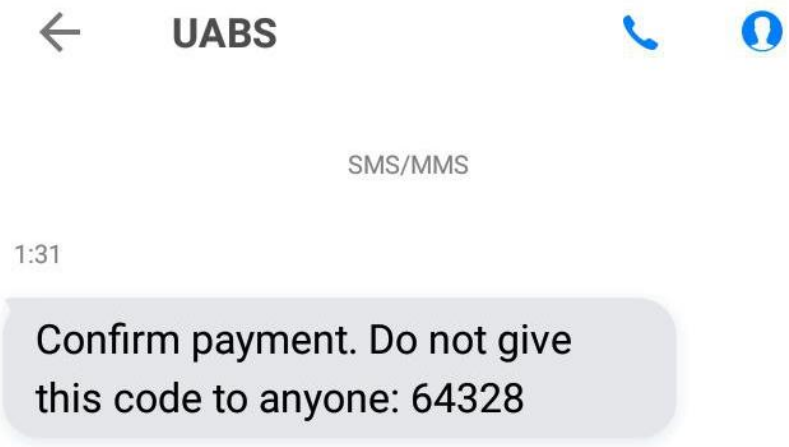


Рисунок 1.64 – СМС з кодом підтвердження

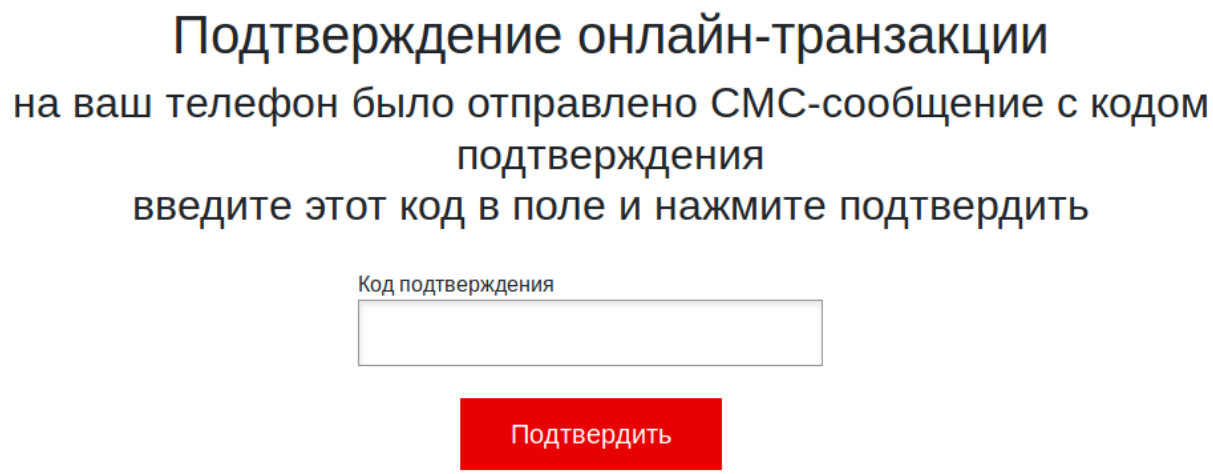


Рисунок 1.65 – Вікно підтвердження платежу

Лістинг 1.2 – Програмний код відправки коду підтвердження

```
$sql = "SELECT telephone FROM user
     INNER JOIN cards c ON c.userID = user.userID
     WHERE c.cardID = " . $cardID;
mysqli_query($link, $sql);
$result = mysqli_fetch_assoc(mysqli_query($link,$sql));
$apiKey = urlencode('cqrSX9lns-nVyN2k3Bfk8ihMXZYGsHSZMvKplNuP');
$numbers = array($result['telephone']);
$numbers = implode(',', $numbers);
$sender = urlencode('UABS');
$message = 'Confirm payment. Do not give this code to anyone: ' .
$code;
$data = array('apikey' => $apiKey, 'numbers' => $numbers, "sender"
=> $sender, "message" => $message, "unicode" => true, "test" =>
true);
$ch = curl_init('https://api.txtlocal.com/send/');
curl_setopt($ch, CURLOPT_POST, true);
curl_setopt($ch, CURLOPT_POSTFIELDS, $data);
curl_setopt($ch, CURLOPT_RETURNTRANSFER, true);
$response = curl_exec($ch);
curl_close($ch);
```

На цьому робота додатку з клієнтом магазину електронної комерції завершується. Друга частина додатку призначена для роботи співробітника банку. Він отримує перелік всіх платежів за участі свого банку, які були визначені як шахрайські операції (рисунок 1.66). Співробітник побачить прізвище та ім’я клієнта, картковий рахунок, телефон, дату проведення платежу, причину визначення його як шахрайського та поточний статус. Отриману інформацію можна фільтрувати по стовпцях. Крім того значення стовпців дати, номера телефону та підтвердження платежу може змінювати відразу в цьому вікні.

Результат работы модуля
операции, которые вызывают подозрения

#	Клиент	Карта	Дата и время	Причина отмены платежа	Операция мошенническая	Телефон
		5168	дд . мм . гггг	---	--	
1	Павлусик Андрей	5168739112345678	2018-10-31	новый город доставки	Нет	380669272071
2	Климов Сергей	5168757399128671	2018-11-19	ошибка во времени	Да	380957684065
3	Климов Сергей	5168757399128671	2018-11-20	разные регионы, ошибка во времени	Нет	380957684065
4	Павлусик Андрей	5168739112345678	2018-11-20	много карт по 1 IP	Да	380669272071
5	Павлусик Андрей	5168739112345678	2018-11-20	разные регионы	Нет	380669272071

Рисунок 1.66 – Вікно виведення шахрайських операцій

Програмний код створення кожної сторінки автоматизованого модуля наведено в Додатку В. В лістингу В.4 наведено код JavaScript, який використовується для роботи з даними у вікні виведених результатів.

Важливим для роботи є програмний код, що реалізує зміну інформації в таблиці веб-додатку у режимі реального часу. Наведемо його також в Додатках, в лістингу В.5

Автоматизований модуль може використовуватися на практиці в електронній комерції для зменшення кількості шахрайських замовлень. Він

також повинен бути інтегрований в інформаційну систему Інтернет-магазину та з’єднуватися з відповідним банком-еквайром.

До рекомендацій стосовно покращення автоматичної системи можна віднести її ускладнення новими функціональними можливостями. Для зменшення шахрайських операцій можна додати ще фільтри, які будуть перевіряти платежі. Проте це може призвести до зменшення конверсії. Тому важливим є налаштуванням системи під окремий вид електронної комерції. Якщо продається товар з низькою націнкою та великою собівартістю, то для погашення його втрати через шахрайство потрібно буде продати велику кількість товару. В цьому випадку необхідно максимально зменшити можливість шахрайських операцій. Якщо навпаки продається товар чи послуга, в ціну якої закладено більше 80% прибутків, то потрібно максимально збільшувати конверсію магазину. Серед можливих засобів фільтрації платежів я рекомендую реалізувати наступні:

– фільтрація за операційної системою та приладом, з якого відбувається платіж;

– фільтрація за сумою платежу (вартість покупки складає більше 90% заощаджень на рахунку);

– фільтрація по випадкам нестачі коштів;

– фільтрація за товарами.

Для удосконалення системи додатково рекомендується створити можливість для співробітника банку формувати звіти, зберігати та імпортувати їх.

Пункт 1.4.3 даного звіту було виконано із використанням матеріалів проміжного звіту про НДР [11], публікацій виконавців [18, 51], магістерської дипломної роботи [52].

2 ОРГАНІЗАЦІЯ СИСТЕМИ НЕЗАЛЕЖНОГО АУДИТУ ДЛЯ ПОПЕРЕДЖЕННЯ ШАХРАЙСТВ, ЯК ПРЕВЕНТИВНА СТРУКТУРА В СИСТЕМІ КІБЕРБЕЗПЕКИ БАНКУ

2.1 Моделювання бізнес-процесів служби аудиту банку

2.1.1 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) [53]. 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 [54].

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 [55].

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» [56]. 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 [57], О. Кірєєв [58], Л. Костирко [59], М. Маркевич [60], М. Письменна [61], О. Сарахман [62, 63], А. Арсланбеков-Федоров [64], С. Банк [65], Г. Бєлоглазова та інші [66], Н. Соколинська [67], А. Баракат (A. Barakat) [68], К. Россітер (C. Rossiter) [69] 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) [70], А. А. Боатенг, Г. О. Боатенг та Х. Акуа (A. A. Boateng, G. O. Boateng, H. Acquah) [71], С. Пальфі та М. Мурешан [72], Д. Петрашку та А. Тіану (D. Petraşcu and A. Tieanu) [73], Р. Саламе, Г. Аль-Вешах, М. Аль-Нсур та А. Аль-Хіяри (R. Salameh, G. Al-Weshah, M. Al-Nsour, A. Al-Hiyari) [74], М. Ула, З. Ісмаїл та З. М. Сідек (M. Ula, Z. Ismail, Z. M. Sidek) [75], А. К. Усман та М. Х. Шах (A. K. Usman and M. H. Shah) [76] 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 [77-81] 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 [82] 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. 2.1).

Таблиця 2.1 – 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 [83, 84].

Перелік способів реалізації загроз кібербезпеки банку, на яких має концентруватись аудит, наведено в таблиці 2.2.

Таблиця 2.2 – 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.

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 [85], 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 2.1.

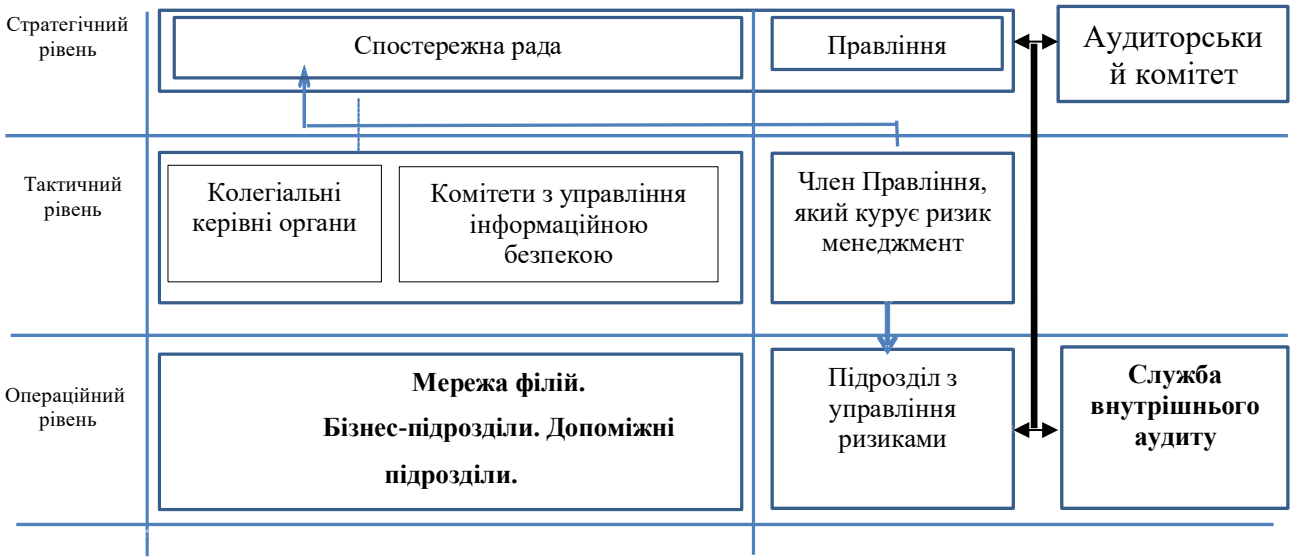


Рисунок 2.1 – Організаційно-управлінська підсистема забезпечення кібербезпеки банку

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 [53, 72, 82, 86, 87]:

– 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 [53, 72, 82, 86, 87].

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 2.2.

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 [88].

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;

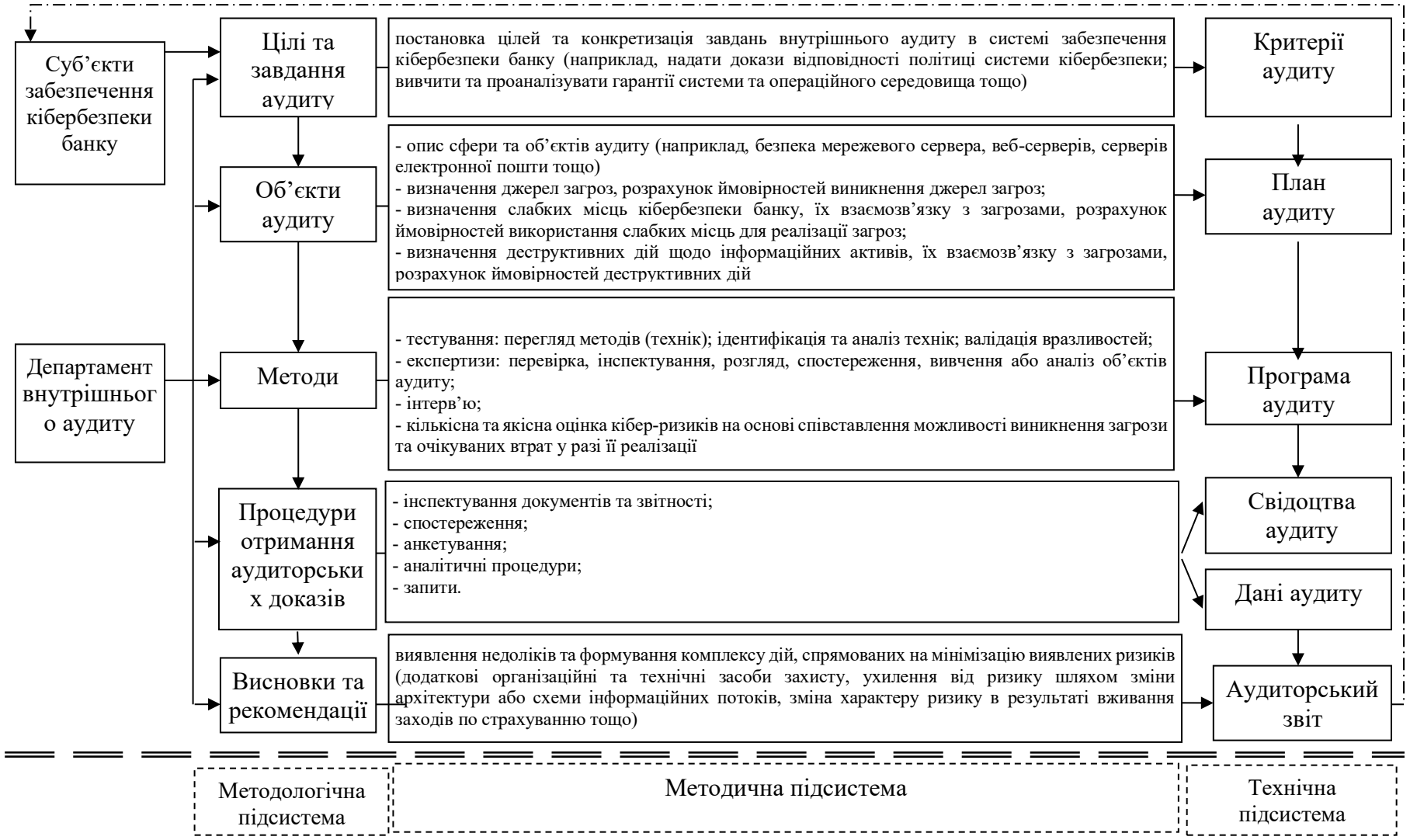


Рисунок 2.2 – Механізм внутрішнього аудиту в системі забезпечення кібербезпеки банку [53, 88, 90, 91]

– 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 [86, 87, 89, 90, 91].

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.

Пункт 2.1.1 даного звіту було виконано із використанням матеріалів проміжного звіту про НДР [92], публікацій виконавців [93, 94, 95, 96].

2.1.2 Дослідження особливостей незалежного аудиту для попередження шахрайства банківського персоналу

Згідно зі звітом Асоціації сертифікованих фахівців із розслідування шахрайства [97], 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 [98]. 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 [99].

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 [100]. Як зазначено в роботі [101], 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 [102] 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» [103], 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 [104].

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 [105], 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» [106]. 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 [107]. Метою фрод-моніторингу в банку згідно [101] 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 [108] 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 [97]. Як зазначено в роботі [107], 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 [105]:

– 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 2.3, найбільше збитків у світі в 2018 році було заподіяно через такі типи шахрайства персоналу [97]: неправдиве відображення фінансової звітності (10% випадків), корупція (38% випадків), незаконне привласнення активів (89% випадків).

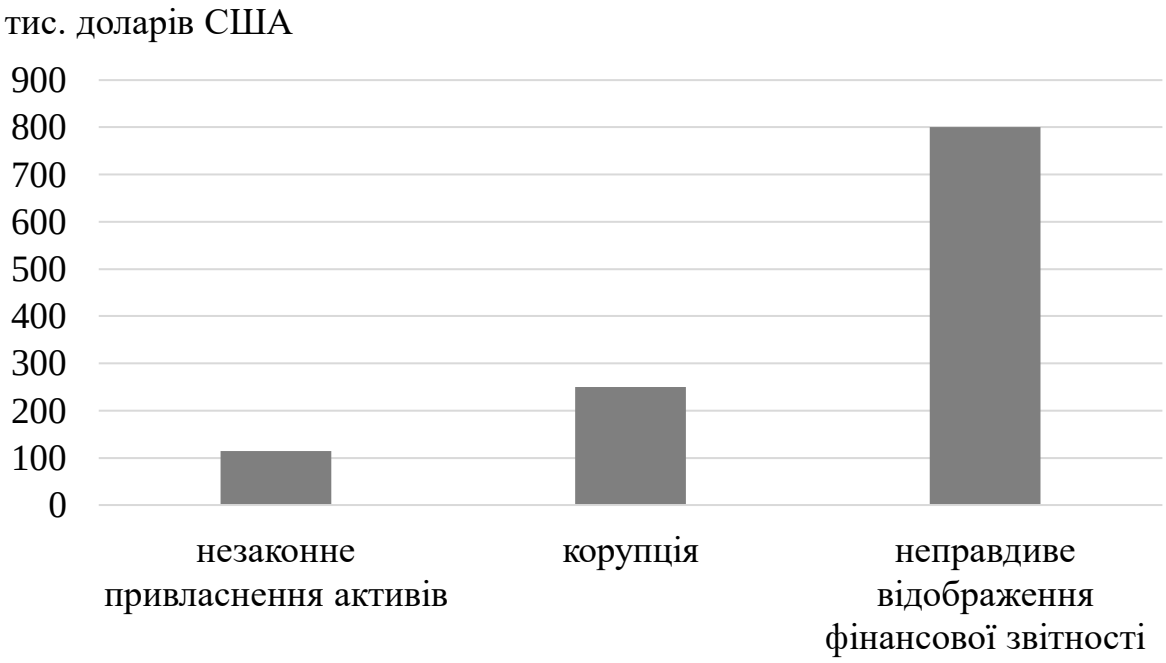


Рисунок 2.3 – Медіана фінансових збитків за типами шахрайства персоналу

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 [109] представлена нечітко-множинна модель, побудована на основі індикаторів ризику шахрайства персоналу, наведених, наприклад, в [110], 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 [111]:

– 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 [106]. 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 [112] 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 [109]. 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 [112].

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 [112] 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 [113] 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 [113] 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 [114] 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 [115] 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 2.3. Оптимальними для врахування невизначеності та виявлення шахрайств у банках є гібридні методи, що використовують сильні сторони різних підходів.

Таблиця 2.3 – 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

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.

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.

Пункт 2.1.2 даного звіту було виконано із використанням матеріалів проміжного звіту про НДР [92], публікацій виконавців [116, 117].

2.1.3 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 [118, 119, 120, 121, 122].

Окрема група науковців Іващенко Г.А., Кавун С.В., Прокопішина О. В. [123, 124, 125] 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. [126, 118, 122].

Дослідженню проблеми фінансового моніторингу присвячено праці наступних вчених Новак О.С., Дмитров С.О., Кузьменко О.В., Куришко О.О., Петрук О.М. та багато інших [127, 128, 129, 130]. 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. [131, 132, 133].

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 [118, 119, 121]. 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 [118, 121]. 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 [118, 122, 126].

Разом з тим, зазначимо, що сучасній глобальній економіці [118, 121] 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 [118, 121].

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 [121, 126, 134].

Більш вузьке поняття, що допомагає забезпечувати національну економічну безпеку, є економічна небезпека регіонів [118] 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 [123, 124, 125], 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 [120, 123, 124, 125]. 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 [123]. 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 [123, 125, 134].

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 [118, 122]:

– 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 [126]:

– 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) [119].

Особливої уваги потребують інструменти забезпечення фінансової безпеки, що безпосередньо пов'язані з регулюванням процесів фінансового моніторингу [119]:

– 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 [127, 128, 129]. 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 [130, 128, 133]. 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 [128, 133]. 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 [129, 131, 132].

В національній економічній системі нашої країни створена та функціонує Державна служба фінансового моніторингу України [122, 128] (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.

Пункт 2.1.3 даного звіту було виконано із використанням матеріалів проміжного звіту про НДР [92], публікацій виконавців [135].

2.2 Розробка алгоритмів виявлення та попередження шахрайств в банках, які здійснюються із зовнішніх джерел

2.2.1 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 [136].

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 [137].

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 [138]. 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 2.4 показано 5 напрямків бізнесу, які понесли найбільші витрати через кібершахрайства у серпні 2018 року. З рисунка 2.4 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.

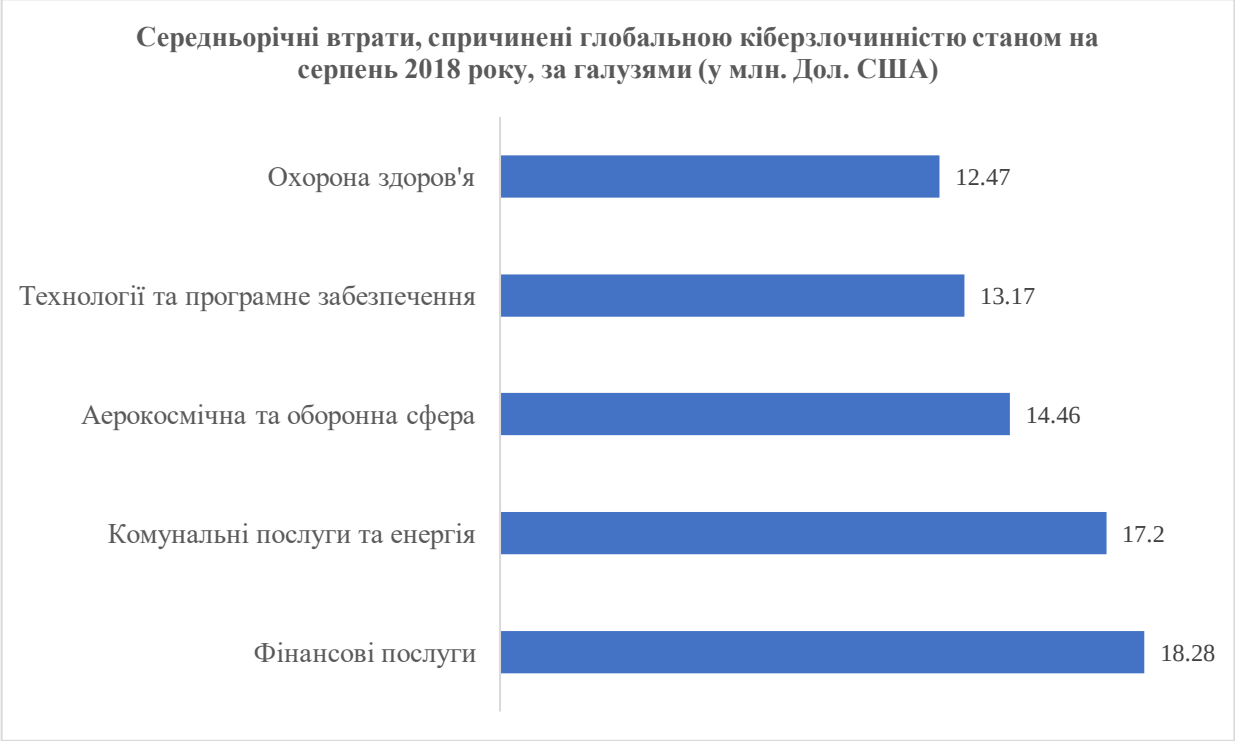


Рисунок 2.4 – Середньорічні витрати, спричинені глобальною кіберзлочинністю станом на серпень 2018 року, за галузями (у млн. дол. США) [139]

Найпоширенішим видом шахрайства в секторі електронного банкінгу є фішинг та його підвиди (рис. 2.5).

Як правило, фішинг можна визначити як масштабований акт обману, за допомогою якого оманливість використовується для отримання інформації від цілі [140]. 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 [141].

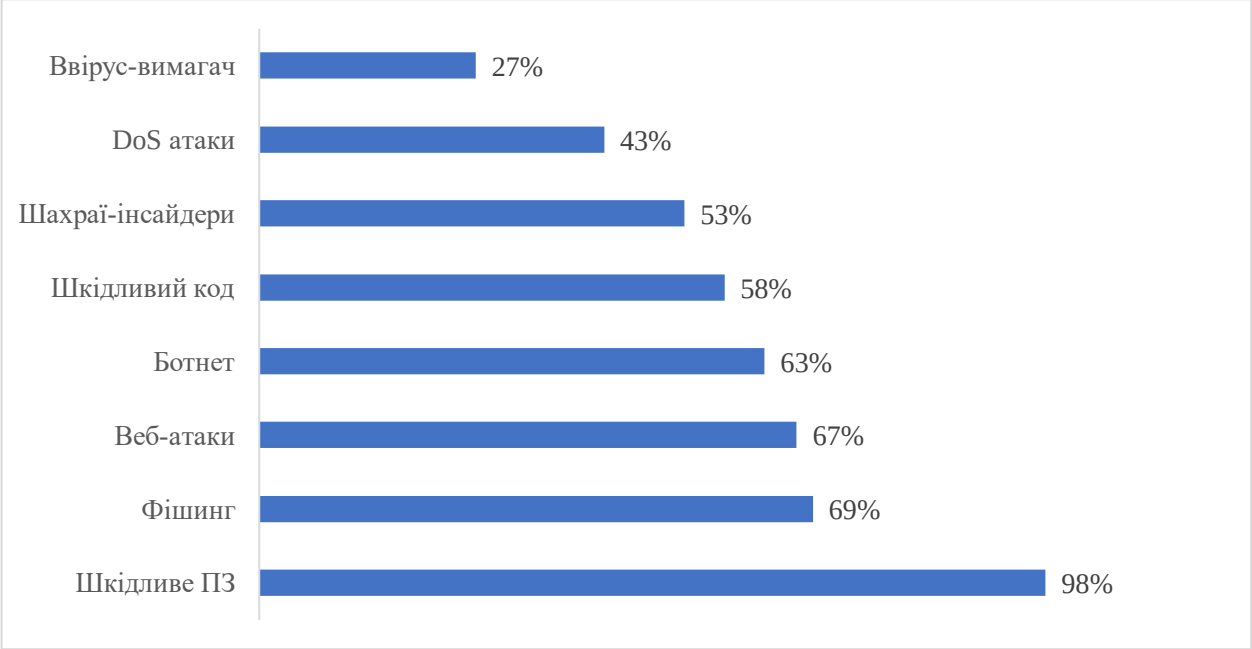


Рисунок 2.5 – Типи кібератак, які зазнавали компанії у всьому світі станом на серпень 2018 року [139]

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 [142]. Потік інформації показаний на рис. 2.6.

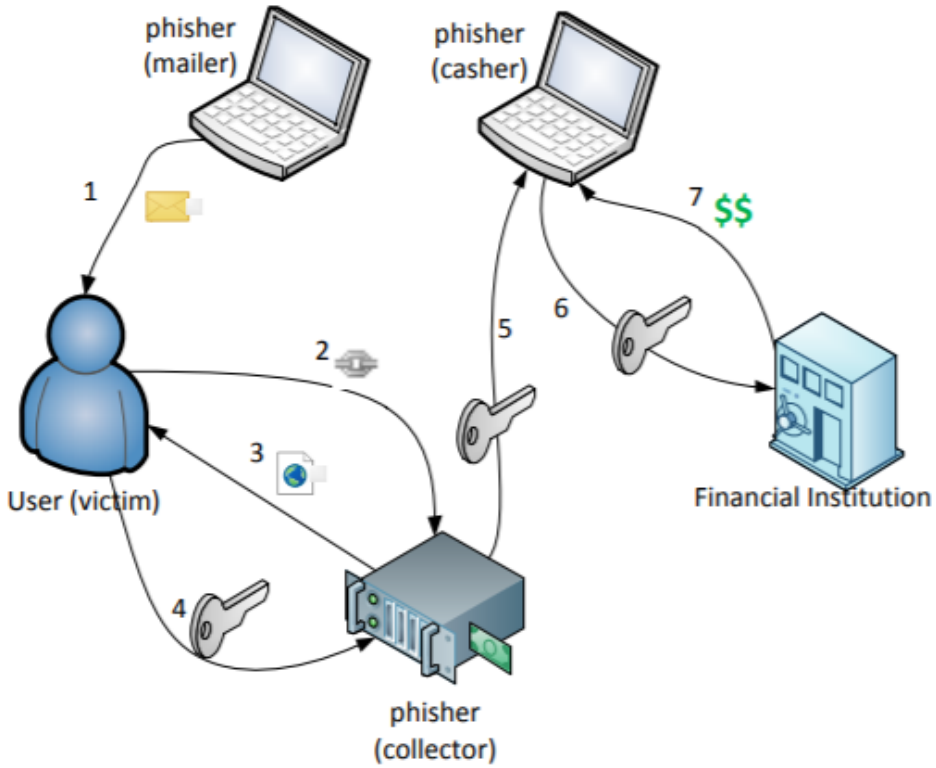


Рисунок 2.6 – Інформаційний потік при фішингу [142]

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 [143];

– оманлива фішинг-атака – надсилання шахрайських повідомлень електронною поштою [144]. Під час такого типу фішинг-атаки, зловмисник

надсилає електронним повідомленням користувачам, маскуючись як один із представників банку [145].

– 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 [142]. 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 [146]. 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 [142].

Аналіз статистики щодо загальної кількості фішинг-атак у всьому світі показує, що їх кількість поступово збільшується (рис. 2.7).

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.

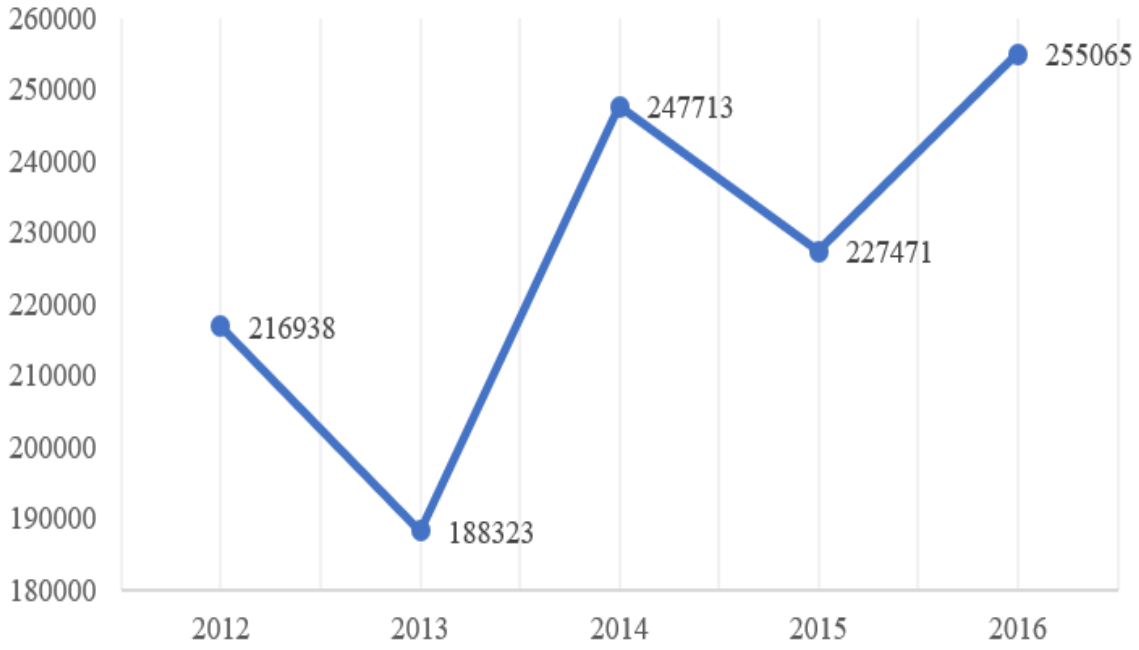


Рисунок 2.7 – Кількість глобальних фішинг-атак з 2012 по 2016 рік у всьому світі [140]

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. Використання інструментів для боротьби з кібератаками та появу нових атак можна порівняти з класичною моделлю «хижак-жертва» (формула 2.1) [143]:

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

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 [147] і моделі Холлінга-Таннера [148] дозволяє запропонувати модель протидії банківським кібератакам (формула 2.2):

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

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 (формули 2.3 – 2.4):

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

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

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 (формула 2.5):

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

Замінюємо *x* і *y* в якобіані значенням другої особливої точки і обчислюємо слід і детермінант для отриманої матриці Якобі (формули 2.6 – 2.7).

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

$$\Delta = a + a \cdot c - 1. \quad (2.7)$$

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

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

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. 2.4).

Таблиця 2.4 – Типи особливої точки залежно від співвідношення вхідних параметрів моделі

Тип особливої точки	Співвідношення вхідних параметрів
Стійкий вузол	$a + a \cdot c - 1 > 0$ $\sqrt{D}/_2 \neq 0$
Стійкий вироджений вузол	$a + a \cdot c - 1 > 0$ $\sqrt{D}/_2 = 0$
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. 2.8).

Структура побудованої моделі представлена в табл. 2.5.

Таблиця 2.5 – 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

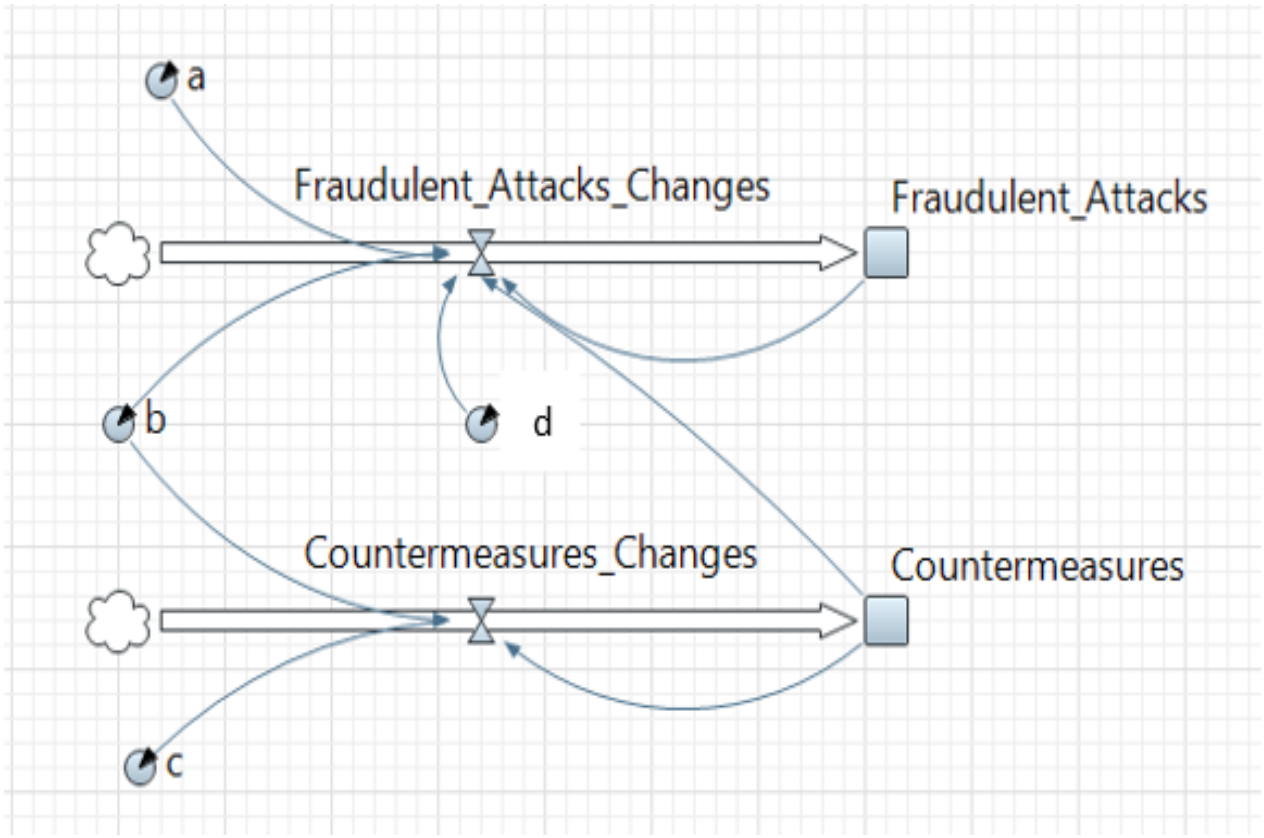


Рисунок 2.8 – Діаграма «потік-дані» для моделі процесу протидії кібершахрайствам в електронному банкінгу

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 межах 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.

Пункт 2.2.1 даного звіту було виконано із використанням матеріалів проміжного звіту про НДР [92], публікацій виконавців [149].

2.2.2 Нечітко-множинна модель оцінки рівня ризику шахрайства банківського персоналу

Банківські втрати через шахрайства становлять приблизно 70 млрд. доларів щорічно, 70 % яких реалізуються за участі банківського персоналу [150], 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 [151] 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 [152] в роботі [151] 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 [151] 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 [153, с. 223].

Модель оцінювання рівня ризику шахрайства банківського персоналу пропонується представити у вигляді представленого на рис. 2.9 деревоподібного графа з двома рівнями ієрархії, побудованого на основі опрацювання [154].

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.

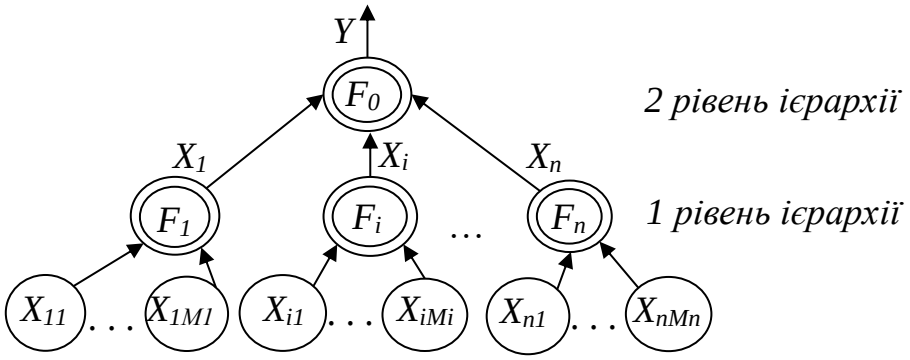


Рисунок 2.9 – Ієрархічна структура моделі оцінювання рівня ризику шахрайства банківського персоналу

Елементи деревоподібного графа (рис. 2.9) 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. 2.9, із пересуванням від нижніх рівнів ієрархії до верхніх. Рівень ризику шахрайства банківського персоналу в цілому опишемо наступною нечіткою ієрархічною моделлю:

$$Y=<G, L, S, F>, \tag{2.9}$$

де G – ієрархічний граф, показаний на рис. 2.9;

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. 2.10.

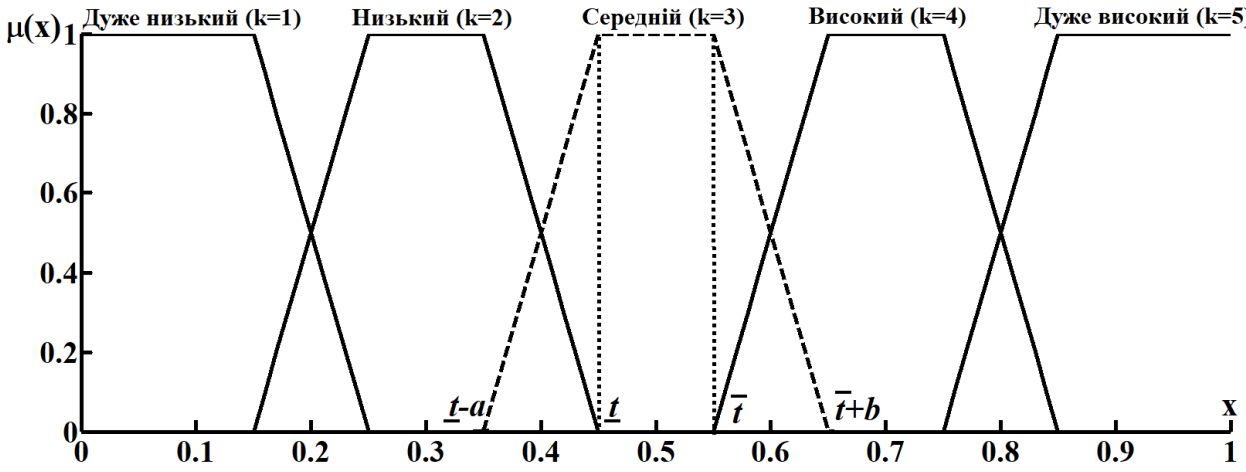


Рисунок 2.10 – Нечітка терм-множина

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

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 2.11 – 2.15 [154]:

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

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

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

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

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

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. 2.10). 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 “1” [154].

Агрегування нечітких оцінок лінгвістичних змінних здійснюється за рівнями ієрархії з пересуванням від нижніх рівнів графа *G* (рис. 2.9) 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 [154, 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 2.16-2.18:

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

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

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

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 [154, с. 37] або матриці парних порівнянь [155]. 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 [151]. 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. 2.6-2.8.

Таблиця 2.6 – 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 операцій при одночасному звітуванні про прибутки та зростання доходів	0,205	
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 / нормативні вимоги.	0,052	

Продовження таблиці 2.6

№	Індикатор фактору ризику	Нормалізована вага індикатора	Рівень присутності індикатора ризику
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 2.7 – 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	0,141	

Продовження таблиці 2.7

№	Індикатор фактору ризику	Нормалізована вага індикатора	Рівень присутності індикатора ризику
	умови клієнтам, що може призвести до шахрайських операцій		
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	
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 ІТ-персоналу	0,333	
2.4.3	Неефективний облік і інформаційні системи, включаючи ситуації, які стосуються умов, що підлягають звітуванню	0,333	

Таблиця 2.8 – 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	
3.1.9	Часті суперечки з поточним (попереднім) аудитором з питань бухгалтерського обліку, аудиту або звітності	0,074	
3.1.10	Невиправдані вимоги до аудитора, такі як необґрунтовані 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, здатність аудитора ефективно спілкуватися з керівництвом	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. 2.9.

Таблиця 2.9 – 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 2.9. Інтерпретація рівнів кількісної оцінки ризику шахрайства персоналу по категоріях здійснена за формулами (2.11)-(2.15). Результати наведені в табл. 2.10.

Таблиця 2.10 – 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 здійснено за формулами (2.11)-(2.18) з використанням інформації, наведеної в таблиці 2.9. Інтерпретація рівнів кількісної оцінки ризику шахрайства персоналу здійснена за формулами (2.11)-(2.15). Результати наведені в табл. 2.11.

Таблиця 2.11 – 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 2.9-2.11 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.

Пункт 2.2.2 даного звіту було виконано із використанням матеріалів проміжного звіту про НДР [92], публікацій виконавців [156, 157, 158].

2.2.3 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 [159] 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) [160]; по даним Організації економічного співробітництва та розвитку - банківська таємниця [161]; з сайту організації Transparency International – індекс сприйняття корупції [162]; з матеріалів досліджень Інституту економіки та миру – глобальний індекс тероризму [108]; з розрахунків Happy Planet Index – світовий індекс щастя [163].

Обґрунтування доцільності включення зазначеного набору індикаторів обумовлене результатами дослідження колінеарності шляхом застосування сигма-обмеженої параметризації (рисунок 2.11) та кореляційного аналізу залежності як регресанда від кожного із індикаторів регресорів, так і факторів між собою (рисунок 2.12). 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.

Аналіз рисунку 2.11 (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.

	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, etc. (	0,8784	1,1384	0,1216	-0,1513	-0,1946	-0,1418	-1,9443	0,0548
Internally displaced persons, new di	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 2.11 – Статистика колінеарності індикаторів статистичної бази дослідження

	Кореляції векторів в матриці плану X Кореляц. матриця для векторів в матриці плану X							
Ефект	GDP per capita (current LCU)	Bank Secrece	Claims on central government, etc. (% GDP)	Internally displaced persons, new displacement associated with conflict and violence (number of cases)	Corruption Perceptions Index	Global Terrorism Index	Happy Planet Index	Risk of money laundering
GDP per capita (current LCU)	1,0000	0,1107	-0,1179	0,0328	-0,0907	0,0864	-0,0144	0,0521
Bank Secrece	0,1107	1,0000	0,2919	-0,2555	0,6115	-0,1009	0,5837	-0,3687
Claims on central government, etc. (%	-0,1179	0,2919	1,0000	-0,1131	0,1342	-0,0085	0,1775	-0,2060
Internally displaced persons, new dis	0,0328	-0,2555	-0,1131	1,0000	-0,2423	0,4847	-0,2154	-0,0064
Corruption Perceptions Index	-0,0907	0,6115	0,1342	-0,2423	1,0000	-0,2598	0,7165	-0,6466
Global Terrorism Index	0,0864	-0,1009	-0,0085	0,4847	-0,2598	1,0000	-0,2005	0,1580
Happy Planet Index	-0,0144	0,5837	0,1775	-0,2154	0,7165	-0,2005	1,0000	-0,5454
Risk of money laundering	0,0521	-0,3687	-0,2060	-0,0064	-0,6466	0,1580	-0,5454	1,0000

Рисунок 2.12 – 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 2.12) 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 [165]:

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

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 [166, 167]:

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

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 [168]:

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):

$$V_{k+1} = V_k - \frac{V_k \cdot s \cdot s^T \cdot V_k}{s^T \cdot V_k \cdot s} + \frac{r \cdot r^T}{s^T \cdot s}, \qquad r = \Delta g_k = g_k - g_{k-1} \tag{2.21}$$

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

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 2.13).

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

Аналіз рисунку 2.13 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 «Продуктивність 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 2.14), 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 ID	Ваги З'єднання 1.MLP 7-6-1	Значення ваг 1.MLP 7-6-1
1	GDP per capita (current LCU) --> прихований нейрон 1	0,24229
2	Bank Secrece --> прихований нейрон 1	-3,56386
3	Claims on central government, etc. (% GDP) --> прихований нейрон 1	-0,35591
4	Internally displaced persons, new displacement associated with conflict and violence (number of cases) --> прихований нейрон 1	0,76272
5	Corruption Perceptions Index --> прихований нейрон 1	-3,36003
6	Global Terrorism Index --> прихований нейрон 1	2,85833
7	Happy Planet Index --> прихований нейрон 1	-1,90713
8	GDP per capita (current LCU) --> прихований нейрон 2	0,09608
9	Bank Secrece --> прихований нейрон 2	-1,74837
10	Claims on central government, etc. (% GDP) --> прихований нейрон 2	0,01076
11	Internally displaced persons, new displacement associated with conflict and violence (number of cases) --> прихований нейрон 2	-0,26839
12	Corruption Perceptions Index --> прихований нейрон 2	-3,03234
13	Global Terrorism Index --> прихований нейрон 2	0,88732
14	Happy Planet Index --> прихований нейрон 2	-2,69782
15	GDP per capita (current LCU) -->прихований нейрон 3	0,14886
16	Bank Secrece --> прихований нейрон 3	-1,73532
17	Claims on central government, etc. (% GDP) --> прихований нейрон 3	-0,10462
18	Internally displaced persons, new displacement associated with conflict and violence (number of cases) --> прихований нейрон 3	-0,58360

Рисунок 2.14 – 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 2.15. 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).

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 2.16 – 2.19).

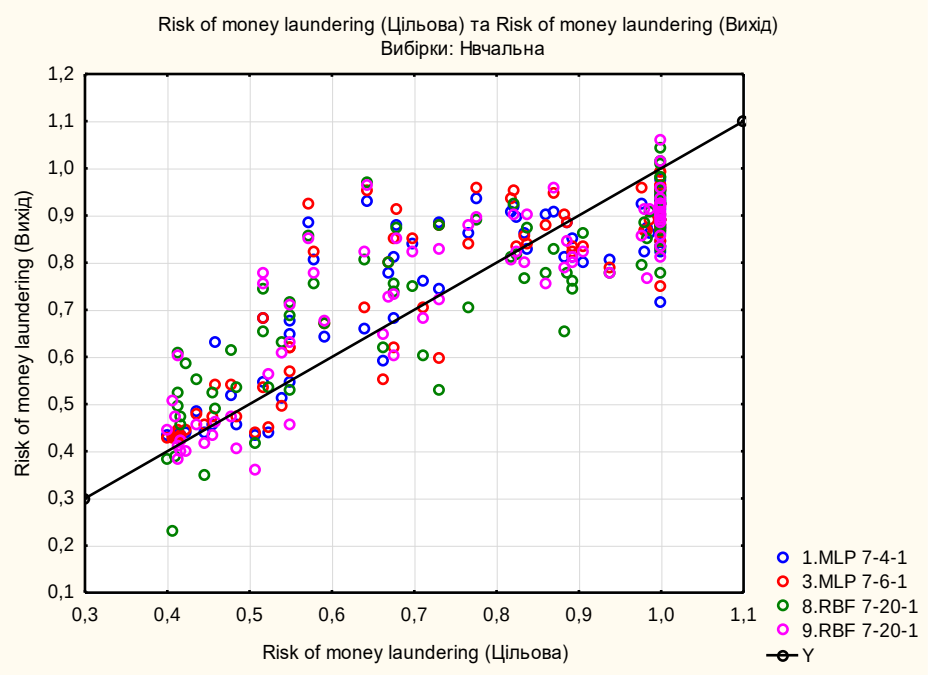


Рисунок 2.15 – Співвідношення фактичних та прогнозних рівнів ризику використання фінансових посередників з метою легалізації кримінальних доходів

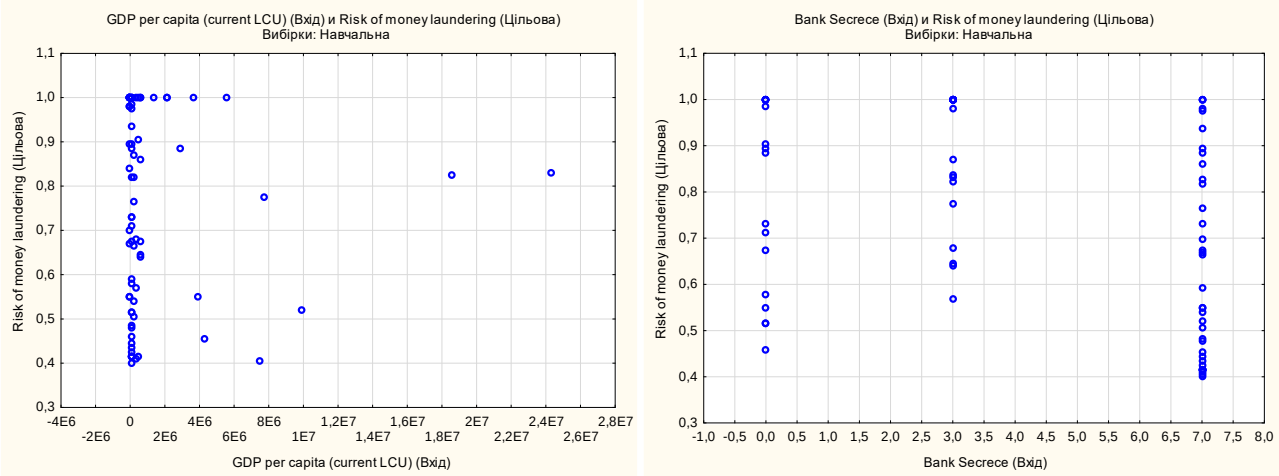


Рисунок 2.16 – Діаграми розсіювання факторів ризику: валовий внутрішній продукт на душу населення, банківська таємниця

Аналіз попарної залежності результативної ознаки від валового внутрішнього продукту на душу населення та банківської таємниці свідчить про (рисунок 2.16): 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 2.17) 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.

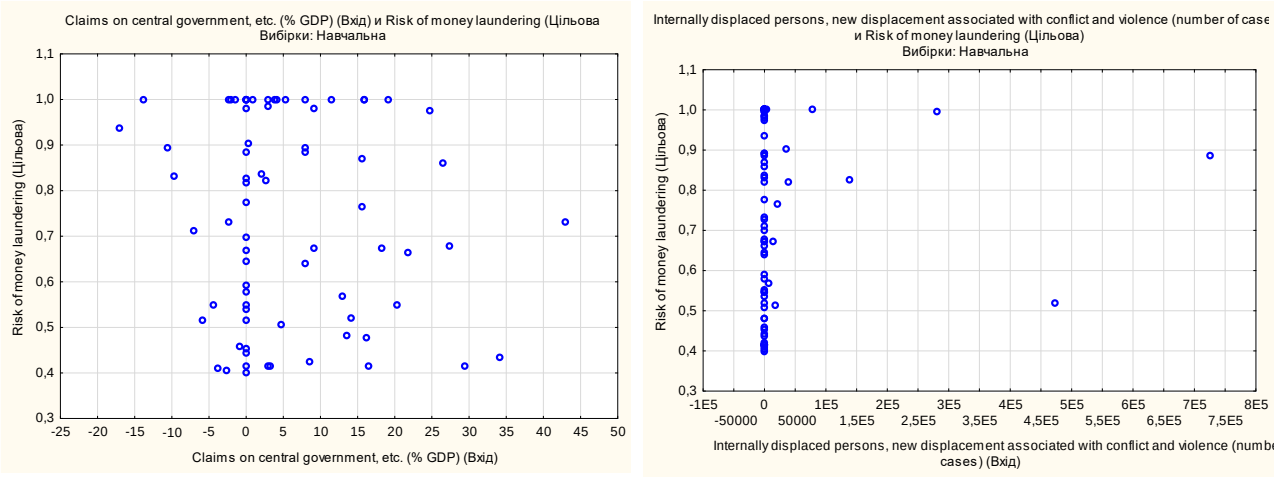


Рисунок 2.17 - Діаграми розсіювання ризику: позови до центрального уряду, внутрішньо переміщені особи, нові переміщення, пов'язані з конфліктом та насильством (кількість випадків)

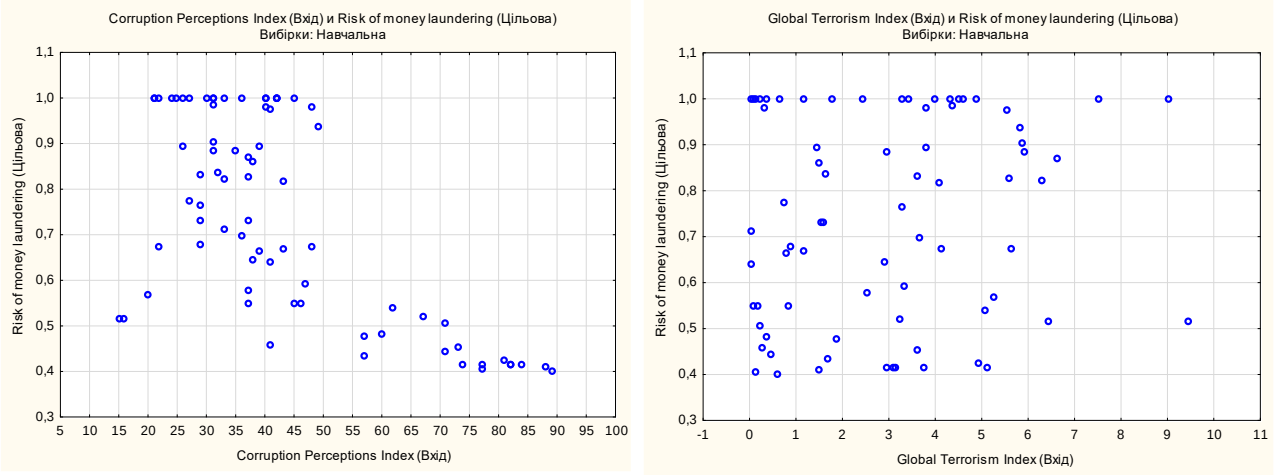


Рисунок 2.18 - Діаграми розсіювання факторів ризику: індекс сприйняття корупції, глобальний індекс тероризму

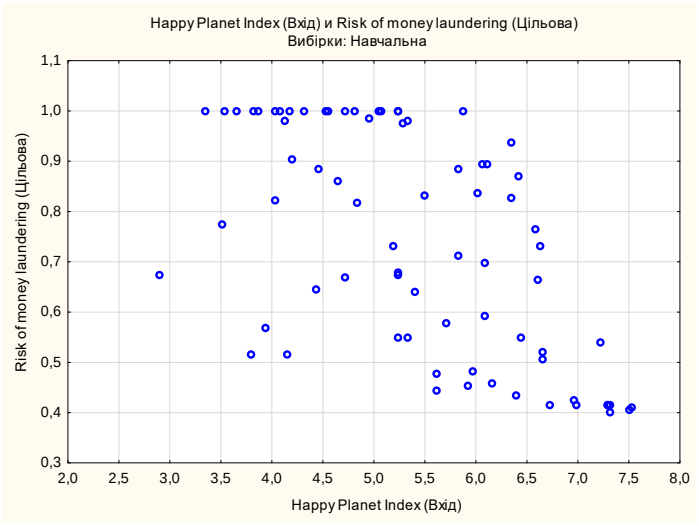


Рисунок 2.19 - Діаграми розсіювання факторів ризику використання фінансових посередників з метою легалізації кримінальних доходів: світовий індекс щастя

Переходячи до дослідження впливу індексу сприйняття корупції (рисунок 2.18) та світового індексу щастя (рисунок 2.19) 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 2.20) та чутливість моделей обраних нейронних мереж в розрізі вхідних предикторів (рисунок 2.21).

	Статистики передбачених значень Цільова: Risk of money laundering			
Статистики	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 2.20 – Статистики передбачених значень

	Чутливість Вибірки: Навчальна						
Мережі	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 2.21 – Чутливість моделей обраних нейронних мереж в розрізі вхідних предикторів

Аналіз статистичних характеристик моделей нейронних мереж, представлених на рисунках 2.20 і 2.21, 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 2.12.

Таблиця 2.12 – 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 2.22, 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 laundering_(t)	GDP per capita (current LCU)	Bank Secrece	Claims on central government, etc. (% GDP)	Internally displaced persons, new displacement associated with conflict and violence (number of cases)	Corruption Perceptions Index	Global Terrorism Index	Happy Planet Index
1	0,446689	0,319165	0,604537	,776998	105238,0	3,000000	19,00000	9600,000	28,00000	28,00000	4,650000
2	0,917014	0,961509	0,889420	,901665	105237,8	3,000000	18,98612	9600,000	28,00000	5,50000	4,650000
3	0,918919	0,960774	0,903671	,909302	136809,2	3,000000	17,08751	8640,000	22,00000	4,50000	4,710000
4	0,933354	0,963849	0,910519	,958199	177851,9	3,000000	15,37876	8208,000	17,00000	3,50000	5,950000
5	0,930361	0,965438	0,942622	,918919	222314,9	3,000000	13,07194	7961,760	13,00000	2,50000	5,110000

Рисунок 2.22 – 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.

Пункт 2.2.3 даного звіту було виконано із використанням матеріалів проміжного звіту про НДР [92], публікацій виконавців [169, 170, 171].

2.3 Розробка алгоритмів виявлення та попередження шахрайств в банках, що здійснюються персоналом банку

2.3.1 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 2.23). 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;

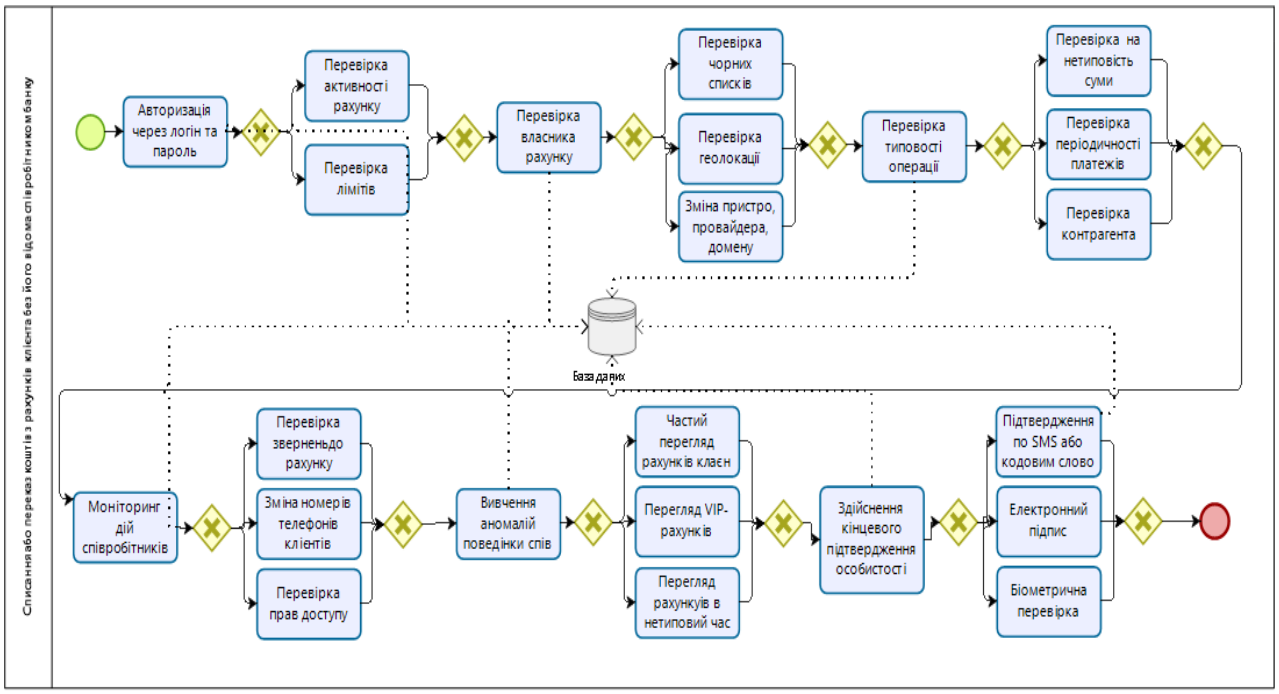


Рисунок 2.23 – Модель бізнес-процесу перевірки операцій працівників щодо здійснення ними шахрайств стосовно клієнтських рахунків

- його геолокація, провайдер, домен, адже різка зміна цих даних може сигналізувати про шахрайство;
- 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 2.24).

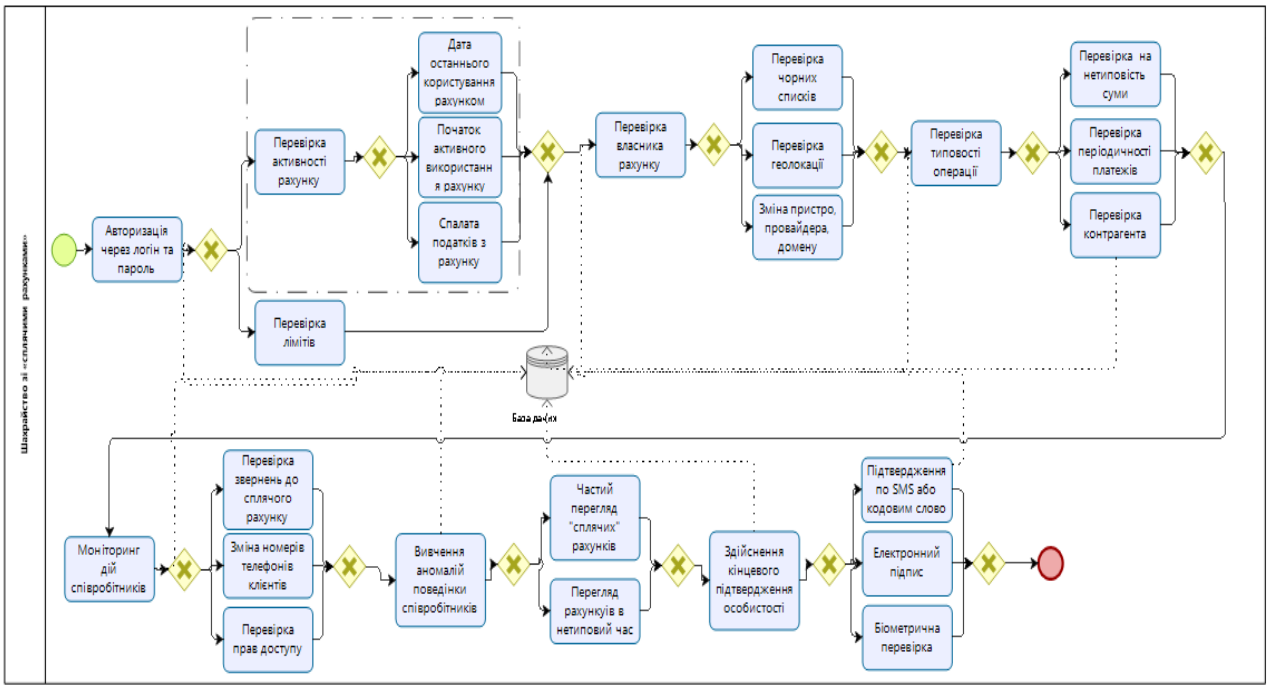


Рисунок 2.24 – Модель бізнес-процесу перевірки операцій працівників щодо здійснення ними шахрайств по відношенню до «сплячих рахунків»

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 2.25).

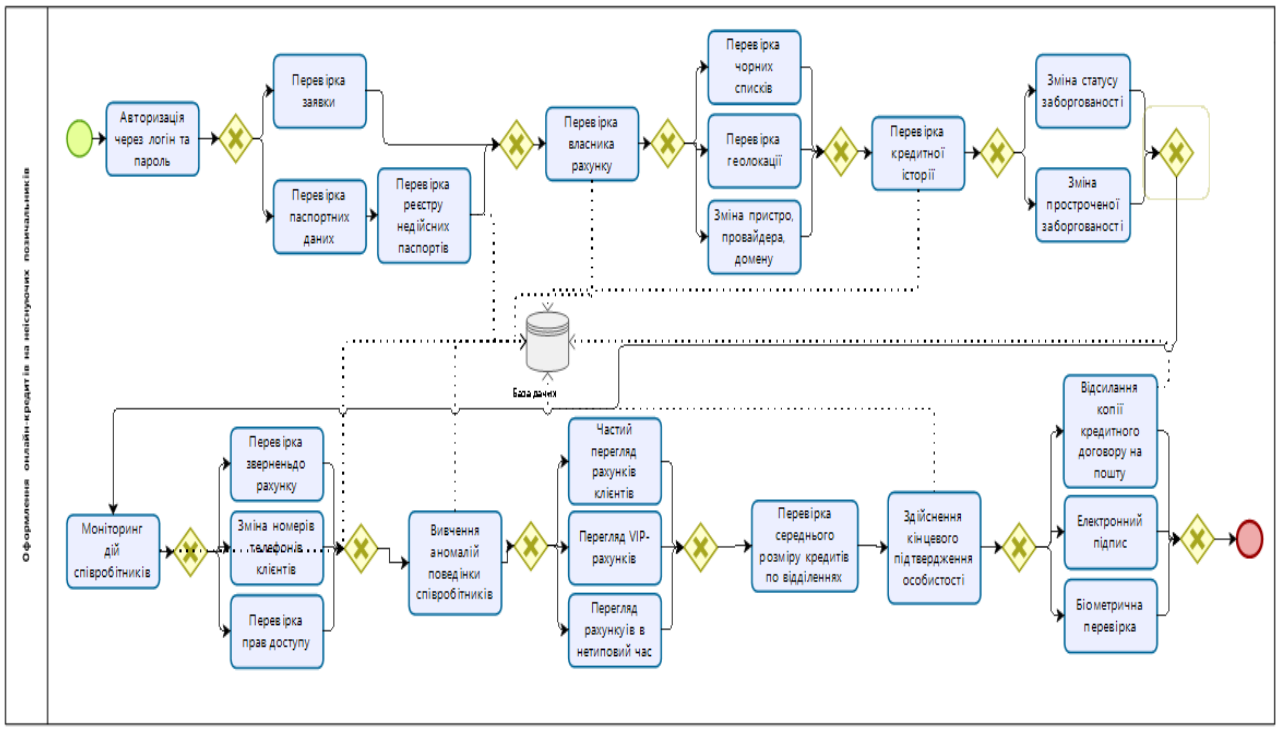


Рисунок 2.25 – Модель бізнес-процесу перевірки операцій працівників щодо здійснення ними шахрайств стосовно оформлення онлайн-кредитів на неіснуючих позичальників

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.

Пункт 2.3.1 даного звіту було виконано із використанням матеріалів проміжного звіту про НДР [92], публікацій виконавців [172].

2.3.2 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 [173]. 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 [174] та програмного забезпечення Bizagi Studio [175] (рис. 2.26.).

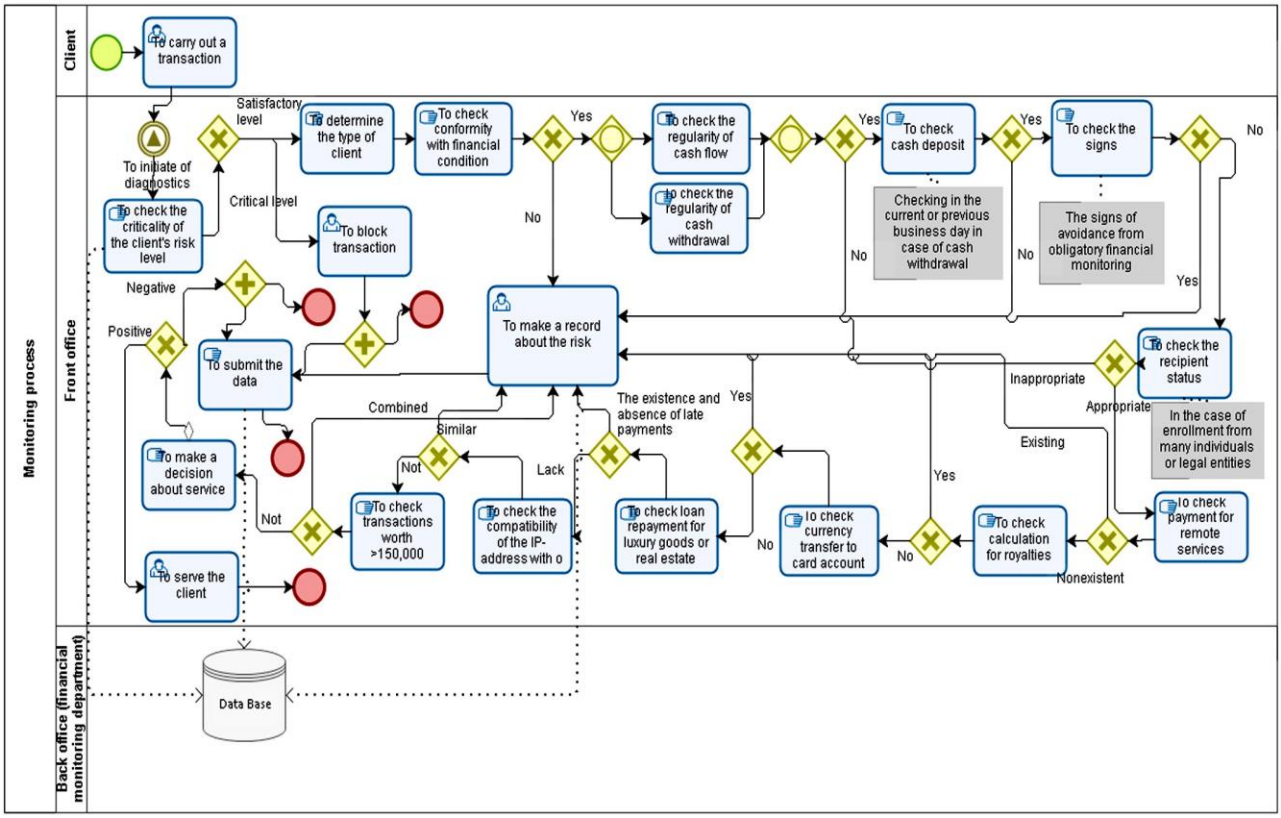


Рисунок 2.26 – Діаграма існуючого бізнес-процесу внутрішньобанківського моніторингу

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 їх зняття;

– 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 рисунку 2.27 представлена схема вдосконаленого бізнес-процесу фінансового моніторингу, яка була розроблена за допомогою нотації BPMN 2.0 [174] та програмного забезпечення Bizagi Studio [175].

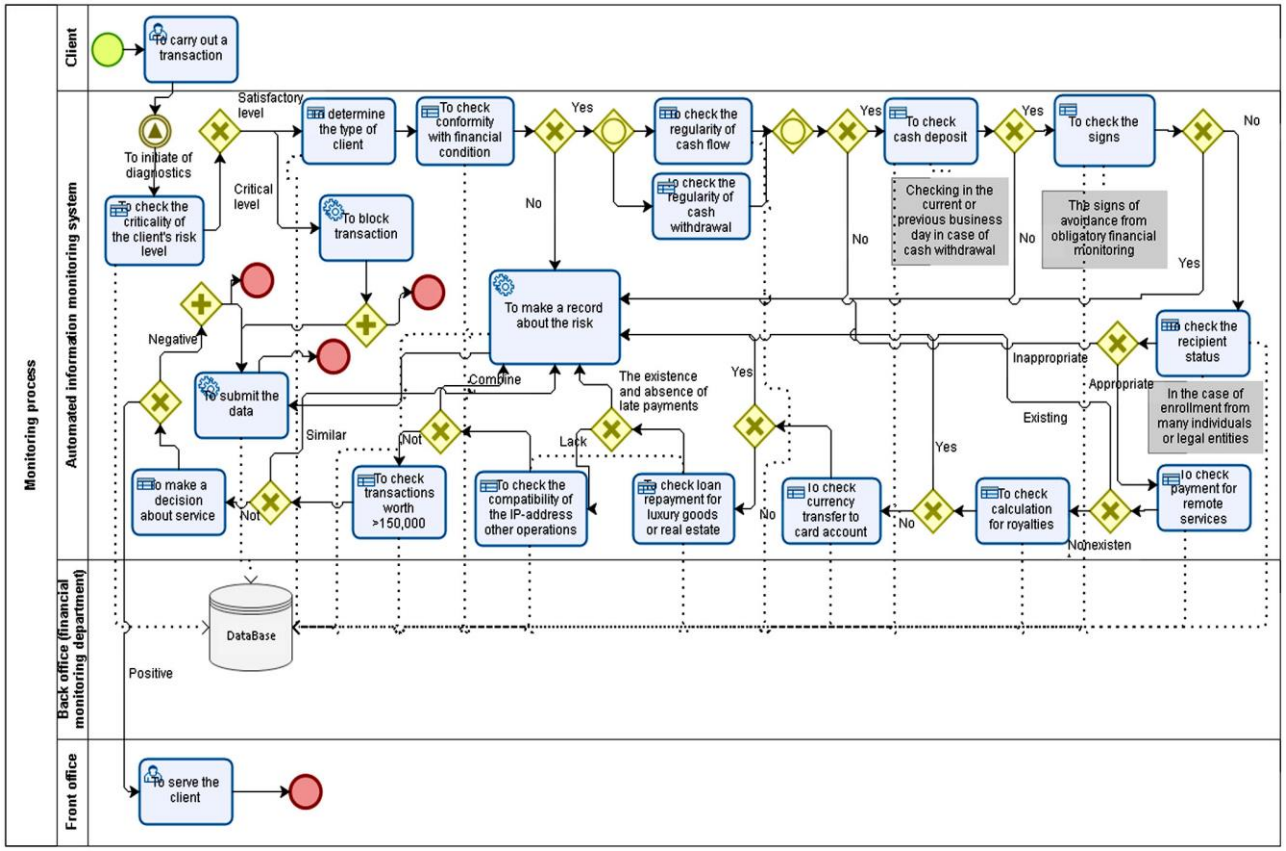


Рисунок 2.27 – Модель бізнес-процесу моніторингу в автоматизованому системному середовищі

Розглядаючи дані, представлені на рисунку 2.27, 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. 2.27) 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 2.28 показаний результат цього моделювання - модель DFD фінансового моніторингу банківських операцій, що виконується в програмному середовищі All Fusion Process Modeller [176].

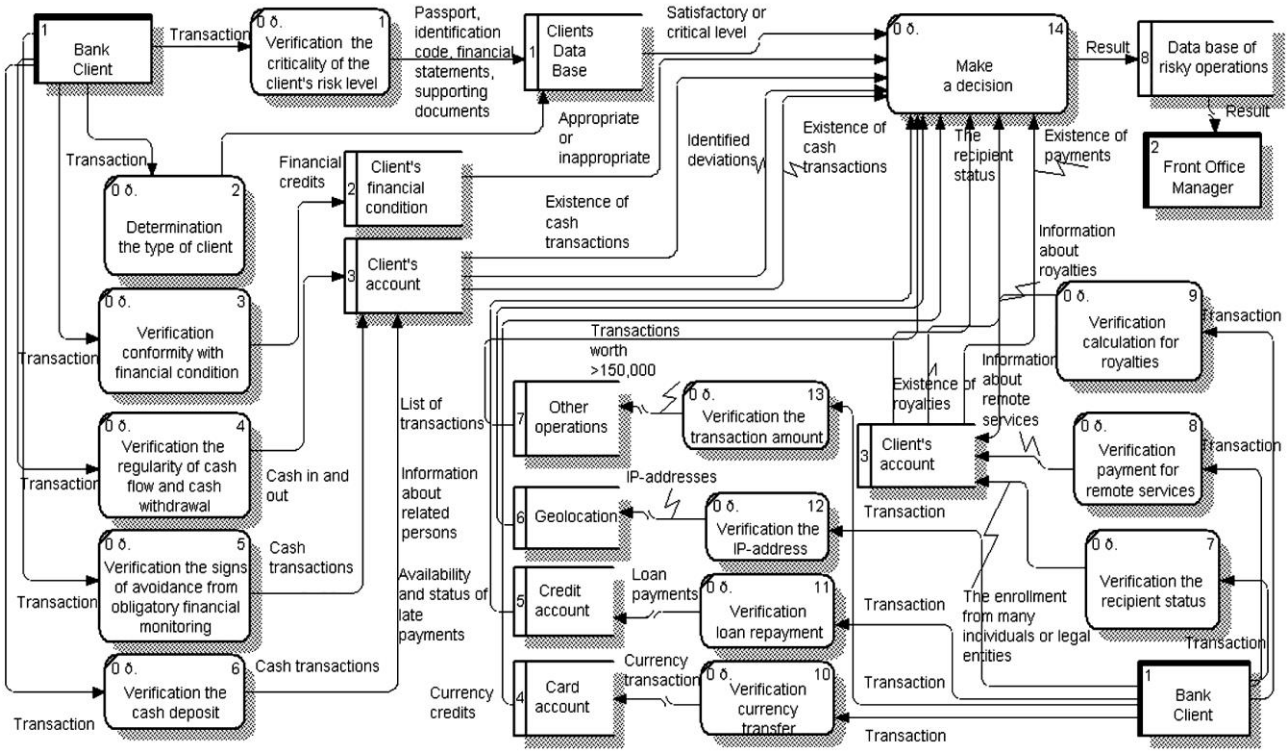


Рисунок 2.28 – DFD-модель автоматизованого моніторингу банківських транзакцій

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 2.28 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 прототип інформаційної 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 [175] (рис. 2.29).

Запропонована модель (рис. 2.29) 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. 2.30).

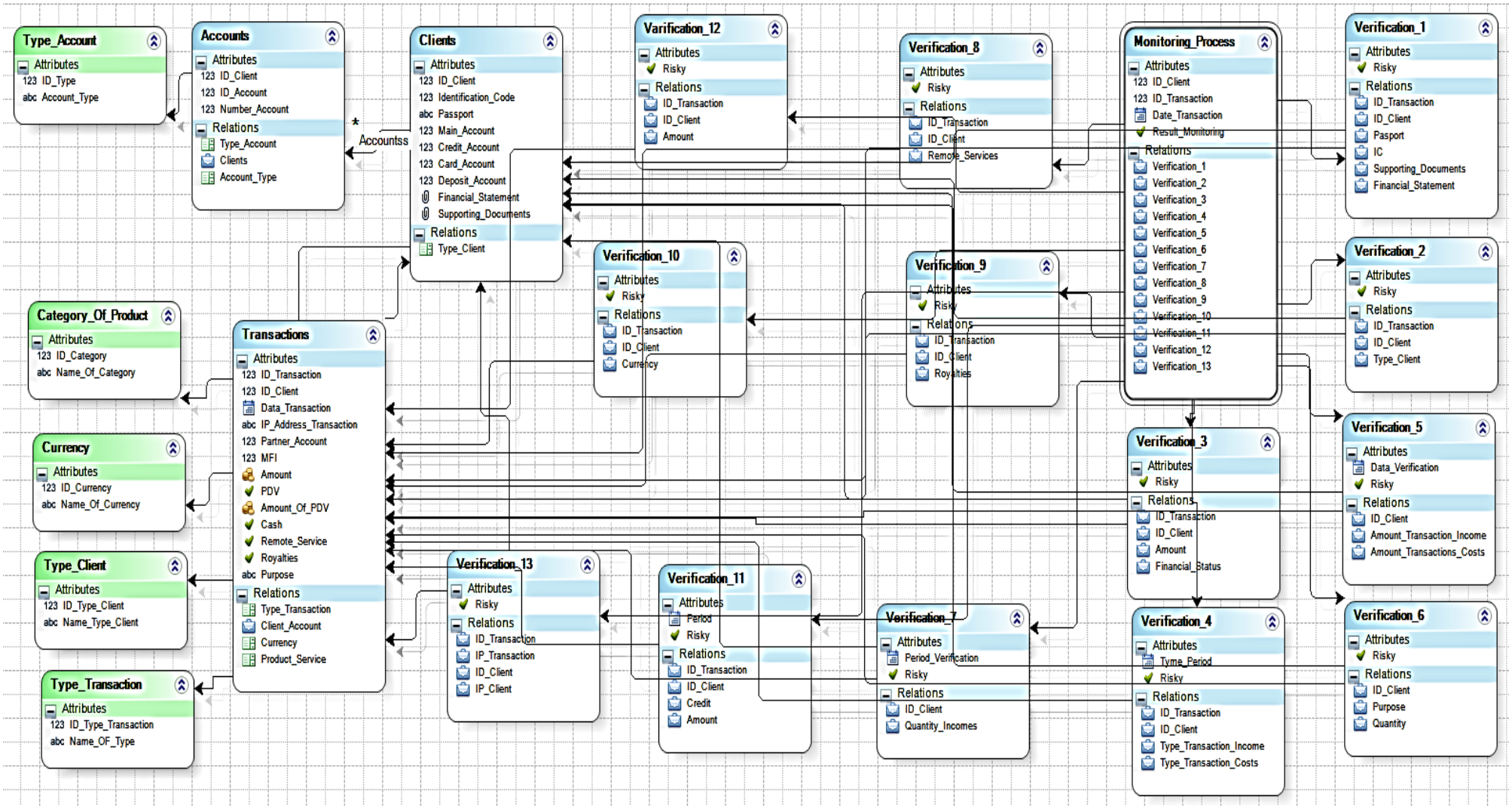


Рисунок 2.29 – Структурна модель бази даних автоматизованої системи моніторингу

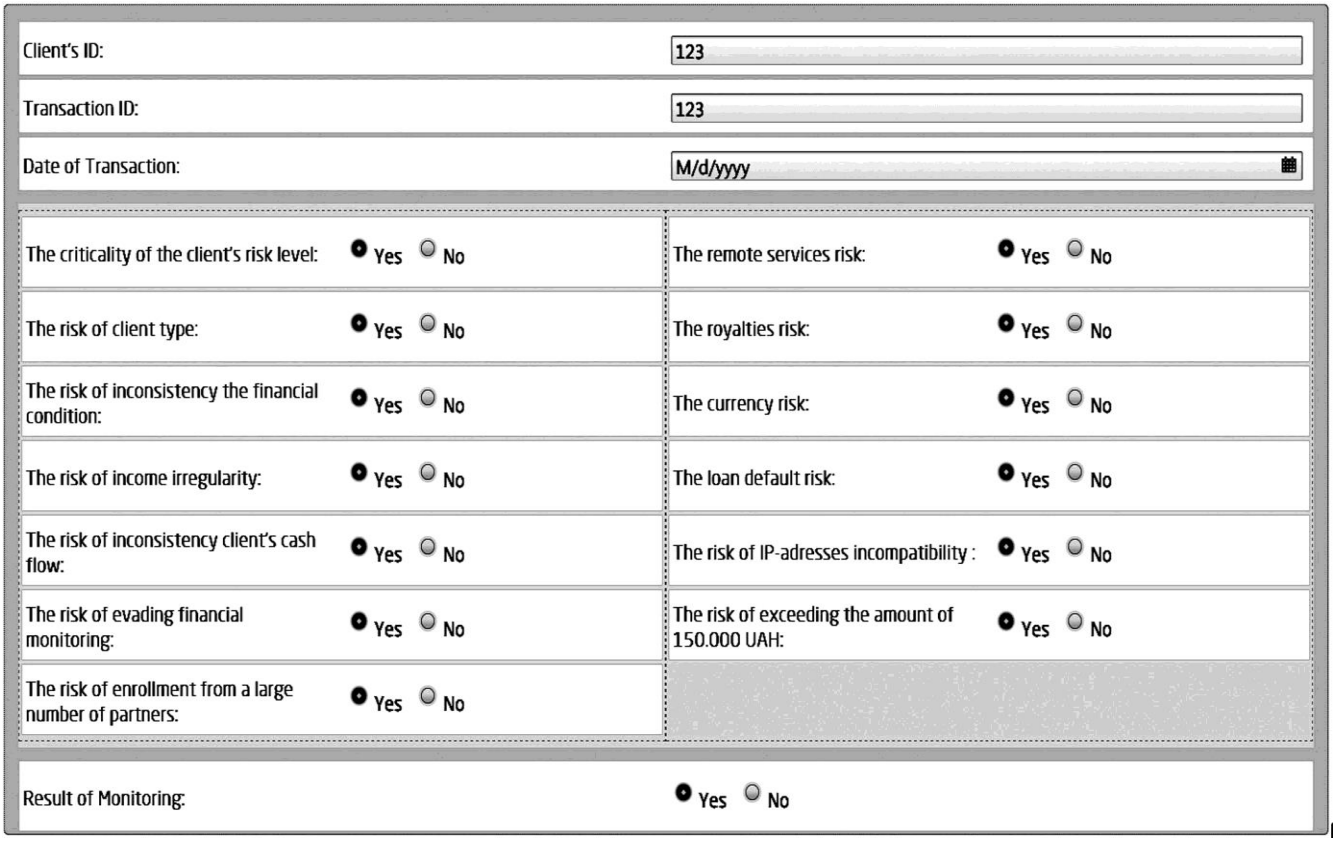


Рисунок 2.30 – Форма інтерфейсу користувача, яка містить результати перевірки

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. Їх розробка здійснювалася за такою логікою, представленою формулами 2.22-2.23.

Для проведення моніторингу – (формула 2.22):

$$\begin{gathered} IF\ [Condition\ of\ Verification\_1 \neq Criteria\ of\ Verification\_1]\ THEN\ [Risk = 1]\ ELSE\ [Risk = 0] \\ \dots \\ IF\ [Condition\ of\ Verification\_N \neq Criteria\ of\ Verification\_N]\ THEN\ [Risk = 1]\ ELSE\ [Risk = 0], \end{gathered} \quad (2.22)$$

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 2.23):

$$\begin{gathered} IF\ [Verification\_1 = 1\ OR\ Verification\_2 = 1\ OR\ Verification\_3 = 1\ OR\ Verification\_4 = 1\ OR\ Verification\_5 = 1\ OR\ Verification\_6 = 1\ OR\ Verification\_7 = 1\ OR\ Verification\_8 = 1\ OR\ Verification\_9 = 1\ OR\ Verification\_10 = 1\ OR\ Verification\_11 = 1\ OR\ Verification\_12 = 1\ OR\ Verification\_13 = 1]\ THEN\ [\text{“YES” } Risk\ AND\ Reject\ operation]\ ELSE\ [\text{“NO” } Risk\ AND\ Accept\ Operation], \end{gathered} \quad (2.23)$$

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.

Пункт 3.3.2 даного звіту було виконано із використанням матеріалів проміжного звіту про НДР [92], публікацій виконавців [169, 177, 178, 179].

3 РОЗРОБКА МЕТОДИЧНИХ ЗАСАД ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ ФІНАНСОВОГО КІБЕРПРОСТОРУ НА ЗАГАЛЬНОДЕРЖАВНОМУ РІВНІ

3.1 Забезпечення розвитку кіберпростору як складової інформаційної безпеки на загальнодержавному рівні

3.1.1 Канонічний аналіз взаємозв'язку інформаційної безпеки та соціо-економіко-політичного розвитку країни

У сучасному світі на тлі промислової революції 4.0 більшість процесів переводиться у цифровий або віртуальний світ. Це пов'язано із тим, що в різних сферах соціального, економічного, політичного розвитку країни знаходять масу переваг у використанні комп'ютерних, інтелектуальних, кібер-фізичних та інших технологій для вирішення нагальних проблем суспільства. Так, завдяки поширення Інтернету речей та Інтернет-торгівельних платформ, компанії збільшують обсяги збуту, нарощують клієнтські бази, що сприяє отриманню надприбутків. Впровадження систем типу «електронна адміністрація», дозволяє знижувати час та грошові витрати на обслуговування громадян, підвищувати якість адміністративних послуг. Переведення платіжних засобів у безготівкову площину сприяє також зниженню витрат для банків на здійснення операцій, підвищує зручності для клієнтів щодо сплати за товари, послуги, отримання та погашення кредитів, здійснення комунальних платежів, тощо. Ці приклади та багато інших показують, на скільки сучасне суспільство є залежним від мобільних пристроїв, комп'ютерних технологій та інформаційних систем.

З іншого боку, цифровізація та комп'ютеризація суспільства призводить до того, що отримання інформації стає метою злочинців та шахраїв, які здійснюють хакерські атаки для незаконного отримання інформації компанії, викрадають дані клієнтів платіжних систем, провадять вірусні атаки для руйнування інформаційного середовища та усунення конкурентів компанії, тощо. Тому зростає необхідність підвищення заходів кібербезпеки зокрема та інформаційної

безпеки в цілому. Дане питання є актуальним не тільки для окремих компаній, різних установ, банків, але це є важливим й для країни в цілому. Інформаційна безпека на рівні держави є доволі складним поняттям, яке уособлює ряд інститутів, заходів, які сприяють захисту інформаційного простору країни та суспільства від здійснення зовнішніх, незаконних інформаційних атак, кібер-тероризму, які завдають шкоди національним інтересам, соціальному, економічному та політичному життю країни. Тому для ефективної організації системи інформаційної безпеки важливо розуміти, яким чином вона формується та від яких чинників залежить. Відповідно, можна сформувати гіпотезу про те, що ефективність системи інформаційної безпеки на державному рівні обумовлюється факторами соціально-економічного розвитку країни, тобто розвинуті країни із потужним соціально-економічним потенціалом та стабільною політичною ситуацією мають підвищений рівень інформаційної безпеки та навпаки, збільшення її рівня впливає на розвиток країни. Дана гіпотеза потребує перевірки та підтвердження або відхилення.

Для доведення висунутої гіпотези у якості показника, що характеризує рівень інформаційної безпеки країни, було обрано національний індекс кібербезпеки, який використовується для оцінки підготовленості країни протидіяти різним кіберзагрозам та можливості керувати різними кібер-інцидентами. Хоча даний показник звужує рамки прийнятого в Україні поняття інформаційної безпеки, але в світовій практиці саме він застосовується для надання актуальної та точної інформації щодо розвитку національних систем кібербезпеки (інформаційної безпеки), порівняння дій влади в галузі безпеки інформації та отримання інформації щодо найкращих практик в цій сфері [180]. Також складові національного індексу кібербезпеки характеризують безпеку за 12 напрямками, а саме: розробка політики та стратегії в галузі кібербезпеки; аналіз та інформація щодо кіберзагроз; організація освіти та професійного розвитку у галузі кібербезпеки; оцінка внеску у глобальну кібербезпеку; рівень захисту цифрових послуг: відповідальність, стандарти, органи; організація захисту основних послуг; електронна ідентифікація та послуги довіри; захист

персональних даних; реагування на кібер-інциденти; кіберрегулювання кризи; боротьба з кіберзлочинністю; військові кібер-операції [180]. Тому, на нашу думку, даний індикатор та його складові дозволять в повному обсязі зробити оцінку щодо рівня інформаційної безпеки країни в цілому.

Використовуючи значення національного індикатора кібербезпеки за 2018 рік для 159 країн світу, побудуємо карту, яка дозволить зробити візуальний аналіз географії країн та дозволить оцінити, для яких країн характерний високий рівень безпеки, а для яких країн низький (рисунок 3.1).

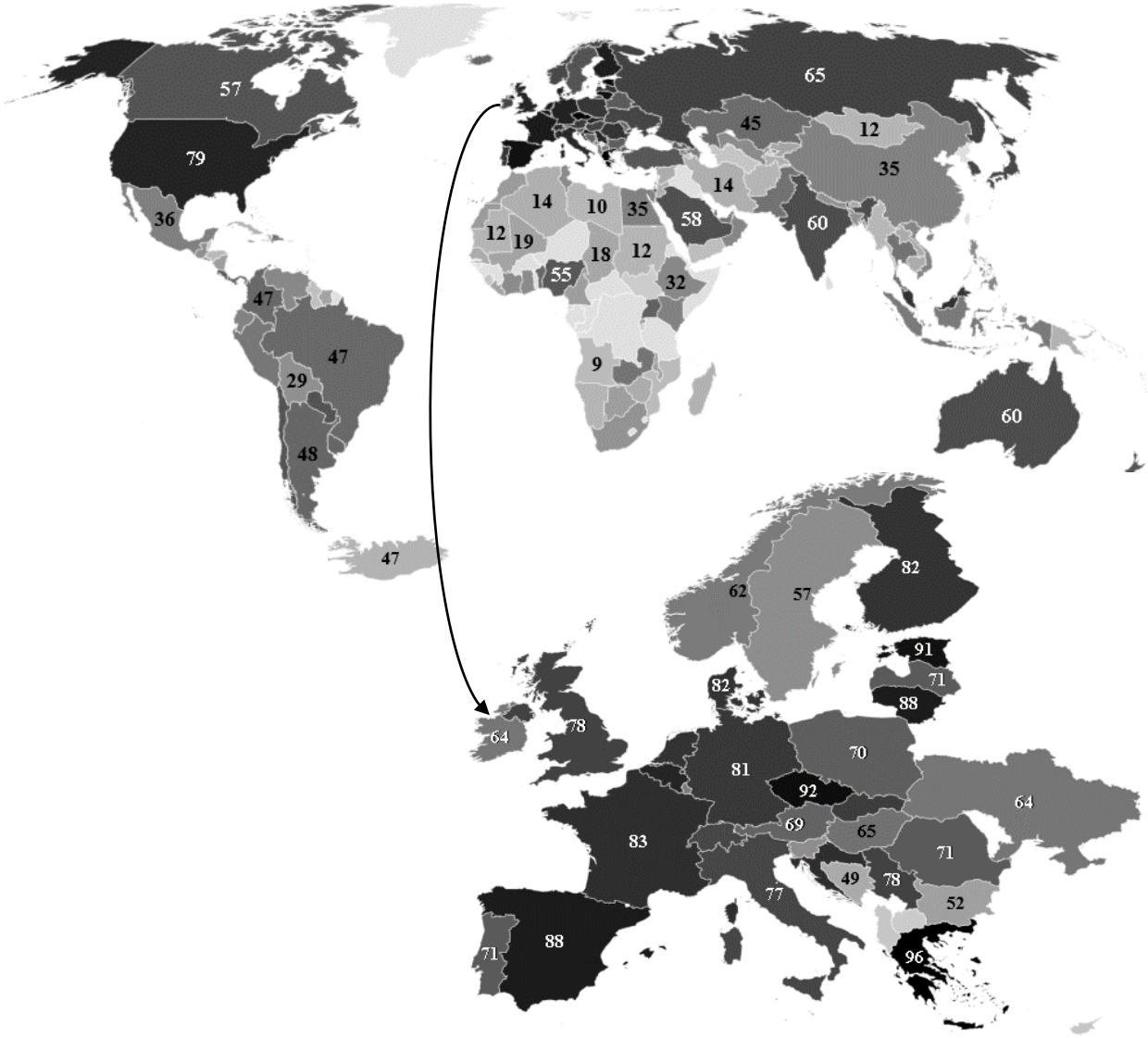


Рисунок 3.1 – Карта країн світу із визначеним національним індексом кібербезпеки

Джерело дослідження: побудовано на основі [181]

Аналізуючи дані, представлені на рисунку 3.1, можна сказати, що держави, які відносяться до розвинутих, а саме країни Європи, США, Канада, Австралія та інші, мають високі значення національного індексу кібербезпеки. Хоча, якщо порівнювати країни, що розвиваються, наприклад, Україна, яка має індекс, рівний 64, та розвинуту країну Австралію з індексом 60, то можна дійти висновку, що рівень безпеки в Україні вищий. Також цей показник у України є вищим у порівнянні з такими розвинутими країнами, як Канада (57), Швеція (57), Норвегія (62), Японія (62). Це характерно й для Малайзії, Росії, Індії та ряду інших країн, що розвиваються, тобто за рівнем національного індексу кібербезпеки вони випереджають ряд розвинутих країн. Можна виділити й Нігерію, показник якої дорівнює 55, тобто за рівнем кібербезпеки дана країна наздоганяє Канаду та Швецію. Що стосується країн, які є найменш розвинутими, то вони мають доволі низькі показники кібербезпеки. Тобто візуальний аналіз нам дозволив зробити висновок, що в основному країни, які є розвинутими мають дійсно високі показники національного рівня кібербезпеки, що говорить про її високий рівень в цілому. Частина країн, які вважаються тими, що розвиваються, також мають високий рівень кібербезпеки. Можна попередньо прийняти нашу гіпотезу щодо існування впливу рівня економіко-соціо-політичного розвитку країн на рівень інформаційної безпеки країни.

Для подальшого підтвердження гіпотези проведемо канонічний аналіз, який дозволить нам математично прийняти або відхилити висунуту гіпотезу. Даний інструмент дозволяє досліджувати залежності між двома множинами змінних та виявляти зв’язки між ними, що дозволить оцінити ступінь впливу однієї множини на іншу та обґрунтувати її статистичну значимість [182, с. 185].

Для проведення дослідження було обрано ряд показників для 159 країн світу. Їх вибір здійснювався, виходячи з того, яким чином дані індикатори відображають розвиток країни: економічний, або соціальний, або політичний. Так, базу даних сформували індикатори економічного розвитку за 2018 рік, а саме [183]: ВВП на душу населення (у поточних доларах США); загальнодержавні витрати на кінцеве споживання (% від ВВП); чисті портфельні

інвестиції (платіжний баланс, у поточних доларах США); загальний рівень безробіття (% від загальної робочої сили); інфляція, дефлятор ВВП (річний у %); загальні резерви (включаючи золото, у поточних доларах США); сальдо поточного рахунку (платіжний баланс, у поточних доларах США); оплачувані та наймані працівники (% від загальної кількості зайнятих); індекс GINI; експорт товарів та послуг (% від ВВП); високотехнологічний експорт (% від промислового експорту); запаси зовнішньої заборгованості, загальна (погашена та непогашена заборгованість, у поточних доларах США); чистий приплив прямих іноземних інвестицій (платіжний баланс, у поточних доларах США); ВВП (поточні долари США); приріст ВВП (річний у %); ВНД на душу населення, за паритетом купівельної здатності (у поточних міжнародних доларах); ВНД, за паритетом купівельної здатності (у поточних міжнародних доларах); валовий капітал (% від ВВП); імпорт товарів та послуг (% від ВВП); промисловість, включаючи будівництво, додана вартість (% від ВВП); дохід, без урахування грантів (% від ВВП); податкові надходження (% від ВВП).

Також було обрано індикатори, які характеризують соціо-політичний рівень розвитку країни [183]: оцінка контролю корупції; оцінка ефективності уряду; оцінка політичної стабільності та відсутності насильства / тероризму; оцінка якості регуляторів; оцінка верховенства права; оцінка потужності статистичної системи країни; ймовірна тривалість життя; кількість підписок на послуги мобільного зв'язку (на 100 осіб); кількість осіб, які користуються Інтернетом (% від населення країни); кількість захищених Інтернет-серверів (на 1 мільйон людей); плата за використання інтелектуальної власності, платежі (BoP, поточні долари США); збори за використання інтелектуальної власності, квитанції (BoP, поточні долари США); патентні заявки, нерезиденти; патентні заявки, резиденти; статті науково-технічних журналів.

На першому кроці було проведено кореляційний аналіз у аналітичному пакеті “STATISTICA” між обраними соціо-економіко-політичними показниками розвитку країн та складовими індикатора національної кібербезпеки. Даний аналіз дозволив нам вибрати саме ті показники, між якими існує статистичний

зв'язок. Як правило, на практиці пріоритет надається тільки тим показникам, між якими існує тісний зв'язок, але нами було враховано всі показники, які мали хоча б, як мінімум, слабкий зв'язок, тобто значення коефіцієнта кореляції для них перевищувало рівень 0,3. Це було зроблено з метою визначення всього набору показників, які мають хоча б якійсь зв'язок з інформаційною безпекою. В результаті було обрано тільки 19 показників соціо-економіко-політичного розвитку та 12 складових національного індикатору кібербезпеки.

На наступному кроці було проведено канонічний аналіз, мета якого полягає у визначенні лінійних залежностей між групами змінних, що дозволяє оцінити вплив однієї групи факторів на іншу та навпаки. Загальну ідею аналізу зобразимо у вигляді наступних рівнянь (формула 3.1):

$$Y = a_1 y_1 + a_2 y_2 + \cdots + a_{12} y_{12};\ X = b_1 x_1 + b_2 x_2 + \cdots + b_{19} x_{19}, \qquad (3.1)$$

де $y_1, y_2, \dots, y_{12}$ – множина змінних, які відображають складові національного індексу кібербезпеки;

$x_1, x_2, \dots, x_{19}$ – множина змінних, які відображають відібрані показники соціо-економіко-політичного розвитку країни;

Y та X – зважені суми змінних кожної множини, які є канонічними змінними та які визначають канонічний корень;

$a_1, a_2, \dots, a_{12};\ b_1, b_2, \dots, b_{19}$ - вагові коефіцієнти, які розраховуються виходячи з максимальної корельованості обох множин.

В результаті виконання модуля канонічного аналізу у пакеті "STATISTICA" отримано підсумки, представлені на рисунку 3.2.

З рисунку 3.2 можна побачити, що значення канонічної кореляції R = 0,89935, тобто між множиною відібраних соціо-економіко-політичних факторів та складових індексу кібербезпеки існує сильний кореляційний зв'язок. Як результат, збільшення впливу соціо-економіко-політичних факторів викликає підвищення рівня кібербезпеки країни та навпаки, посилення рівня кібербезпеки позитивно впливає на соціо-економіко-політичний розвиток країни.

N=159	Canonical Analysis Summary (Data_Stat.sta) Canonical R: .89935 Chi²(228)=535.10 p=0.0000 **Left Set**	Right Set
No. of variables	12	19
Variance extracted	100.000%	74.8349%
Total redundancy	49.1399%	38.4118%
Variables: 1	1. Cyber Security Policy Development	GDP per capita
2	2. Cyber Threat Analysis and Information	General government expenditure
3	3. Education and Professional Development	Life expectancy
4	4. Contribution to global cyber security	Wage and salaried workers
5	5. Protection of digital services	Control of Corruption: Estimate
6	6. Protection of essential services	Government Effectiveness: Estimate
7	7. E-identification and trust services	Political Stability and Absence of Violence/Terrorism: Estimate
8	8. Protection of personal data	Regulatory Quality: Estimate
9	9. Cyber incidents response	Rule of Law: Estimate
10	10. Cyber crisis management	Exports of goods and services
11	11. Fight against cybercrime	GNI per capita
12	12. Military cyber operations	High-technology exports
13		Mobile cellular subscriptions
14		Revenue, excluding grants
15		Statistical Capacity score
16		Tax revenue
17		Individuals using the Internet
18		Secure Internet servers
19		Charges for the use of intellectual property, payments

Рисунок 3.2 – Підсумки канонічного аналізу

Значимість коефіцієнта кореляції підтверджує високе значення критерію Пірсона ($\chi^2 = 535{,}10$), рівень значущості якого не перевищує 0,05 (p = 0,0000). Також можна побачити, що значення надмірності для лівої множини, яка відповідає складовим показника кібербезпеки, дорівнює 49,1399%, тобто змінні правої множини, які відповідають обраним індикаторам соціо-економіко-політичного розвитку країни, на 49,1399% пояснюють мінливість показників кібербезпеки, що є досить високим показником. В свою чергу, фактори кібербезпеки на 38,4118% пояснюють мінливість факторів соціо-економіко-політичного розвитку країни, тобто приблизно на 40% розвиток країни залежить також від рівня захищеності інформаційного та кібернетичного простору держави, що є досить значним для такої специфічної сфери, як інформаційна безпека.

Для подальшого аналізу необхідно обрати ті канонічні корені, які є статистично значущими. Результат отриманих коренів та перевірки їх статистичної значущості представлений на рисунку 3.3.

Root Removed	Chi-Square Tests with Successive Roots Removed					
	Canonicl R	Canonicl R-sqr.	Chi-sqr.	df	p	Lambda Prime
0	0.899347	0.808825	535.1017	228	0.000000	0.023091
1	0.688300	0.473757	300.1535	198	0.000004	0.120783
2	0.576003	0.331780	208.9906	170	0.022707	0.229520
3	0.499428	0.249428	151.7451	144	0.313391	0.343480
4	0.472961	0.223692	111.0024	120	0.709467	0.457624
5	0.431163	0.185902	75.0473	98	0.958868	0.589487
6	0.322475	0.103990	45.8415	78	0.998612	0.724099
7	0.280212	0.078519	30.2494	60	0.999520	0.808137
8	0.209031	0.043694	18.6377	44	0.999719	0.876998
9	0.205652	0.042293	12.2935	30	0.998235	0.917068
10	0.162657	0.026457	6.1572	18	0.995513	0.957566
11	0.128105	0.016411	2.3497	8	0.968367	0.983589

Рисунок 3.3 – Оцінка статистичної значущості канонічних коренів

З рисунку 3.3 визначаємо, що Хі-квадрат у першому рядку, який відповідає аналізу без видалення коренів, є статистично значущим ($p < 0,05$), тому хоча б один канонічний корень є також статистично значущим. При видаленні першого найбільш значущого кореня (другий рядок таблиці на рисунку 3.3) отримали, що інші корені, які залишилися, є також значущими. Процедуру повторюємо доти, доки $p > 0,05$. В результаті отримали три статистично значущих корені, тобто доцільно розглядати три пари канонічних змінних. Але для отримання достовірних оцінок навантажень канонічних факторів для трьох пар канонічних змінних, необхідно мати вибірку, яка буде перевищувати в 40-60 раз кількість початкових даних [182, с. 190]. Тому приймаємо рішення, що будемо розглядати тільки перший найбільш значущий корень. Для підтвердження своїх висновків визначимо факторну структуру та надмірність (рис. 3.4-3.5).

Найбільші факторні навантаження мають показники, що відповідають першому кореню, як для лівої, так й для правої множини. Оскільки факторні навантаження представляють собою кореляції між показниками множини, то показники національної безпеки демонструють середній та вище середнього кореляційний зв'язок. Що стосується факторів розвитку, то між ними зустрічаються ті, які демонструють слабкий зв'язок.

Root Variable	Factor Structure, left set		
	Root 1	Root 2	Root 3
1. Cyber Security Policy Development	0.760024	0.002491	-0.186045
2. Cyber Threat Analysis and Information	0.804363	0.223792	-0.221587
3. Education and Professional Development	0.829012	-0.085878	0.070746
4. Contribution to global cyber security	0.687848	0.309192	-0.028693
5. Protection of digital services	0.481421	0.564479	0.326512
6. Protection of essential services	0.640548	0.376292	0.366621
7. E-identification and trust services	0.693371	-0.233652	0.395539
8. Protection of personal data	0.677602	-0.036897	0.190406
9. Cyber incidents response	0.616932	-0.004646	0.156909
10. Cyber crisis management	0.690835	-0.005328	0.244479
11. Fight against cybercrime	0.795608	-0.300298	0.119870
12. Military cyber operations	0.659978	0.026670	-0.313077

Рисунок 3.4 – Факторна структура для складових національної кібербезпеки (фрагмент)

Root Variable	Factor Structure, right set		
	Root 1	Root 2	Root 3
GDP per capita	0.690718	0.287945	-0.094678
General government expenditure	0.582425	0.012476	0.040691
Life expectancy	0.560505	-0.073121	0.092636
Wage and salaried workers	0.689980	-0.055039	0.015387
Control of Corruption: Estimate	0.670031	0.287895	-0.102873
Government Effectiveness: Estimate	0.828089	0.155910	-0.005329
Political Stability and Absence of Violence/Terrorism: Estimate	0.386819	0.291094	0.076111
Regulatory Quality: Estimate	0.857579	0.086692	0.056519
Rule of Law: Estimate	0.751873	0.300340	-0.058753
Exports of goods and services	0.422173	0.302194	0.706982
GNI per capita	0.778433	0.178293	0.027060
High-technology exports	0.533411	0.270292	0.166244
Mobile cellular subscriptions	0.526399	-0.278181	0.250180
Revenue, excluding grants	0.643730	0.081836	0.122554
Statistical Capacity score	-0.408921	-0.592820	0.198385
Tax revenue	0.520408	0.027981	0.075796
Individuals using the Internet	0.775450	0.060895	0.247898
Secure Internet servers	0.396156	0.382797	-0.107892
Charges for the use of intellectual property, payments	0.334831	0.253151	0.071409

Рисунок 3.5 – Факторна структура для факторів розвитку країни (фрагмент)

Але оскільки нам важливо виявити показники, які мають будь-який рівень зв’язку, то будемо мати на увазі, що оцінка політичної стабільності та відсутності насильства / тероризму, експорт товарів та послуг, оцінка потужності статистичної системи країни, кількість захищених Інтернет-серверів, платежі за

використання інтелектуальної власності, чинять слабкий вплив на рівень національної кібербезпеки.

Проаналізуємо отримані частки та надмірності дисперсії. У випадку аналізу складових національної кібербезпеки 100% дисперсії будуть пояснювати усі вилучені корені, у випадку факторів розвитку країни – тільки 74,8%. Перший канонічний корень вилучає 49,1119% дисперсії із складових національної кібербезпеки та 38,2117% дисперсії з факторів розвитку країни, тобто пояснює 49,1119% та 38,2117% зміни рівня національної кібербезпеки та рівня соціо-економіко-політичного розвитку. Інші корені, хоча ми не прийматимемо їх до уваги, пояснюють від 2 до 6% змін, що є незначним. З огляду на надмірність, 39,7229% факторів розвитку пояснюють зміни показників лівої множини, тобто складових національної кібербезпеки. 30,9065% факторів національної кібербезпеки пояснюють зміни, що пов'язані із розвитком країни. Як результат, фактори розвитку є більш інформативними для передбачення рівня національної кібербезпеки країни.

Для подальшого аналізу визначимо канонічні ваги, які є коефіцієнтами регресійних рівнянь, де канонічні змінні є відповідними відкликами (рис. 3.6-3.7).

Variable	Canonical Weights, left set		
	Root 1	Root 2	Root 3
1. Cyber Security Policy Development	0.093381	-0.185643	-0.532721
2. Cyber Threat Analysis and Information	0.276326	0.439113	-0.584769
3. Education and Professional Development	0.256820	-0.243435	-0.077787
4. Contribution to global cyber security	0.107176	0.440184	0.010013
5. Protection of digital services	-0.094643	0.609075	0.196664
6. Protection of essential services	0.058188	0.392554	0.564118
7. E-identification and trust services	0.050683	-0.385354	0.517350
8. Protection of personal data	0.280400	0.059237	-0.014170
9. Cyber incidents response	0.098364	-0.082615	0.004520
10. Cyber crisis management	0.028405	-0.169556	0.449290
11. Fight against cybercrime	0.071589	-0.551104	0.212369
12. Military cyber operations	0.100034	-0.036566	-0.537026

Рисунок 3.6 – Канонічні ваги для складових національної кібербезпеки (фрагмент)

Variable	Canonical Weights, right set		
	Root 1	Root 2	Root 3
GDP per capita	-0.033104	-0.138295	-0.614914
General government expenditure	0.090716	-0.054161	-0.008651
Life expectancy	0.070309	-0.128029	0.196566
Wage and salaried workers	0.028595	0.016751	-0.389475
Control of Corruption: Estimate	-0.399981	0.020568	-0.051804
Government Effectiveness: Estimate	0.339411	-0.387680	-0.341282
Political Stability and Absence of Violence/Terrorism: Estimate	-0.285751	0.132452	0.139113
Regulatory Quality: Estimate	0.532497	-0.646778	0.240597
Rule of Law: Estimate	0.253941	0.914662	-0.036946
Exports of goods and services	-0.191654	0.353281	1.079455
GNI per capita	0.210886	-0.734044	0.204656
High-technology exports	0.058820	0.398051	-0.099102
Mobile cellular subscriptions	-0.033339	-0.192015	0.207310
Revenue, excluding grants	0.524632	0.682581	0.044147
Statistical Capacity score	0.060800	-0.836141	0.019507
Tax revenue	-0.448721	-0.601972	-0.002488
Individuals using the Internet	0.205069	-0.022148	0.064643
Secure Internet servers	0.087222	0.364151	-0.423961
Charges for the use of intellectual property, payments	-0.027525	0.078019	0.300656

Рисунок 3.7 – Канонічні ваги для факторів розвитку країни (фрагмент)

Значення канонічних вагів дозволяє визначити вклад кожного показника у формування значень канонічних змінних. В національну кібербезпеку вноситимуть найбільший вклад (рис. 3.6): захист персональних даних; аналіз та інформація щодо кіберзагроз; організація освіти та професійного розвитку у галузі кібербезпеки; найменший вклад – організація захисту основних послуг; електронна ідентифікація та послуги довіри; кіберрегулювання кризи.

Що стосується факторів розвитку, то найбільший вклад втілюватимуть (рис. 3.7): оцінка якості регуляторів; дохід, без урахування грантів; податкові надходження; найменший вклад – оплачувані та наймані працівники; платежі за використання інтелектуальної власності; ВВП на душу населення; кількість підписок на послуги мобільного зв'язку. При цьому треба враховувати знак значення показника. Якщо вага має знак «+», то із збільшенням фактору значення кореня збільшується, якщо «–», навпаки, значення кореня зменшується. Наприклад, якщо платежі за використання інтелектуальної власності будуть збільшуватися, то це буде зменшувати внесок даного вкладу у значення кореня.

Значення канонічних вагів дозволило нам визначити рівняння регресії для канонічних змінних лівого та правого множин (формула 3.2):

$$\begin{aligned} Y\ (1\ \text{корень}) = {} & 0{,}0934\ y_1 + 0{,}2763\ y_2 + 0{,}2568\ y_3 + 0{,}1072\ y_4 - 0{,}0946\ y_5 \\ & + 0{,}0582\ y_6 + 0{,}0507\ y_7 + 0{,}2804\ y_8 + 0{,}0984\ y_9 + 0{,}0284\ y_{10} \\ & + 0{,}0716\ y_{11} + 0{,}1000\ y_{12}, \\ X\ (1\ \text{корень}) = {} & -0{,}0331\ x_1 + 0{,}0907\ x_2 + 0{,}0703\ x_3 + 0{,}0286\ x_4 - 0{,}4000\ x_5 \\ & + 0{,}3394\ x_6 - 0{,}2858\ x_7 + 0{,}5324\ x_8 + 0{,}2539\ x_9 - 0{,}1917\ x_{10} \\ & + 0{,}2109\ x_{11} + 0{,}0588\ x_{12} - 0{,}0334\ x_{13} + 0{,}5246\ x_{14} + 0{,}0608\ x_{15} \\ & - 0{,}4487\ x_{16} + 0{,}2051\ x_{17} + 0{,}0872\ x_{18} - 0{,}0275\ x_{19} \end{aligned} \qquad (3.2)$$

Якщо є потреба у визначенні для кожної країни значення канонічних змінних, то необхідно підставити в отриманні рівняння 2 значення факторів розвитку та складових національного індикатору кібербезпеки. Це дозволить знайти зважену суму факторів з урахуванням впливу множин один на одну.

На наступному кроці побудовано діаграму розсіювання канонічних значень для першої пари канонічних коренів (рисунок 3.8), в якій горизонтальна вісь – це складові національного індексу кібербезпеки, а вертикальна – показники соціо-економіко-політичного розвитку.

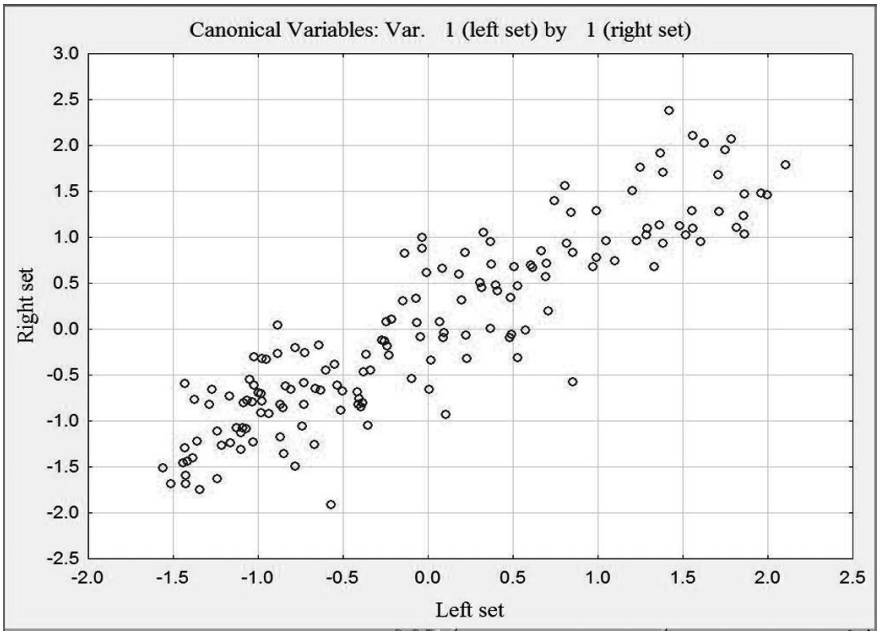


Рисунок 3.8 – Діаграма розсіювання канонічних значень

На діаграмі 3.8 можна побачити, що скупчення спостережень є характерним для лінійної залежності, при цьому графік не містить значних викидів. Це свідчить про те, що між складовими національної кібербезпеки та факторами соціо-економіко-політичного розвитку є досить тісний зв'язок, який говорить про те, що рівень національної кібербезпеки, а в нашому випадку інформаційної безпеки, залежить від рівня розвитку країни, при цьому рівень безпеки може також впливати й на розвиток країни.

Виходячи з результатів проведеного дослідження, можна прийняти гіпотезу щодо обумовленості ефективності системи інформаційної безпеки факторами соціально-економічного розвитку країни. Дану гіпотезу було підтверджено візуальним аналізом карти країн світу, розподілених за національним індексом кібербезпеки. Даний аналіз підтвердив, що країни, які відносяться до розвинутих, мають найвище значення національного індексу кібербезпеки. Найменш розвинуті країни мають найнижчі значення індексу. В результаті проведеного канонічного аналізу було визначено, що приблизно 49% множини складових показника кібербезпеки пояснюються факторами соціо-економіко-політичного розвитку. Оскільки дані фактори оцінюють спроможність країни протистояти різним кіберзагрозам, то у країн із високим економічним потенціалом збільшуються можливості їм протидіяти, а також зростає фінансова спроможність для організації додаткових заходів, залучення більш сучасних технологій, кваліфікованих фахівців. Але з іншого боку, саме у таких країнах підвищується ризик кібератак, інформаційного тероризму та кібершахрайства. Тому треба провести додаткове дослідження щодо аналізу впливу рівня кіберзагроз на різні країни світу.

Також було визначено, що 38% множини факторів розвитку країни пояснюється за рахунок складових національної кібербезпеки. Тобто підвищення рівня інформаційної безпеки в цілому та кібербезпеки зокрема сприятиме розвитку країни в частині соціального, економічного чи політичного розвитку. Чим вище рівень захищеності персональних даним, тим вище довіра

населення до держави та різних інститутів. Якщо це фінансові дані людини, тим вище надійність банківської системи та менше втрати від кібершахраїв.

Отримані в роботі результати сприятимуть виробленню ряду стратегічних заходів саме в тих напрямках, де цей зв'язок є тіснішим. Як наслідок, це призведе до посилення інститутів безпеки, впровадження нових методів та заходів безпеки, що, в свою чергу, позитивно впливатиме на політичну стабільність в країні, соціальну захищеність населення від кібершахрайств, зниження збитків економіки держави та суб’єктів господарювання від незаконного використання ресурсів. Впровадження спеціалізованих програм навчання, створення ефективних інститутів для боротьби з кібертероризмом, розробка відповідних норм законодавства, які підвищують відповідальність за кіберзлочини, впровадження потужних аналітичних систем та інше – все це напрямки впливу на успішний розвиток будь-якої країни.

Пункт 3.1.1 даного звіту було виконано із використанням матеріалів публікацій виконавців [184, 185, 186].

3.1.2 Використання карт Кохонена для аналізу рівня інформаційної безпеки країн з урахуванням їх розвитку

Сьогодні дуже важко уявити різні сфери діяльності суспільства без використання комп’ютерних та інформаційних технологій. Особливо це відчувається в бізнесі, політиці, повсякденному житті людини. Процесу інформатизації та комп’ютеризації також сприяють й результати четвертої промислової революції, яка впливає на підвищення можливостей кіберфізичних систем для вирішення потреб країни, суспільства, суб’єктів господарювання, окремої людини. Але такий стрімкий розвиток призводить також й до того, що новітні технології стають інструментами для незаконного збагачення різного роду злочинців. Це проявляється у збільшенні випадків хакерських атак на бізнес

підприємств з метою отримання фінансової інформації. Також збільшується кількість кібер-шахраїв, які застосовують програмно-технологічні можливості для ошукування населення. Це може бути й інформаційний вплив на суспільство із використанням соціальних мереж, що призводить до інформаційних війн та політичної дестабілізації у країні.

Перелічені факти є одними з видів загроз, які призводять до зниження ефективності інформаційної безпеки, як окремого суб'єкта, так й країни в цілому. Тому важливо розуміти, які проблеми в галузі інформаційної безпеки існують, що є фактором їх виникнення, та як його наслідки впливатимуть на рівень розвитку країни в цілому. Поняття інформаційної безпеки є комплексним, яке охоплює мікро- та макрорівень, а також включає різні її аспекти: правову, освітню, інституційну, програмно-технологічну та інші. Досліджуючи рівень інформаційної безпеки країни, слід також враховувати й ці аспекти. Варто зазначити, що фактори економічного, соціального та політичного розвитку країни також можуть впливати на рівень безпеки, оскільки країна із високими соціальними стандартами та рівнем життя запроваджує найбільш ефективні заходи безпеки. Таким чином, дослідження рівня інформаційної безпеки країн з урахуванням їх розвитку є актуальним та потребує системного вивчення.

Для проведення дослідження було обрано вхідні дані, які характеризують два аспекта: рівень інформаційної безпеки країни та рівень розвитку. З цією метою проведено дослідження офіційних джерел в галузі інформаційної безпеки, в результаті чого було виділено 5 основних показників, які характеризують її окремі сфери: Global Cybersecurity Index характеризує рівень кібербезпеки для країн-членів Міжнародного союзу електрозв'язку; National Cyber Security Index визначає рівень готовності країни протидіяти кіберзагрозам; ICT Development Index вимірює рівень розвитку інформаційних технологій в країні; Networked Readiness Index визначає ступінь технологічної готовності країни для застосування новітніх інформаційно-комунікаційних технологій в різних сферах; Digital Development Level характеризує рівень цифровізації країни [187]. Оскільки на практиці не існує показника, який би вимірював рівень

інформаційної безпеки, то поєднання наведених індексів можна використовувати для оцінки окремих її напрямків.

У якості показників розвитку було проаналізовано базу даних Світового банку, серед яких було виділено 37 індикаторів, для яких було зроблено припущення, що вони мають зв'язок із показниками безпеки. В результаті проведеного кореляційного аналізу було виділено 12 показників, для яких рівень їх статистичного зв’язку із показниками безпеки характеризується як тісний, тобто коефіцієнт кореляції перевищує 0,5 або -0,5. Таким чином, було відібрано: GDP per capita (current US$); Life expectancy; Wage and salaried workers, total (% of total employment); Control of Corruption: Estimate; Government Effectiveness: Estimate; Regulatory Quality: Estimate; Rule of Law: Estimate; GNI per capita, PPP (current international $); Mobile cellular subscriptions (per 100 people); Revenue, excluding grants (% of GDP); Individuals using the Internet (% of population); General government expenditure (% of GDP) [188].

Розрахунки проводилися для 159 країн світу. У якості розрахункового періоду було обрано 2018 рік. Це було зроблено, виходячи з повноти наявності даних для кожного з обраних показників.

Для того, щоб дані можна було піддавати подальшому аналізу, необхідно провести їх нормалізацію, оскільки кожен з відібраних показників має різні виміри та значення. З цією метою було обрано метод нелінійної нормалізації, оскільки він дозволяє отримати більш ефективні оцінки, ніж лінійна нормалізація, в межах [0, 1]. Дану процедуру було проведено за формулою 3.3:

$$Z_{ij} = \left(1 + e^{\frac{\overline{y_j} - y_{ij}}{\sigma(y)}}\right)^{-1}, \tag{3.3}$$

де Z_{ij} – нормалізоване значення j-го показника в розрізі і-ої країни;

$\overline{y_j}$ – середнє значення j-го показника в межах досліджуваного переліку країн;

y_{ij} – фактичне значення j-го показника в розрізі і-ої країни;

$\sigma(y_j)$ – середнє квадратичне відхилення j-го показника в межах досліджуваного переліку країн.

Після проведення нормалізації вхідних даних, необхідно здійснити їх перевірку на якість, виявлення викидів, дублікатів та протиріч. Даний процес було проведено за допомогою аналітичної платформи Deductor Academic. В результаті аналізу якості даних було виявлено 3 викиди за індикатором «Life expectancy», що свідчить про необхідність коректування даних за цим показником. Але в цілому отриманий показник якості знаходиться в межах (0,7299; 0,9842), що говорить о високій якості початкового набору даних. Перевірка даних на наявність дублікатів та протиріч виявила, що вони відсутні у наборі даних. В результаті проведених перевірок було здійснено коректування тільки даних індикатора «Life expectancy», для чого було обрано розрахунок ймовірного значення для спостережень, які є викидами.

Після підготовки даних проведено аналіз рівня інформаційної безпеки країн з урахуванням їх розвитку, що здійснювалося із використанням самоорганізованих карт Кохонена на платформі Deductor Academic. Карти Кохонена представляють собою вид нейронної мережі з некерованим навчанням, яка проектує дані з багатовимірного простору у двовимірний. Даний інструментарій було розроблено фінським вченим Теуво Кохоненом у 1982 році [189].

В процесі побудови карти було експериментальним шляхом випробувано різні способи її побудови. В результаті було враховано наступні опції:

1) для усіх змінних було задано призначення «Вхідні», тільки змінну «Назва країни» було враховано, які «Інформаційне»;

2) розбиття даних на навчальну множину та тестову не проводилося з урахуванням того, що будь-який алгоритм кластеризації, в тому числі й карти Кохонена, є доволі суб’єктивним;

3) при налаштуванні параметрів карти було обрано розміри 24:18, оскільки стандартний розмір 16:12 не дозволив виявити всіх кластерів;

4) кількість епох було обрано 500 та рівень похибки для розпізнавання було обрано менше 0,05;

5) для визначення початкових вагів нейронів було обрано спосіб «З власних векторів», який дозволяє ініціалізувати початкові ваги нейронів значеннями підмножини гіперплощини, через яку проходять два власних вектори матриці коваріації вхідних значень вибірки. Результати з використанням цього способу виявилися кращими для матриці похибок квантування та матриці щільності квантування у порівнянні із способами «З навчальної множини» та «Випадковими значеннями»;

6) у якості функції сусідства було «Ступінчату», оскільки результати порівняння матриці похибок квантування та матриці щільності квантування для даної функції виявилися кращими ніж для функції «Гауссова»;

7) при порівнянні результатів автоматичного визначення кількості кластерів та ручного визначення, врешті-решт було обрано автоматичне визначення з рівнем значущості 0,5%. Кількість кластерів при ручному режимі виставлялося рівним 5, бо саме стільки кластерів було отримано при ручній перевірці з використанням методу k-means. Але результати автоматичного визначення виявилися кращими.

Після виконання процедур алгоритму побудови карт Кохонена отримано 7 кластерів та для кожного з відібраних показників побудовано карту. Результати представлені на рисунку 3.9. Також було виведено спеціальні карти, які дозволили зробити порівняння із іншими варіантами карт, побудованих для різних функцій сусідства та методів ініціалізації початкових вагів. Кінцевий результат матриць помилок квантування, щільності попадання та відстаней представлено на рисунку 3.10. В процесі аналізу даних карт, було виявлено 16 країн, помилка квантування для яких перевищує 10%, що складає близько 10% від загальної кількості країн. Можна вважати, що це допустимий рівень відхилення для моделей кластеризації.

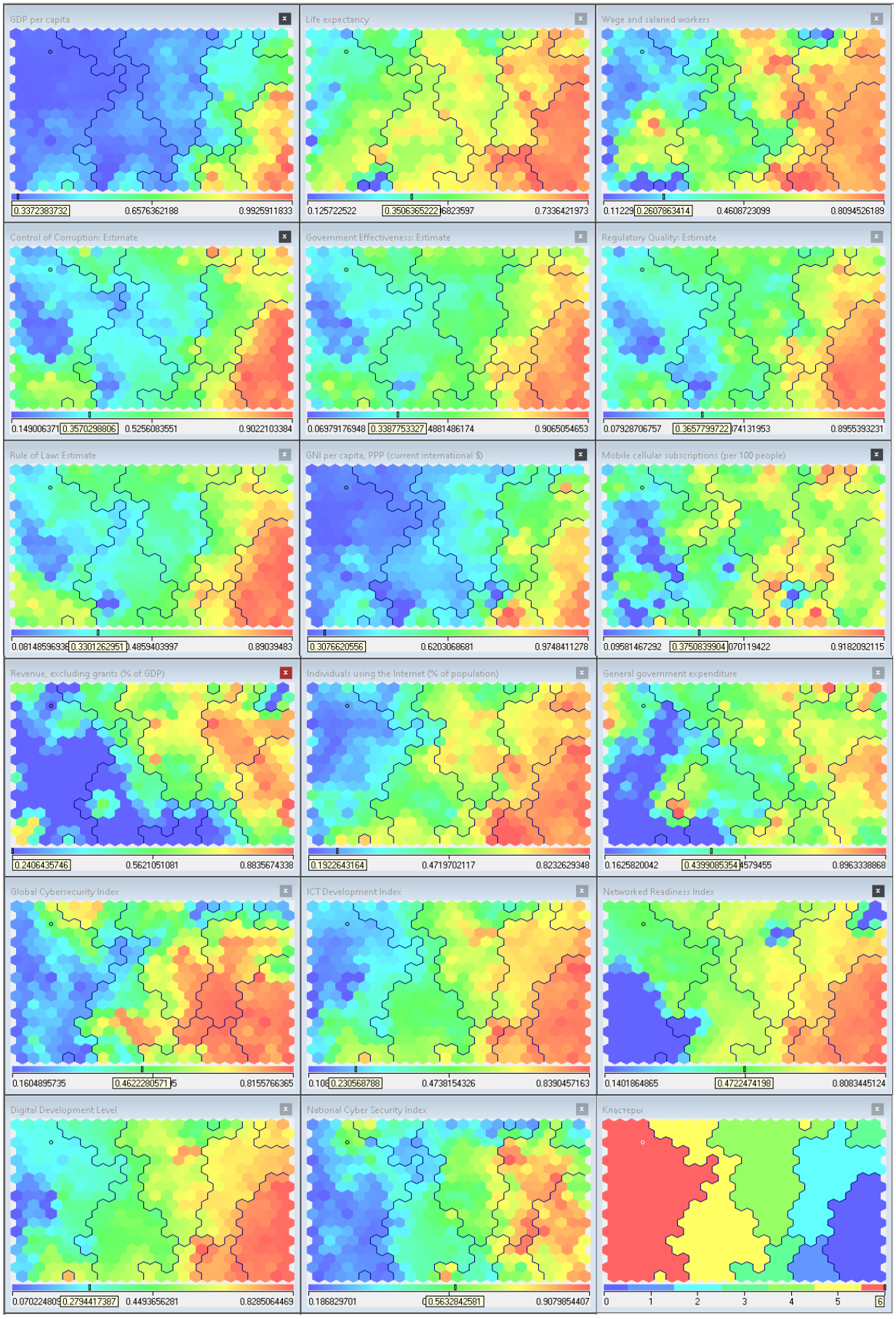


Рисунок 3.9 – Карти Кохонена показників інформаційної безпеки та розвитку

Рисунок 3.10 – Матриці помилок квантування, щільності попадання, відстаней

Так, до 0-го кластеру увійшла 21 країна: Австралія, Австрія, Бельгія, Великобританія, Данія, Естонія, Ізраїль, Ісландія, Ірландія, Канада, Люксембург, Нідерланди, Німеччина, Нова Зеландія, Норвегія, Сінгапур, США, Фінляндія, Франція, Швеція, Швейцарія. Даний кластер сформували розвинуті країни з потужним економічним потенціалом та високим рівнем інформаційної безпеки (див. рис. 3.9 та табл. 3.1). Тобто, при виникненні різного роду загроз інформаційній безпеці, ці країни зможуть швидше подолати наслідки інформаційної кризи. Також високий рівень їх безпеки говорить про те, що вони для системи безпеки застосовуються сучасні комп'ютерні технології та програмні засоби, які дозволяють їм швидко попереджати загрози.

Кластер 1 сформували 4 країни: Японія, Іспанія, Катар та Арабські Емірати. Вони мають також високі показники розвитку та інформаційної безпеки, які представлені у таблиці 3.1 та на рисунку 3.9. Але у порівнянні із країнами 0-го кластеру, країни 1-го кластеру мають рівень інформаційної безпеки значно нижчим, що проявляється у таких показниках, як ICT Development Index, Networked Readiness Index, Digital Development Level, National Cyber Security Index. Це говорить про те, що ймовірно є певні проблеми в системі інформаційної безпеки даних країн, які потребують вирішення шляхом зміни стратегії інформаційної безпеки.

До 2-го кластеру увійшли 20 країн: Болгарія, Чилі, Хорватія, Кіпр, Чехія, Греція, Угорщина, Італія, Латвія, Литва, Малайзія, Мальта, Маврикій, Польща, Португалія, Румунія, Саудівська Аравія, Словакія, Словенія, Уругвай. Тобто

сюди ввійшла частина розвинутих країн та ті, що розвиваються, які мають середні показники розвитку, що говорить про їх достатні можливості подолання інформаційної кризи (див. рис. 3.9 та табл. 3.1).

Таблиця 3.1 – Середні значення показників у відповідності із профілем кластера

Назва показника	0 кластер	1 кластер	2 кластер	3 кластер	4 кластер	5 кластер	6 кластер
GDP per capita	58179,42	45353,09	19481,37	21216,71	7133,42	5018,98	2825,30
Life expectancy	81,85	81,36	78,12	77,29	73,82	69,87	63,90
Wage and salaried workers	87,59	92,34	82,18	84,82	63,97	49,86	32,86
Control of Corruption	1,81	0,98	0,43	0,46	-0,22	-0,40	-0,70
Government Effectiveness	1,64	1,19	0,71	0,50	0,01	-0,23	-0,87
Regulatory Quality	1,67	0,93	0,79	0,45	0,05	-0,40	-0,80
Rule of Law	1,68	1,01	0,64	0,40	-0,21	-0,44	-0,69
GNI per capita	56525,24	61757,50	32200,00	27756,25	16200,77	9450,69	5560,59
Mobile cellular subscriptions	122,33	151,94	128,07	111,12	124,97	106,35	58,79
Revenue, excluding grants	32,38	8,21	34,35	2,05	27,40	9,98	6,06
Individuals using the Internet	90,45	93,87	77,35	85,17	66,51	53,09	26,28
General government expenditure	19,72	16,85	17,42	19,46	16,26	11,57	6,26
Global Cyber-security Index	84,00	86,25	72,25	56,88	55,81	46,45	20,73
ICT Develop-ment Index	82,81	76,50	70,20	70,63	57,19	43,38	24,73
Networked Readiness Index	80,29	74,75	65,05	41,50	56,35	47,79	22,65
Digital Develop-ment Level	81,50	75,62	67,50	68,97	58,21	48,15	31,04
National Cyber Security Index	71,37	61,69	67,53	38,47	38,81	30,32	15,89

Але показники безпеки є нижчими у порівнянні із країнами 1-го кластеру, особливо це стосується ICT Development Index, Networked Readiness Index, Digital Development Level, Global Cyber Security Index. Проблемами інформаційної безпеки країн даного кластеру можуть бути ті, які пов’язані із

правовими аспектами в даній сфері, рівнем організації освіти, недостатнім рівнем інвестування у новітні інформаційні технології, тощо.

До 3-го кластеру увійшли 8 країн: Багами, Бахрейн, Барбадос, Бруней, Південна Корея, Монтенегро, Оман, Сербія. Ряд показників розвитку країн даного кластеру перевищую показники країн 2-го кластеру, а саме: GDP per capita, Wage and salaried workers, Individuals using the Internet, General government expenditure (див. рис. 3.9 та табл. 3.1). Це свідчить про те, що ці країни знаходяться на стадії свого активного розвитку, як і країни 2-го кластеру. Але що стосується рівня інформаційної безпеки, то є проблеми в частині розвитку загальної стратегії інформаційної безпеки, про що свідчать низькі показники National Cyber Security Index, Global Cybersecurity Index та Networked Readiness Index. Окрім цього можна виділити проблему, пов'язану із низьким рівнем технологічної готовності країни до забезпечення надійної системи інформаційної безпеки.

До 4-го кластеру увійшли 26 країн: Албанія, Аргентина, Вірменія, Азербайджан, Беларусь, Боснія та Герцеговина, Ботсвана, Бразилія, Колумбія, Коста Ріка, Грузія, Ямайка, Йорданія, Казахстан, Мексика, Молдова, Монголія, Марокко, Намібія, Північна Македонія, Російська Федерація, Сейшели, Південна Африка, Тайланд, Туреччина, Україна. Частину країн даного кластеру сформували колишні республіки Радянського Союзу, а також ряд країн, які пережили становлення через минулі військові події. На даний момент їх усіх можна віднести до групи країн, що розвиваються, але вони мають ряд суттєвих проблем в економічній, соціальній та політичній сфері. Це підтверджується їх низькими значеннями показників розвитку у порівнянні із країнами попередніх кластерів (див. рис. 3.9 та табл. 3.1). Що стосується їх стану інформаційної безпеки, то отримані показники безпеки свідчать про їх невисокий рівень. Тобто для розвитку сфери безпеки є потреба у залученні коштів для забезпечення змін не тільки на рівні стратегії інформаційної безпеки, але й на рівні її окремих складових – рівня технологічного розвитку, впровадження нових комп'ютерних програм, зміни стандартів, реформування законодавства, тощо.

До 5-го кластеру увійшли 29 країн: Алжир, Бутан, Болівія, Китай, Кот-д'Івуар, Куба, Домініканська республіка, Еквадор, Єгипет, Ель Сальвадор, Гана, Гватемала, Індія, Індонезія, Іран, Кенія, Киргизстан, Панама, Парагвай, Перу, Філіппіни, Руанда, Сан Кітс и Невіс, Сенегал, Тринідад і Тобаго, Туніс, Узбекистан, Венесуела, В'єтнам. Даний кластер сформували країни, які розвиваються, але мають низькі показники розвитку та низький рівень інформаційної безпеки (див. рис. 3.9 та табл. 3.1). Хоча до даного кластеру увійшли також й країни, які є новими індустріальними, - Індія, Індонезія, Китай, Філіппіни, але й вони мають досить низький рівень безпеки, що дозволило віднести їх до даної групи. Головними проблемами цього кластеру є передусім вирішення питань, пов'язаних із економічним розвитком, але ці країни мають відповідний потенціал для розвитку й інформаційної безпеки. Про це свідчить їх достатній рівень розвитку інформаційних технологій, цифровізації різних сфер та технологічної готовності.

До 6-го кластеру увійшла 51 країна, які відносяться до групи найменш розвинутих країн, що характеризуються дуже низькими показниками розвитку економіки, соціальної та політичної сфери (див. рис. 3.9 та табл. 3.1). Більшість країн даного кластеру – це країни Африки та Близького Сходу, де тривають озброєні конфлікти. Для таких країн першочерговим є подолання конфліктів у суспільстві та розвиток економіки. Для підвищення рівня їх інформаційної безпеки їм необхідно долучатися до програм та стартапів, які сприятимуть припливу інвестицій та зміни програмно-технічної інфраструктури на мікро-рівні, а потім й на рівні держави.

Проблеми, пов'язані із інформаційною безпекою, є досить актуальними у світі, тому дійсно є потреба у проведенні аналізу країн на предмет відповідності їх рівня розвитку рівню інформаційної безпеки. Це дозволить виділити не тільки групи країн, які слабко розвиваються у напрямку підвищення ефективності системи інформаційної безпеки, але й виділити ті сфери, які потребують додаткової уваги з боку відповідних державних органів, які займаються питаннями безпеки країни. Одним із дієвих інструментів для проведення такого

аналізу є самоорганізовані карти Кохонена, які дозволяють не тільки зробити візуалізацію кластерів, але й детально проаналізувати отримані профілі у відповідності із досліджуваними показниками.

В результаті проведеного кластерного аналізу та побудови карт Кохонена для 159 країн світу із використанням показників розвитку та інформаційної безпеки, було отримано 7 кластерів країн. Кожна країна однієї групи характеризується близьким рівнем розвитку та інформаційної безпеки. Так, країни 0-го та 1-го кластеру характеризуються найвищими показниками розвитку та безпеки, країни 2-го кластеру мають показники вище середнього, країни 3-го кластеру можна охарактеризувати, як країни із середнім рівнем розвитку та інформаційної безпеки, країни 4-го кластеру відповідають нижче середнього рівню, рівень розвитку та інформаційної безпеки 5-го кластеру можна охарактеризувати як низький, 6-го – дуже низький. Експериментальне дослідження із зміною різних опцій налаштувань нейронної мережі та аналізом матриць помилок квантування, щільності попадання та відстаней дозволило визначити розподіл даних на 7 кластерів, як найбільш ефективним.

Пункт 3.1.2 даного звіту було виконано із використанням матеріалів публікацій виконавців [186, 190].

3.1.3 Стратегія визначення рейтингу країн за рівнем кібербезпеки

Стрімкий розвиток новітніх інформаційних технологій, комп’ютеризація та діджиталізація багатьох сфер діяльності суспільства призвели до збільшення рівня кіберзлочинності у світі. Це проявляється у здійсненні масових хакерських атак, в результаті яких компанії втрачають велику кількість інформації, що стосується клієнтів, фінансових транзакцій, секретних даних. Також збільшилася кількість вірусних повідомлень, дія яких призводить до порушення роботи програмного, технічного забезпечення. Регулярно з’являються нові способи

кібершахрайства, які націлені на отримання різного роду інформації від користувачів. Кіберзлочинці почали втручатися й у роботу державних органів, що призводить до появи кібервійн між державами, виникнення інформаційних криз, тощо. Дана проблема набула масштабного характеру, що потребує розробки та впровадження більш ефективних рішень боротьби на рівні держави.

Одним з таких напрямків є формування ефективної стратегії кібербезпеки країни, яка повинна включати систему заходів, пов’язаних із організацією відповідних інститутів та органів, діяльність яких спрямована на забезпечення кіберзахисту. Стратегія повинна також охоплювати напрямки: формування політики кібербезпеки, розробки відповідної законодавчої бази, освітніх програм, системи відповідальності за кіберзлочини, інвестування у наукові дослідження з питань кіберзахисту, розробки потужних кіберфізичних комплексів, програмного забезпечення для моніторингу, попередження та виявлення кіберзлочинів, тощо. В процесі розробки стратегії важливо розуміти, які аспекти кібербезпеки країни потребують покращення та посилення, а які вже мають потужний базис та вимагають підтримки. Це можливо оцінити в процесі визначення рейтингу країн, який формується за рівнем кібербезпеки.

Існує ряд показників, які застосовуються для рейтингування країн, серед яких виділяється National Cybersecurity Index, який дозволяє оцінити рівень готовності країн протидіяти кіберзагрозам. Для його розрахунку використовується ряд показників, які стосуються різних аспектів кібербезпеки: правової, організаційної, технічної, освітньої, тощо. Після отримання їх оцінок відбувається розрахунок узагальненого показника, що здійснюється шляхом знаходження долі сумарної оцінки для країни від сумарної максимальної оцінки. Але даний підхід не враховує важливості показників в процесі формування загального рейтингу, не реагує на випадки, коли вони мають різну амплітуду значень, а також не передбачає використання додаткових характеристик, які б допомогли чітко бачити відхилення від фактичних максимальних оцінок. Тому застосування різних підходів, таких як, наприклад, багатокритеріальний аналіз рішень, дозволить проводити оцінку рейтингів більш зважено, оскільки вони

нівелюють згадані недоліки. Хоча дані методи застосовуються в процесі вибору та прийняття рішень, але вони дозволяють ефективно оцінити об’єкти дослідження. Вибір методу оцінки може значно вплинути на формування стратегії кібербезпеки для країни, тому треба врахувати результативність методу та його додаткові можливості.

Важливим напрямком у розвитку кібербезпеки країни є використання сучасних методів та інструментів, які спрямовані на підвищення її ефективності. Так, увагу VIKOR-методології щодо її можливостей оцінки для вибору методів поводження з відходами та місця для встановлення ТЕЦ було приділено авторами у праці [191]. Ghaleb A. M., Kaid H., Alsamhan A., Mian S. H. та Hidri L. провели порівняльний аналіз MCDM підходів для вибору виробничих процесів [192]. Mardani A., Zavadskas E.K., Govindan K., Amat Senin A. та Jusoh, A. дослідили можливості застосування VIKOR техніки у таких галузях, як стійкість та відновлювальна енергія [193]. Suniantara I. K. P. та Putra I. G. E. W. провели порівняльну характеристику методів VIKOR та TOPSIS з метою вибору значних змінних процесу щодо змінних реакцій яскравості та болючості у процесі виготовлення конвертів [194]. Chatterjeea P. та Chakraborty S. провели оцінку ефективності абразивних матеріалів на основі семи критеріїв, в ході чого було застосовано метод VIKOR та його різні модифікації [195]. Тобто багатокритеріальні методи прийняття рішень є широко уживаними не залежно від об’єкту дослідження, тому їх можна використовувати для рейтингування країн щодо рівня їх кібербезпеки.

Таким чином, не зважаючи на значний науковий доробок для вирішення проблематики кібербезпеки, є ряд питань, які досить слабко представлені науковими працями фахівців. Це стосується й розвитку напрямку розробки ефективної системи оцінювання країн за рівнем їх кібербезпеки, що сприятиме виробленню потужної національної стратегії країни у майбутньому.

Для проведення дослідження було узято 12 показників, які характеризують різні аспекти кібербезпеки країни, використовуються для визначення National

Cybersecurity Index та відповідного рейтингу країни. Так, базу емпіричних даних сформували [196]:

1) Cyber Security Policy Development характеризує загальний рівень політики кібербезпеки у країні, що проявляється у створенні відповідних груп та союзів з цього питання, забезпеченні їх координації, розробці стратегії та плану реалізації кібербезпеки;

2) Cyber Threat Analysis and Information відображає напрямки, пов'язані із формуванням інформаційного забезпечення з питань кібербезпеки, куди входить щорічне звітування про кіберзагрози у світі та розробка спеціальних веб-ресурсів, а також напрямки щодо створення та розвитку спеціалізованих аналітичних груп, які регулярно здійснюють аналіз стану кібербезпеки у світі;

3) Education and Professional Development характеризує рівень освіти у галузі кібербезпеки, що проявляється у визначенні компетенцій з цього напрямку для різних рівнів освіти: початкової, середньої, бакалаврату, магістра, PhD, а також передбачає створення професійної асоціації кібербезпеки, яка охоплює провідних фахівців з вирішення даної проблеми;

4) Contribution to global cyber security відображає напрямки, пов'язані із діяльністю країни на глобальному рівні щодо формування її внеску у розробку Конвенції про кіберзлочинність, міжнародних представництв, організацій з кібербезпеки, а також щодо формування можливостей нарощування потенціалу кібербезпеки для інших країн;

5) Protection of digital services передбачає оцінку дій країни щодо забезпечення відповідальності для постачальників цифрових послуг, розробки стандартів кібербезпеки для державного сектору та формування спеціальних компетентних наглядових органів;

6) Protection of essential services характеризує заходи країни щодо визначення операторів основних служб, розробки вимог до них, створення компетентного наглядового органу у цій сфері, здійснення регулярного моніторингу заходів безпеки в процесі здійснення основних послуг;

7) E-identification and trust services відображає дії держави щодо створення унікальних ідентифікаторів, компетентних наглядових органів, розробки вимог до криптосистем, електронної ідентифікації та підпису;

8) Protection of personal data стосується напрямків, пов’язані із формуванням ефективного законодавства в частині захисту персональних даних, та створенням відповідних органів;

9) Cyber incidents response передбачає дії країни щодо формування спеціальних підрозділів реагування на кіберінциденти, єдиної контактної точки для міжнародної координації, розробки системи відповідальності за звітування щодо випадків кіберзлочинів;

10) Cyber crisis management включає питання, пов’язані із формуванням плану управління кіберкризисними ситуаціями на національному рівні; участю у міжнародних навчаннях з кіберкризи; оперативною підтримкою волонтерів під час кіберкризи;

11) Fight against cybercrime характеризує аспекти діяльності спеціалізованих підрозділів з питань кіберзлочинності, цифрової криміналістики, контактної точки з питань міжнародної кіберзлочинності;

12) Military cyber operations стосується напрямків щодо здійснення спеціалізованих кібер-операцій та участі країни у міжнародних кібернетичних навчаннях.

Дані показників було узято для 160 країн світу за 2018 рік [196]. Всі значення вимірюються у однакових величинах від 0 до 10 та представляють собою оцінки, які надаються кожній країні на основі наданої нею інформації.

Для проведення дослідження було обрано Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS), яка відноситься до класу розв’язання багатокритеріальних задач та яку було розроблено Ching-Lai Hwang та Yoon у 1981 [197]. У наступних роках дана методика набула подальшого розвитку та удосконалення. Її основна ідея полягає у визначенні двох альтернатив, одна з яких має найменшу геометричну відстань до позитивного ідеального рішення, а інша має найбільшу геометричну відстань до від’ємного ідеального рішення. Як

результат, методика дозволяє визначити відносну відстань до ідеального рішення, що сприяє отриманню загальної оцінки для кожної альтернативи, яка може виступити у якості її рейтингу. TOPSIS передбачає виконання наступних етапів.

На першому етапі створюється матриця з m-альтернатив та n-критеріїв. У якості альтернативи обираємо країни, для яких необхідно визначити рейтинг. У якості показників виступатимуть індекси кібербезпеки.

На другому етапі визначаються нормалізовані значення показників кібербезпеки. Початкові дані приводяться до безрозмірних величин, тобто нормалізуються, оскільки їх значення можуть бути неспівставними. Для цього кроку використовується формула 3.4:

$$u_{ij} = \frac{a_{ij}}{\sqrt{\sum_{j=1}^{n} a_{ij}^2}}, \tag{3.4}$$

де u_{ij} – нормалізовані значення окремих j-их показників кібербезпеки для i-ої країни ($i = 1 \div m$; $j = 1 \div n$);

m – кількість альтернатив, у нашому випадку дорівнює кількості країн ($m = 160$);

n – кількість цільових функцій, які дорівнюють кількості показників кібербезпеки ($n = 12$);

a_{ij} – фактичне значення окремого j-ого показника кібербезпеки для i-ої країни.

На третьому етапі визначається зважена нормалізована матриця рішень, в якій враховується вага окремого показника для прийняття рішення щодо рейтингу країни (формула 3.5):

$$x_{ij} = w_j \cdot u_{ij}, \tag{3.5}$$

де x_{ij} – зважені нормалізовані значення окремих j-их показників кібербезпеки для i-ої країни ($i = 1 \div m$; $j = 1 \div n$);

w_j – вага кожної j-ої цільової функції, яка відображає значимість показника кібербезпеки для загального рейтингу країни, при чому $\sum_{j=1}^{n} w_j = 1$. У нашому випадку вагу було визначено як долю нормативного значення j-го показника у їх сумарній оцінці(формула 3.6):

$$w_j = \frac{w_j^*}{\sum_{j=1}^{n} w_j^*}, \tag{3.6}$$

де w_j^* – нормативна оцінка j-го показника кібербезпеки.

На четвертому етапі визначається позитивне та від'ємне ідеальне рішення, тобто визначається країна, яка має найвищий рівень кібербезпеки, та країна з найгіршими показниками (формули 3.7-3.8):

$$A^+ = \{x_1^+, \dots, x_n^+\},$$
$$x_j^+ = \left\{\max_i x_{ij} | j \in C_j(max); \min_i x_{ij} | j \in C_j(min)\right\}, \tag{3.7}$$

$$A^- = \{x_1^-, \dots, x_n^-\},$$
$$x_j^- = \left\{\min_i x_{ij} | j \in C_j(min); \max_i x_{ij} | j \in C_j(max)\right\}, \tag{3.8}$$

де A^+ та A^- – відповідно найкраща та найгірша альтернативи або позитивне та від'ємне ідеальне рішення, які представлені набором показників кібербезпеки;

x_j^+ – розраховані максимальні значення для тих критеріїв, які позитивно впливають на формування найкращої альтернативи, або мінімальні значення, які також здійснюють позитивний вплив;

x_j^- – розраховані мінімальні значення для тих критеріїв, які негативно впливають на формування найгіршої альтернативи, або максимальні значення, які також здійснюють негативний вплив;

C_j – сукупність значень для j-ого показника кібербезпеки.

На п’ятому етапі проводиться оцінка відстаней для кожної країни до ідеальної альтернативи. Відстань до найкращої (позитивної) альтернативи розраховується за формулою 3.9 та її значення для конкретної i-ої країни показує, що чим воно менше, тим ближче дана країна до ідеальних значень показників безпеки, а її рейтинг буде вищим. Відстань до найгіршої (від’ємної) альтернативи визначається за формулою 3.10 та її значення свідчить, що чим воно менше, тим ближче країна знаходиться до найгіршого варіанту, тобто вона матиме низький рейтинг за рівнем кібербезпеки.

$$S_i^+ = \sqrt{\sum_{j=1}^{n} \left(x_{ij} - x_j^+\right)^2}, \tag{3.9}$$

$$S_i^- = \sqrt{\sum_{j=1}^{n} \left(x_{ij} - x_j^-\right)^2}, \tag{3.10}$$

де S_i^+ – відстань показників країни до найкращої (позитивної) альтернативи;

S_i^- – відстань показників країни до найгіршої (від’ємної) альтернативи.

На шостому етапі здійснюється розрахунок відносної відстані до ідеальної альтернативи, що передбачає визначення подібності значень критеріїв для кожної i-ої країни із найгіршим станом (формула 3.11):

$$Q_i = \frac{S_i^-}{S_i^+ + S_i^-} \tag{3.11}$$

Якщо отримане значення Q_i наближається до 1, то це говорить про те, що i-та країна має найкращу комбінацію показників кібербезпеки, яка є близькою до ідеальної комбінації. Якщо значення Q_i наближається до 0, то це свідчить про

найгіршу комбінацію показників кібербезпеки та дана країна буде мати досить низький рейтинг.

На сьомому етапі проводиться оцінка рейтингу шляхом визначення рангу для розрахованих значень. З цією метою проводиться ранжування країн за отриманим показником Q_i у порядку його убування. Далі їм надається порядковий номер у ряді. Якщо значення Q_i однакові, то для розраховується стандартизований ранг, як середньоарифметичне значення порядкових номерів для однакових Q_i. Для перевірки правильності отриманих рангів необхідно знайти їх суму для всього ряду та дане значення порівняти із $N \cdot (N + 1)/2$, де N – це кількість країн у ряді, тобто 160.

Наступний метод, який було обрано для проведення розрахунків, це original VIKOR (Vlse Kriterijumska Optimizacija Kompromisno Resenje, in Serbian), який означає багатокритеріальну оптимізацію та компромісне рішення. Він був запропонований у 1979 році сербським вченим S. Opricovic, але міжнародного визнання його класичний варіант набув у публікації [198]. Суть методу полягає у знаходженні багатокритеріальної оцінки, яка знаходиться як міра відносної близькості до ідеального компромісного рішення. VIKOR має декілька модифікацій, а саме comprehensive VIKOR, fuzzy VIKOR, regret theory-based VIKOR, modified VIKOR та interval VIKOR, але для типових задач найкращим є original VIKOR, що доведено у [195]. Реалізація даного методу передбачає виконання наступних етапів.

На першому етапі створюється матриця альтернатив та критеріїв, яка є аналогічною матриці, створеною за методом TOPSIS.

На другому етапі проводиться нормалізація початкових показників кібербезпеки, представлених у вигляді матриці. Але при цьому враховується факт впливу показника. Якщо його значення здійснює позитивний вплив, тобто є стимулятором, то нормалізація проводиться за формулою 3.12, якщо показник впливає негативно (є дестимулятором), то нормалізація відбувається за формулою 3.13.

$$x_{ij} = w_j \cdot \frac{a_j^{max} - a_{ij}}{a_j^{max} - a_j^{min}}, \quad (3.12)$$

$$x_{ij} = w_j \cdot \frac{a_{ij} - a_j^{min}}{a_j^{max} - a_j^{min}}, \quad (3.13)$$

де x_{ij} – нормалізоване значення j-ого показника кібербезпеки для i-ої країни ($i = 1 \div m$; $j = 1 \div n$);

w_j – вага кожного j-ого показника кібербезпеки, яка відображає його значимість для загального рейтингу країни, при чому $\sum_{j=1}^{n} w_j = 1$;

a_{ij} – фактичне значення j-ого показника кібербезпеки для i-ої країни;

a_j^{max} – максимальне значення j-ого показника кібербезпеки;

a_j^{min} – мінімальне значення j-ого показника кібербезпеки.

Оскільки всі показники кібербезпеки є стимуляторами, то для їх нормалізації використовуємо формулу 3.12. Підхід до визначення вагів використовуємо аналогічно до того, який застосовувався у методі TOPSIS.

На третьому етапі розраховуємо зважену та нормовану відстань Манхеттена (S_i) за формулою 3.14, а також зважену та нормовану відстань Чебишева (R_i) за формулою 3.15.

$$S_i = \sum_{j=1}^{n} x_{ij}, \quad (3.14)$$

$$R_i = \max_i x_{ij}. \quad (3.15)$$

На четвертому кроці обчислюється оцінка відстані для i-ої країни до ідеального рішення, тобто оптимальної комбінації показників кібербезпеки (формула 3.16):

$$Q_i = v \cdot \frac{S_i - S^-}{S^+ - S^-} + (1 - v) \cdot \frac{R_i - R^-}{R^+ - R^-}, \quad (3.16)$$

де Q_i – оцінка відстані для i-ої країни до ідеального рішення, значення якої знаходиться в межах від 0 до 1. Чим ближче вона до 0, ти ближче відстань для i-ої країни до ідеального рішення. Якщо оцінка наближається до 1, то параметри країни значно віддаляються від ідеального рішення;

S^-, S^+ – розраховуються за формулою 3.17:

$$S^- = \min_i S_i, S^+ = \max_i S_i ; \quad (3.17)$$

R^-, R^+ – розраховуються за формулою 3.18:

$$R^- = \min_i R_i, R^+ = \max_i R_i \quad (3.18)$$

v – це вага стратегії більшості атрибутів або групової корисності, значення якої знаходиться в межах від 0 до 1. Найбільша перевага надається значенню 0,5, яке показує збалансованість при прийнятті рішення. Якщо воно дорівнює 1, то мова йде про стратегію максимізації групової корисності, якщо 0, то про стратегію мінімізації індивідуального співчуття, тобто знаходиться мінімальне значення критерію для кожної альтернативи серед максимальних індивідуальних відхилень від ідеального значення.

На п’ятому етапі здійснюється ранжування для отриманих оцінок з метою визначення рейтингу країни аналогічно до процесу ранжування, описаному в методі TOPSIS.

Третій метод, який використовується у дослідженні, це Multi-attribute Attitude Model (MAAM), яка заснована на моделі Фішбейна, що була запропонована у 1963 році [199]. Її суть полягає у визначенні відношень споживачів до конкретного продукту в залежності від оцінок його атрибутів. Відповідно до умов даного дослідження відбуватиметься оцінка показників

кібербезпеки для кожної країни з метою виділення найслабших та найсильніших країн щодо створених ними умов забезпечення відповідного рівня безпеки. Метод є дуже простим у реалізації й передбачає здійснення наступних кроків.

Перший етап здійснюється аналогічно, як й за методами TOPSIS та VIKOR.

На другому етапі визначається оцінка загального рівня кібербезпеки за допомогою формули 3.19:

$$Q_i = \sum_{j=1}^{n} w_j \cdot a_{ij}, \tag{3.19}$$

де Q_i – оцінка загального рівня кібербезпеки для i-ої країни;

w_j – вага кожного j-ого показника кібербезпеки, яка відображає його значимість ($\sum_{j=1}^{n} w_j = 1$);

a_{ij} – фактичне значення j-ого показника кібербезпеки для i-ої країни.

Третій етап присвячується розрахунку рейтингу для i-ої країни, який здійснюється аналогічно до методів TOPSIS та VIKOR.

Розрахунки здійснювалися за допомогою програми Microsoft Office Excel. В результаті було отримано рейтинги країн за рівнем кібербезпеки, які було отримано за трьома методами. Фрагмент отриманих результатів представлено в таблиці 3.2. Розрахунок за методом VIKOR відбувався з урахуванням ваги групової корисності 1 та 0.5. При v=0 результати рейтингів виявилися неадекватними.

Для отримання адекватної оцінки, було проведено порівняння отриманих рейтингів із фактичним значенням рейтингу, сформованого за National Cbersecurity Index, значення якого наводиться у таблиці 3.2. Для проведення аналізу було знайдено різницю між фактичним значенням рейтингу та розрахованим. На рисунку 3.11 представлено різницю, отриману в результаті порівняння рейтингу за методом TOPSIS та фактичним значенням.

Таблиця 3.2 – Результати розрахунків рейтингів країн за методами TOPSIS, MAAM, VIKOR (фрагмент)

№	Country	Real Rank	TOPSIS	MAAM	VIKOR	
					v=1	v=0.5
1	Afghanistan	131	134	130.5	133.5	135
2	Albania	68	71	70.5	67	90
3	Algeria	122	122	122	124	128.5
4	Angola	144	144	148.5	145.5	146
5	Antigua and Barbuda	136	141	141	133.5	135
6	Argentina	55	52	57	54.5	49
7	Armenia	91	84	81	89	84
8	Australia	36	37	37	35.5	64
9	Austria	23	24	19.5	23	20
10	Azerbaijan	80	79	79	82	79
11	Bahamas	103	105	101	102	104.5
12	Bahrain	100	104	100	100	91
13	Bangladesh	92	94	96	94	102
14	Barbados	121	130	117.5	119	101
15	Belarus	46	40	43	45.5	33
16	Belgium	5	4	5	5	7
17	Belize	152	150	151.5	151	151
18	Benin	57	58	58	58.5	63
19	Bhutan	115	114	117.5	114.5	123.5
…	…	…	…	…	…	…
142	Tonga	100	101	105.5	102	119
143	Trinidad and Tobago	115	108	108	107.5	108
144	Tunisia	88	90	92.5	89	99.5
145	Turkey	69	65	68.5	67	54
146	Turkmenistan	159	155	154	154	154
147	Tuvalu	156.5	159	157.5	157.5	157.5
148	Uganda	48	48	50	49	45
149	Ukraine	29	34	24	28.5	27
150	United Arab Emirates	71	68	62	70.5	57
151	United Kingdom	14	11	12	14	11
152	United States	27	20	30.5	28.5	61
153	Uruguay	56	55	56	54.5	62
154	Uzbekistan	89	85	88	89	99.5
155	Vanuatu	138	142	142	140	141
156	Venezuela	85	82	77	85	81.5
157	Vietnam	81	73	89	80	96
158	Yemen	148	147	147	148	148
159	Zambia	66	66	67	67	71
160	Zimbabwe	118	119	115	119	112

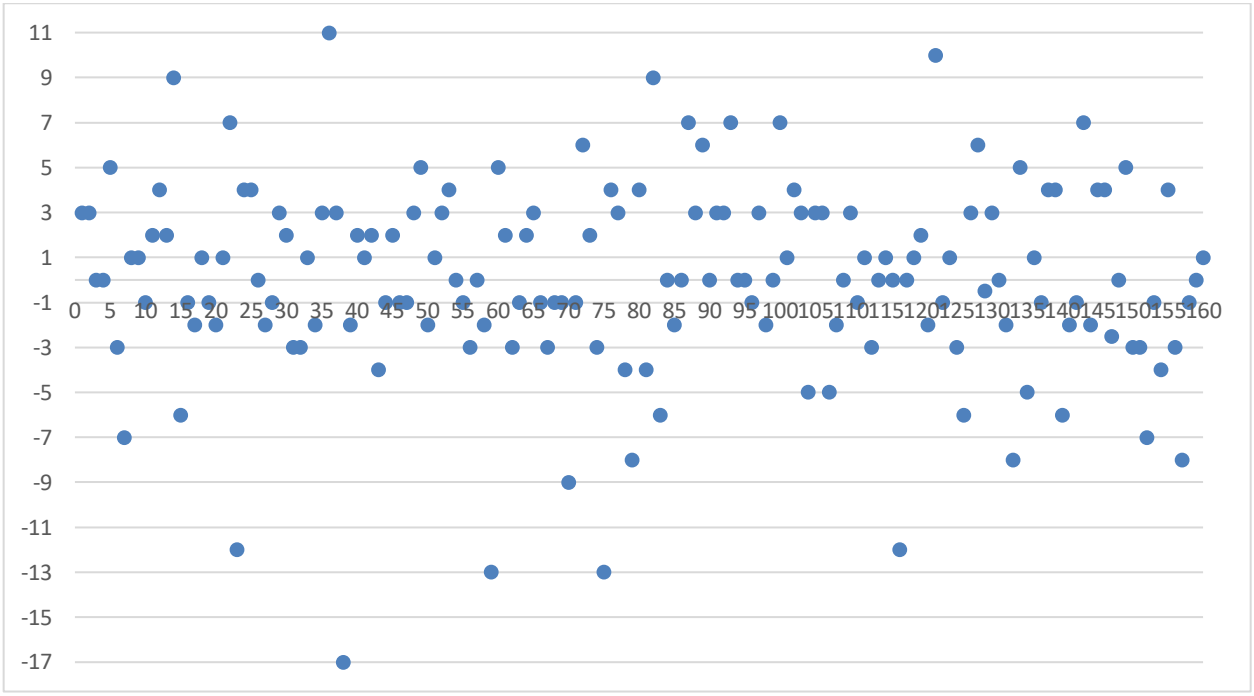


Рисунок 3.11 – Різниця, отримана в результаті порівняння рейтингу за методом TOPSIS та фактичним значенням

На рисунку 3.11 можна побачити, що відхилення між фактичним значенням та розрахованим за методом TOPSIS знаходиться від -17 до 11 позицій, що говорить значний розкид у значеннях. Тільки для 18 країн рейтинги співпали, що складає тільки 11.25% від загального обсягу країн. Оскільки підхід до визначення фактичного рейтингу не враховує багатьох аспектів, таких як важливість показників кібербезпеки, оцінка відхилення значень для країни по різних показниках, визначення кращої або гіршої альтернативи, то можна сказати, що отримані результати рейтингу за методом TOPSIS доцільно використовувати з позиції розробки стратегії знаходження сильних та слабких місць в кібербезпеці країни. З цією метою будується пелюсткова діаграма, яка дозволяє провести такий аналіз (рисунок 3.12).

На рисунку 3.12 представлена найкраща (позитивна) альтернатива, найгірша (від'ємна) альтернатива, альтернативне рішення для Естонії, яка займає 1-е місце в отриманому рейтингу, альтернатива для України – країни із середнім рейтингом, рішення для Південного Судану – країни, що займає останнє місце в

рейтингу. Оскільки усі значення від'ємної альтернативи дорівнюють 0, то візуально на графіку вона відображається у вигляді крапки.

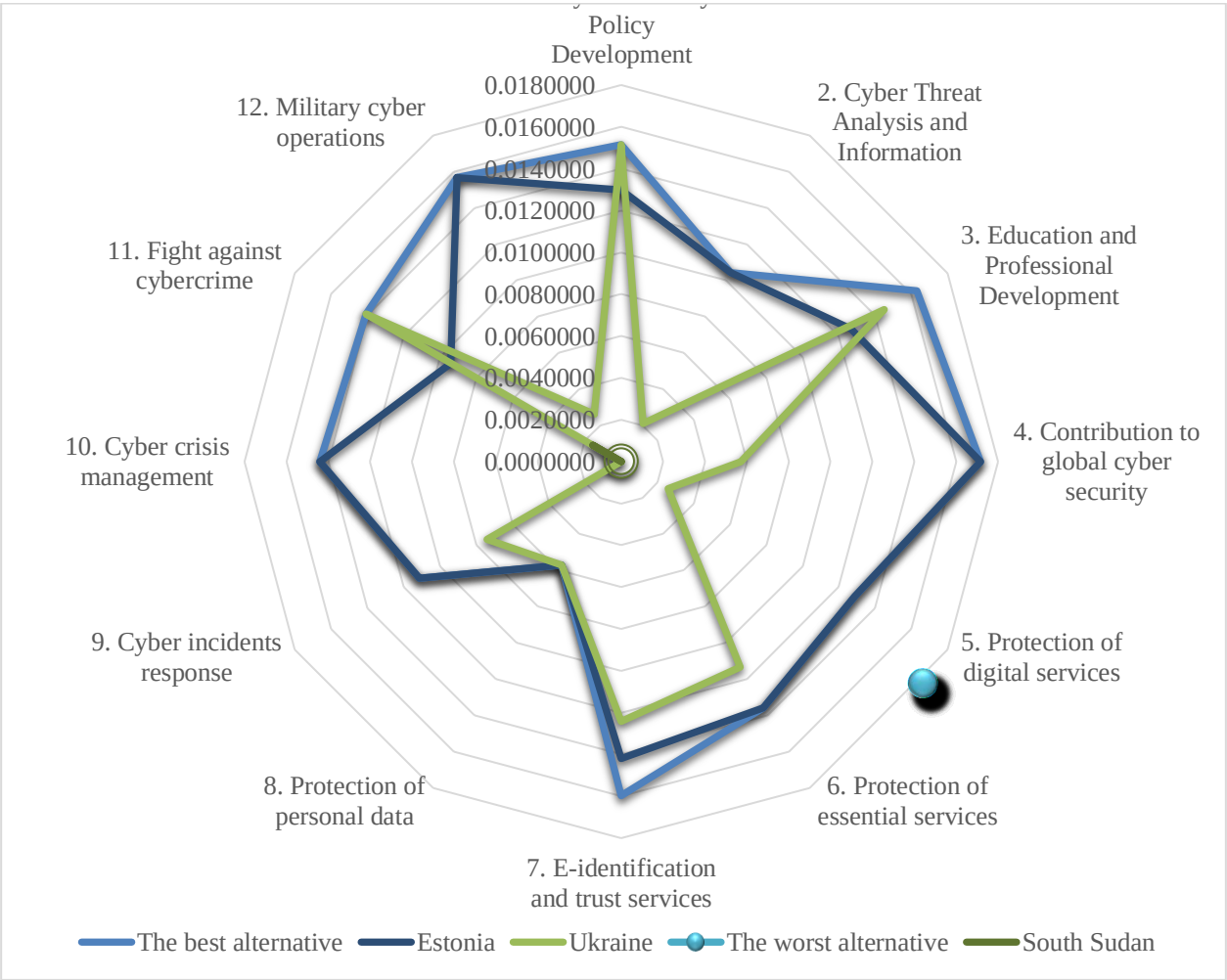


Рисунок 3.12 – Діаграма альтернатив рішень для країн

Аналізуючи показники для Естонії, можна побачити, що даній країні слід приділити більшу увагу розробці Cyber Security Policy, питанням Education and Professional Development, E-identification and trust services та Fight against cybercrime, оскільки їх значення відхиляються від найкращої (позитивної) альтернативи. Це говорить про існування певних проблем, які потребують удосконалення законодавчої бази, впровадження нових спеціальностей, пов'язаних із захистом інформації та кіберзахистом, модернізації технологій в галузі електронної ідентифікації, розробки більш дієвих організації, направлених на боротьбу з кіберзлочинами.

Результати для України представляють значний контраст, оскільки частина показників відповідають найкращій альтернативі або наближаються до неї, а частина інших прямують до значень найгіршої. Тобто спостерігаються проблеми, пов'язані із Cyber Threat Analysis and Information, Contribution to global cyber security, Protection of digital services, Protection of essential services, E-identification and trust services, Cyber incidents response, Cyber crisis management, Military cyber operations. При чому показник Cyber crisis management взагалі дорівнює 0, що свідчить про відсутність відповідних планів управління кібербезпекою, кіберкризами на національному рівні, оперативної підтримки волонтерів під час кіберкризи, участі у міжнародних навчаннях з питань кібербезпеки.

Що стосується результатів для Південного Судану, то фактично дана країна не забезпечує кібербезпеку для своїх громадян, підприємств та держави в цілому. Це пов'язано із історією становлення даної держави та постійними військовими конфліктами в середині. Відповідно сьогодні проблема кібербезпеки не є пріоритетною для неї.

Різниця, отримана в результаті порівняння фактичного рейтингу країни та рейтингу за методом VIKOR, представлена на рисунках 3.13 та 3.14.

Так, на рисунку 3.13 можна побачити розкид значень у межах від -3 до 3, що говорить про подібність результатів розрахункової оцінки рейтингів до фактичної. 40 країн мають оцінки, аналогічні до оцінок фактичного рейтингу, що складає 25% від загальної кількості. Оскільки для розрахунків використовувалося значення ваги групової корисності $v = 1$, коли відбувається його максимізація, то дані результати свідчать про позитивний погляд до сумарних оцінок рейтингу для країни. Результати розрахунків за збалансованим підходом, коли $v = 0.5$, представлені на рисунку 3.14, який показує різницю між оцінками з розкидом від -30.5 до +38. Кількість країн, які мають схожі оцінки, дорівнює 10, що складає 6.25%.

Рисунок 3.13 – Різниця, отримана в результаті порівняння рейтингу за методом VIKOR та фактичним значенням (v=1)

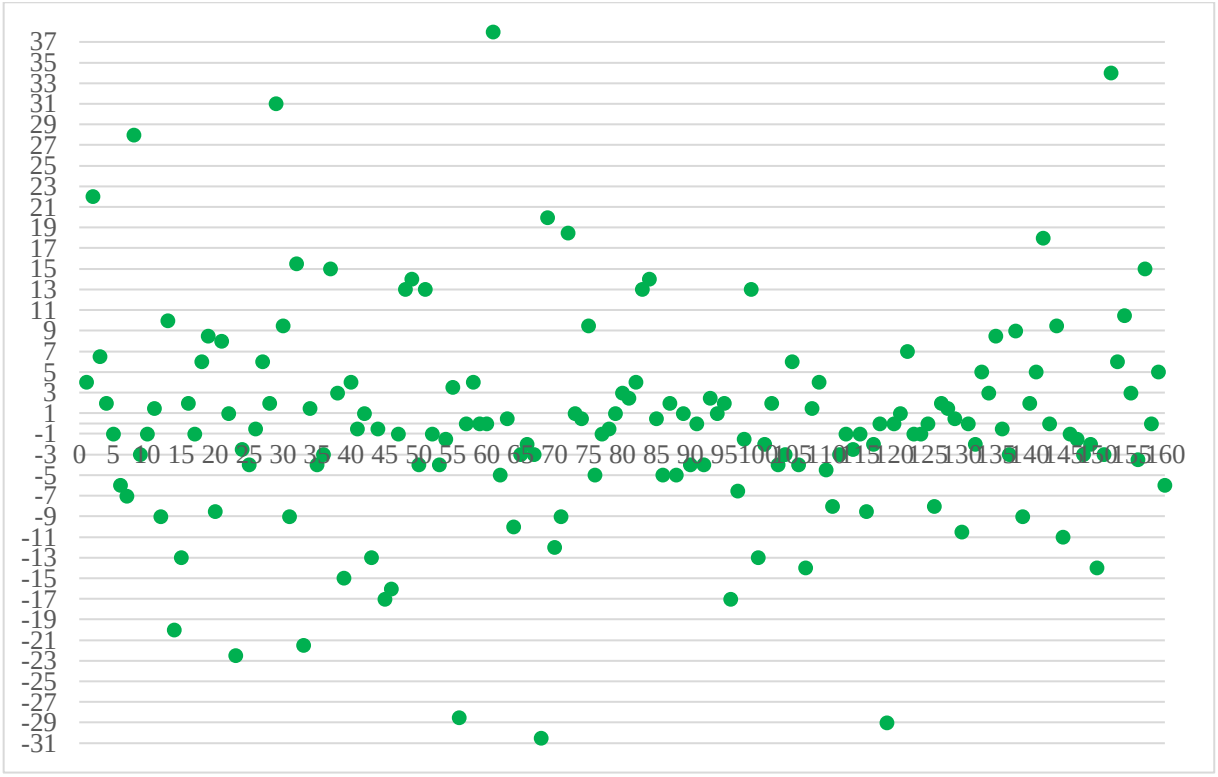


Рисунок 3.14 – Різниця, отримана в результаті порівняння рейтингу за методом VIKOR та фактичним значенням (v=0.5)

Рейтингування за методом VIKOR за умови, коли $v = 0.5$, доцільно у випадку знаходження компромісу за умовою використання суперечливих критеріїв. У випадку проведеного дослідження даний метод доцільно було б використати, якщо показники кібербезпеки мали б протилежні значення або здійснювали протилежний вплив на формування загальної оцінки.

Що стосується порівняння рейтингу, розрахованого за методом MAAM, із фактичним рейтингом, то отримані різниці представлені на рисунку 3.15.

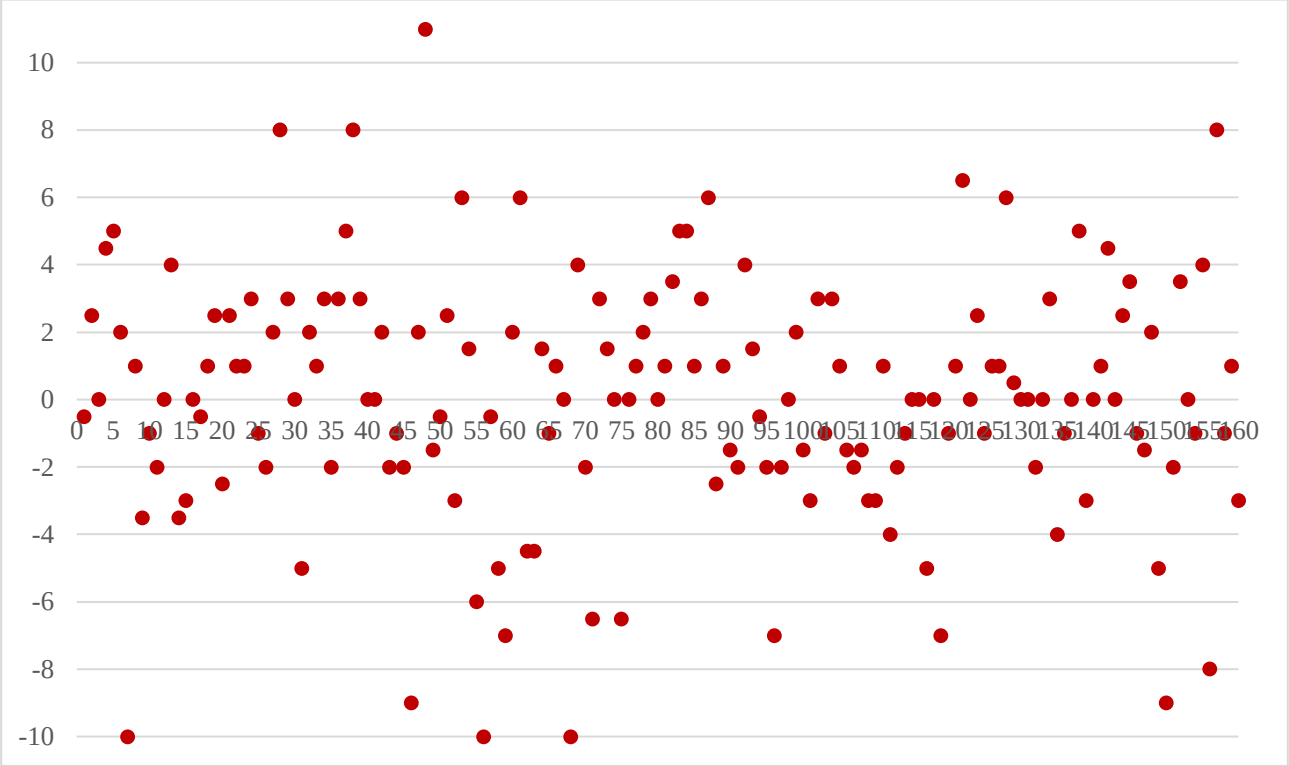


Рисунок 3.15 – Різниця, отримана в результаті порівняння рейтингу за методом MAAM та фактичним значенням

Результати порівняння, відображені на рисунку 3.15, показують, що різниця між оцінками коливається від -10 до +11, тобто результати є однаковими для 22 країн, що складає приблизно 13.75%. Також дані розбіжності близькі до тих, які були отримані при порівнянні фактичного рейтингу та оцінки за методом TOPSIS. Але даний метод не передбачає застосування нормалізації даних, що робить його не придатним для застосування у випадках, коли критерії мають різну розмірність.

На рисунку 3.16 представлені порівняння отриманих рейтингів для країн, які мають найнижчий показник (Південний Судан), найвищий результат (Чеська республіка та Естонія) та помірний результат (Україна).

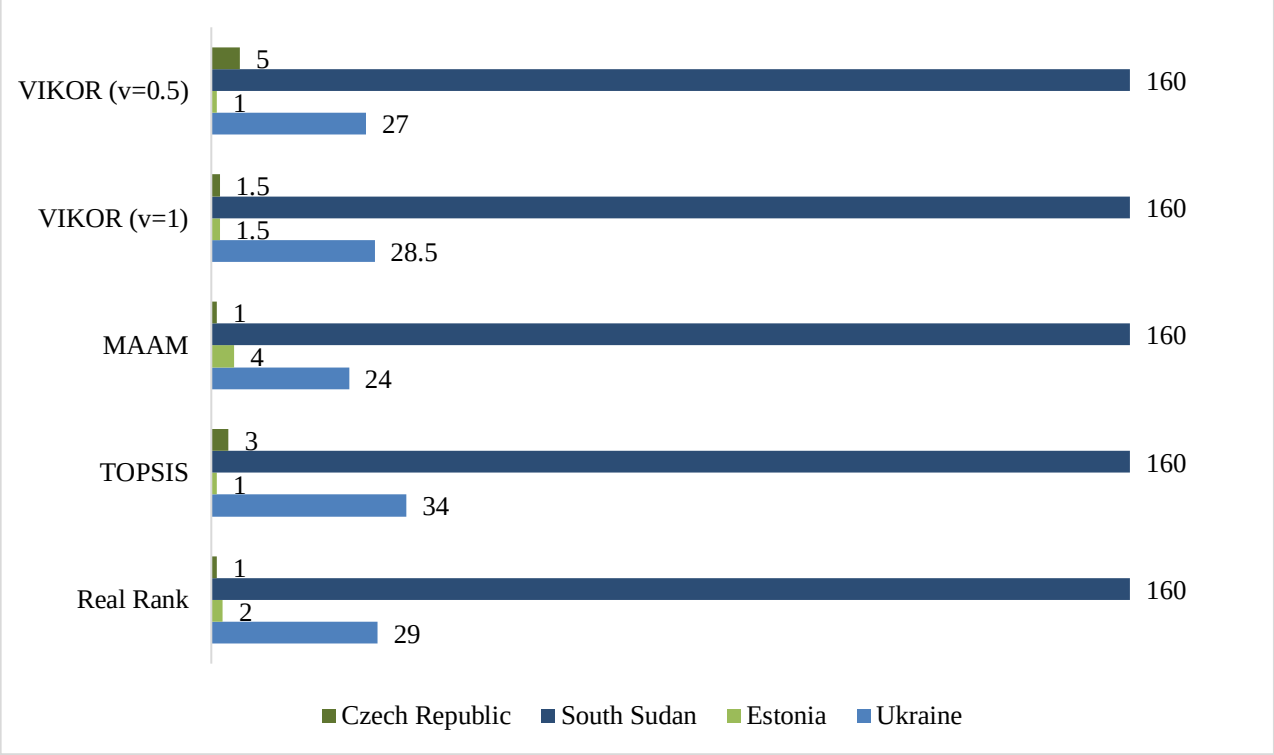


Рисунок 3.16 – Порівняння результатів рейтингових оцінок

Для порівняння було обрано країни із найкращими та найгіршими показниками. Так, у випадку із Південним Судам за всіма методами було отримано однакову рейтингову оцінку, яка також співпадає із фактичним рейтингом. Для України результати значно відрізняються, при чому за методом TOPSIS країну було оцінено більш критично, а за іншими методами вона отримала оцінки, вищі ніж реальний рейтинг. Що стосується Естонії та Чеської республіки, то вони є лідерами за різними методами, при чому їх оцінки коливаються в межах від 1 до 5 для Чеської республіки, та від 1 до 4 для Естонії. Можна прийти до висновку, що в залежності від стратегії рейтингування, можна обирати будь-який із приведених методів, але у випадку нерівномірного коливання значень критеріїв, їх результати будуть кардинально відрізнятися.

Проведемо перевірку ефективності застосовуваних методів шляхом розрахунку коефіцієнту рангової кореляції Спірмена за формулою 3.20, результати чого наведені у таблиці 3.3:

$$r = 1 - 6 \cdot \frac{\sum \left(d_x - d_y\right)^2}{n^3 - n}, \tag{3.20}$$

де r – коефіцієнт рангової кореляції Спірмена;

n – кількість спостережень;

d_x and d_y – пари співставних значень рангів.

Таблиця 3.3 – Значення коефіцієнта рангової кореляції Спірмена

	Real rating	TOPSIS	MAAM	VIKOR (v=1.0)	VIKOR(v=0.5)
Real rating	1	0.9956	0.9969	0.9997	0.9759
TOPSIS	–	1	0.9940	0.9958	0.9723
MAAM	–	–	1	0.9971	0.9817
VIKOR (v=1.0)	–	–	–	1	0.9764
VIKOR(v=0.5)	–	–	–	–	1

Отримані значення коефіцієнта кореляції наближаються до 1, що свідчить про високу ефективність отриманих результатів ранжування. Але метод VIKOR (v=0.5) надає нижчі результати ефективності у порівнянні із іншими методами. Інші методи мають досить рівнозначні оцінки, що говорить про високий рівень довіри до отриманих даних.

Питання визначення рейтингу країн за рівнем їх кібербезпеки є досить актуальним, оскільки сприяє отриманню адекватної оцінки країни щодо її можливостей протистояти кіберзагрозам. Застосування багатокритеріальних методів прийняття рішень дозволяє вирішити ряд проблем, пов’язаних із розмірністю даних, визначенням вагів показників, врахуванням різнонаправленості значень показників та їх кардинальних відмінностей. Саме тому використання подібних методів може стати альтернативою в процесі

визначення рейтингів в порівнянні із традиційними методами розрахунку, для яких характерні саме ці недоліки.

В роботі реалізовано методи TOPSIS, VIKOR and MAAM, які було застосовано для визначення рейтингу країн на основі оцінок показників, що характеризують окремі аспекти кібербезпеки. В результаті отримано, що рейтинги за методом MAAM мають близько 25% подібності із оцінками реального рейтингу країн. Це свідчить про низькі можливості даного методу, оскільки він також має ряд недоліків, як й оцінка реального рейтингу. Але головною превагою даного методи є простий алгоритм розрахунку. Найкращі результати продемонстрували методи TOPSIS та VIKOR, хоча VIKOR (v=0.5) виявив нижчу ефективність у порівнянні з іншими методами, про що свідчать отримані результати коефіцієнта рангової кореляції Спірмена. Отримані оцінки є збалансованими, що говорить про гарні можливості для застосування даного методу в процесі визначення рейтингу країн щодо рівня їх кібербезпеки. VIKOR (v=1.0) показав також відмінності від оцінок реального рейтингу, хоча різниці є найменшими у порівнянні з іншими методами. Оскільки вибір такого значення ваги свідчить про максимізацію групової корисності показників, що є доцільним у випадку вибору альтернатив. Але у випадку тільки оцінки рейтингу, цей фактор може значно впливати на результати, що є неприпустимим для здійснення оцінок окремої країни.

Метод TOPSIS є найбільш прийнятним для проведення рейтингування країн за рівнем кібербезпеки, оскільки він має високі показники ефективності, нівелює перелічені недоліки методів реальної оцінки, дозволяє визначати альтернативні стратегії на відміну від інших методів, які можна також використовувати для аналізу окремих показників. Тому вважаємо, що в умовах вирішення проблематики дослідження, даний метод дозволить не тільки отримати ефективні оцінки рейтингу, але допоможе визначити критичні показники для окремої країни, виявити держави з ідеальними альтернативами, що сприятиме вивченню їх досвіду щодо розробки стратегії кібербезпеки.

В процесі порівняння оцінок, розрахованих за різними методами, було виявлено, що країни Естонія та Чеська Республіка мають найвищі рейтинги та значення їх показників найбільше наближається до ідеальних. Тобто, доцільно звернути увагу на їх практику щодо формування стратегії кібербезпеки, особливо в частині тих показників, які для кожної окремої країни значно відхиляються від ідеальних та мають критичні значення. Країною із самим низьким рейтингом, що було підтверджено розрахунками за всіма методами, є Південний Судан. Оскільки вона має проблеми політичного, військового, соціально-економічного характеру, то це підтверджує відсутність пріоритету забезпечення її кіберзахисту.

Пункт 3.1.3 даного звіту було виконано із використанням матеріалів публікацій виконавців [200].

3.2 Визначення кількісного та якісного рівня ефективності роботи внутрішньобанківської системи кібербезпеки

На сьогоднішній день у функціонуванні світової економічної системи простежується кардинальна перебудова фінансової та, як її вагомої частини, банківської сфер. Банківська система по всім світовим країнам, незалежно від економічної моделі кожної держави та організації суспільних відносин, наразі відіграє одну з найважливіших ролей щодо забезпечення руху грошових потоків, так як вона приймає участь у виконанні головних функцій фінансової системи. А в теперішніх умовах глобалізації, інновацій, розвитку науково-технічного прогресу у банківський сфері виникають та загострюються ризики та загрози, пов’язані з обігом нелегальних коштів. На сучасному етапі процес розвитку економіки України передбачає необхідність адекватного виявлення новітніх ризиків і пошуку дієвих інструментів їх вимірювання, мінімізації та попередження. Досить специфічним ризиком у роботі банків виділяється ризик

використання банківських послуг для легалізації кримінальних доходів або фінансування тероризму.

Протягом останніх десяти років спостерігається суттєве пришвидшення еволюції все нових методів легалізації доходів, отриманих злочинним шляхом, що стають більш різноманітними та специфічними, а самі механізми представлення кримінальних доходів у вигляді доволі легальних прибутків ускладняються та диверсифікуються. А існуюча певна слабкість національних систем, суттєві прогалини у регулюванні фінансової системи, недосконаліть системи фінансового моніторингу, відсутність єдиного підходу до оцінки ризиків, сприяють успішній реалізації злочинних операцій, приховуванню справжніх джерел походження нелегальних коштів. Тому, питання оцінювання ризиків легалізації коштів, одержаних злочинним шляхом, потребує поглибленого вивчення, аналізу та розвитку.

Керівники усіх банківських установ наразі прагнуть удосконалити функціонування своєї організації шляхом найефективнішого та найраціональнішого використання ресурсів. Одним з найдієвіших способів ефективної реалізації фінансового моніторингу у банках за напрямом оцінювання ризиків легалізації коштів, одержаних злочинним шляхом, фінансування тероризму та розповсюдження зброї масового знищення, виступає усвідомлення банківськими робітниками принципів діяльності системи фінансового моніторингу, запровадження комплексної оцінки роботи такої системи на постійній основі. Таким чином, постає необхідність аналізу ефективності фінансового моніторингу банків в розрізі оцінювання ризиків легалізації коштів, одержаних злочинним шляхом із застосуванням новітніх методик.

Ризик виступає доволі складним та багатоаспектним явищем не лише в економіці, але й у інших сферах життєдіяльності суспільства. Це підтверджується різноманітністю точок зору на сутність поняття ризику, а також існуючими недоліками у законодавстві. В сучасній економічній літературі, поширення набули такі аспекти формалізації: ризик у якості економічної

категорії [201], ризик як явище або процес [202], непередбачуваність і можливість настання подій з негативними наслідками [203]. Більше того, в роботах науковців, таких як: Бунчук М. М. Глібчук В.М, Глущевський В.В. , Донець Л. І. , Васильєва Т. А, Кривич Я. М. ,. Ю. , Патюта І. М., Худокормова М. І. та інші [204, 205, 206, 207, 208, 209, 210] було проведено ідентифікацію існуючих ризиків, аналіз та методи їх оцінювання, фінансові механізми управління ризиком, описано сутність, класифікацію і характеристики економічних ризиків, подано методи оцінки ризиків і способи вибору з існуючих альтернатив оптимальних рішень, приведена система категорій факторів ризику та їх оцінка в процесах фінансового моніторингу банків України; важливим постає питання ідентифікації, контролю та мінімізації категорій ризиків, які мають негативний вплив на систему фінансового моніторингу в банках України; визначено джерела фінансування терористичної діяльності, можливі способи переміщення коштів терористичними угрупуваннями та напрямки наступного застосування таких коштів для фінансування тероризму; проаналізовано особливості оцінювання ризиків легалізації незаконних доходів суб’єктів первинного фінансового моніторингу.

Значна увага науковців, а саме: Журавель В. А , Ніколаюк С. І. , Погорецький М. А. , Сухонос В.В. та інші [211, 212, 213, 214] приділяється наступним питанням: механізми відмивання нелегальних коштів шляхом застосування незаконних схем грошових потоків, практична сторона контактування з офшорними зонами; обмін світовим досвідом протидії руйнівним наслідкам у роботі з офшорними зонами; новітні напрямки у застосуванні спеціальних знань та навичок при розслідуванні злочинів; врегулювання функціонування правоохоронних органів щодо розслідування легалізації (відмивання) коштів, одержаних злочинним шляхом.

Також, частина авторів: Філ Сеіб, Дана М.Джанбек, Антипенко В. Ф. , Богуцький П , Іващенко О. А. , Підюков П. П., Устименко Т. П., Осипенко Р. І., Грищук В. К. [215, 216, 217, 218, 219, 220] у своїх трактатах наголошують на необхідності: розв’язання проблеми тероризму в його різних аспектах;

узагальнюючому здійсненні аналізу характерних особливостей міжнародної терористичної діяльності; ідентифікації сьогоденних недоліків державної політики у частині протидії тероризму; оцінюванні терористичних злочинів та їх руйнівних наслідків; необхідності збільшення кримінальної відповідальності за фінансування та вчинення терористичних актів.

Серед досягнень правового характеру дослідниками , такими як: Гуржій С.Г., Копиленко О.Л., Янушевич Я.В., Бисага К. В.,. Чернадчук В.Д., Ковальчук А., Криштоф А. та ін.. [221, 222, 223, 224], зроблено наступне: розглянуто особливості регулювання та протидії легалізації коштів, отриманих злочинним шляхом; встановлено виникаючі проблемні питання протидії інвестування коштів у розповсюдження зброї масового знищення; надано певні пропозиції по удосконаленню нормативної бази; проаналізовано особливості ідентифікації злочинів легалізації (відмивання) доходів, одержаних незаконним шляхом, встановлено причини недостатньої дієвості сучасних існуючих методів боротьби з легалізацією та фінансуванням тероризму, приведено конкретні рекомендації щодо протидії відмивання нелегальних доходів.

Дослідження понять фінансовий моніторинг, легалізація кримінальних доходів та ефективність у взаємозв’язку в наявних літературних джерелах також проведено за допомогою побудови карти наукової бібліографії категорій «financial monitoring» (фінансовий моніторинг), «money laundering» (легалізація кримінальних доходів), «efficiency» (ефективність) за проміжок часу протягом п’яти останніх років, а саме з 2016р. по 2020р. у напряму таких галузей: в економіці, фінансах, управлінні, економетриці, бухгалтерському обліку, бізнесі, шляхом застосування програми VOSViewerv.1.6.10. Отримані результати дослідження наявної літератури показано у вигляді графіку (рисунок 3.17). Створення карти наукової бібліографії досліджуваних термінів ґрунтується на даних робіт, знайдених, відсортованих, побудованих у архіві трактатів бази Scopus.

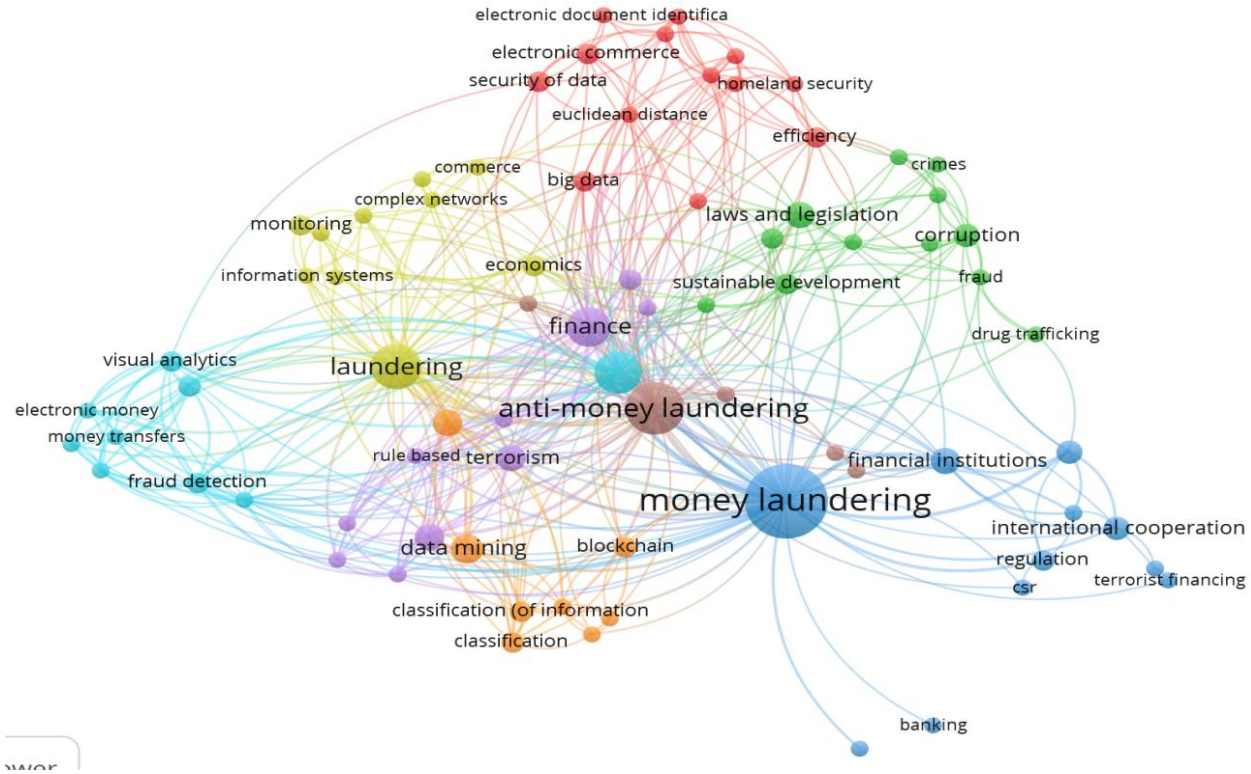


Рисунок 3.17 - Карта наукової бібліографії категорій «financial monitoring», «money laundering», «efficiency»

Наступний аналіз рисунку 3.17 дає змогу прийти до висновку, що вивчення питання ефективності фінансового моніторингу банків в розрізі оцінювання ризиків легалізації коштів, одержаних злочинним шляхом, на сьогоднішній день є особливо нагальним та актуальним , а підтвердженням цього виступає значна кількість трактатів науковців у цьому напрямі. Так, було визначено 8 окремих кластерів, що містять певні ключові слова, що відрізняються один від одного кольоровою гамою. Серед них, особливої уваги заслуговують кластери, що безпосереднє пов'язані з категоріями, такими як: протидія відмивання грошей, боротьба з фінансуванням тероризму, виявлення шахрайства, економічна та фінансова безпека, сталий розвиток, корупція, тощо.

Для розрахунку ефективності банківських установ України запропоновано використовувати програмне забезпечення Banxia Frontier Analyst 4. Згідно аналізу трактувань, що описують практичні аспекти вищевказаного ПЗ [225, 226, 227, 228], зазначено - Frontier Analyst є інструментом проведення аналізу ефективності Windows, що використовує в своїй основі технологію із назвою

Data Envelopment Analysis (DEA). Цей інструмент застосовується для вивчення та встановлення відносної ефективності визначених одиниць з аналогічними властивостями. В межах проведення аналізу відбувається ідентифікація входів і виходів, а змінні діляться на керовані та некеровані характеристики. Відповідне співвідношення виходів та входів обчислюється для усіх представлених змінних, при чому в кінці встановлюється результат проведеного оцінювання ефективності усіх одиниць вказаного аналізу. Далі передбачаються порівняльний процес , що є в такому випадку одноранговим, а майбутній потенціал поліпшень, запропонованих для неефективних одиниць аналізу, прогнозується у вигляді реалістичних та досяжних цифр. ПЗ Frontier Analyst допомагає здійснити порівняльний аналіз ефективності; розробити візуалізацію важливої інформації, що буде застосовуватись в подальших дослідженнях; проводити ефективніший розподіл наявних ресурсів; знаходити інформацію, потрібну для розроблення ефективної стратегії планування; визначати найгірші та найкращі елементи; проводити глибше дослідження показників і одиниць.

Певні питання, що виникають у цьому напрямку, наразі недостатньо та неповно розкриті в наявних літературних виданнях, і тому вимагають подальшого вивчення, дослідження та удосконалення. Так, базуючись на особливостях оцінки ефективності банківських установ України в частині національної системи оцінки ризиків легалізації доходів, отриманих нелегальним шляхом, фінансування тероризму та розповсюдження зброї масового знищення, постає потреба у виявленні чи розробці дієвого інструментарію економіко-математичного моделювання, що зможе допомогти не тільки здійснити групування банківських установ, а також і надати досить обґрунтовану оцінку поданого виду ризику, провести ідентифікацію визначених проблемних напрямків аналізу.

Для подальшого розвитку розглянутої проблематики пропонується науково-методичний підхід до оцінювання технічної ефективності фінансового моніторингу банків України на основі проведення фронтірного DEA-аналізу середовища функціонування шляхом побудови: 1) вхідно-орієнтованої BCC-

моделі задачі дробно-лінійного програмування мінімізації умовних входів (частка фінансових операцій, зареєстрованих за ознаками внутрішнього фінансового моніторингу; порушення ПП НБУ; порушення ЗУ "Про легалізацію"; порушення ЗУ "Про банки"; частка надходжень готівкових коштів від загальної суми надходжень; частка видатків готівкових коштів від загальної суми видатків); 2) вихідно-орієнтовної CCR-моделі задачі дробно-лінійного програмування максимізації умовних виходів (оцінка ризику легалізації кримінальних доходів) з постійною віддачею від масштабу. Умовні входи розраховуються на основі адитивної згортки зважених методом першої головної компоненти показників характеристики ефективності функціонування банків України. Кластеризація банків ґрунтується на застосуванні методу k-середніх. На відміну від існуючих запропонований підхід дозволяє сформувати групи ефективно та неефективно працюючих банків, визначити наявний резерв та потенціал збільшення ефективності як для групи в цілому, так і для кожного окремого банку, надати графічну інтерпретацію поточної позиції банків відносно конкурентів в середовищі функціонування на ринку банківських послуг в розрізі різних напрямків стратегічного управління.

Реалізацію науково-методичного підходу до оцінювання технічної ефективності фінансового моніторингу банків України на основі проведення фронтірного DEA-аналізу пропонується провести у вигляді наступної послідовності етапів.

1 етап. Кластеризація банків України на основі методу k-середніх. Запропонована методика кластеризації, тобто ітеративний дівізівний метод k-середніх у частині множини багатомірних науково-дослідницьких методик. Практичне виконання здійснене з використанням програми Statistica 8. У межах застосування методу k-середніх в частині початкових центрів певних кластерів, пропонується використати підхід розгляду відстані та обрання спостереження саме на сталих інтервалах. Метод k-середніх базується на визначених кількісних характеристиках: середні показники для кожного з кластерів (тобто передбачає

усереднення всередині окремого кластера), евклідові відстані (так звані евклідові метрики), а також квадрати евклідових відстаней між певними кластерами.

Далі описується здійснення на практиці кластеризації визначених досліджуваних об'єктів шляхом запропонованого методу та програмного засобу. Так, для оцінки та порівняння різних кластерів запропоновано застосовувати результати дисперсійного аналізу, що подаються на рисунках 3.18 – 3.20 та рисунках Г.1-Г.10 в частині виокремлення послідовно від 2 до 14 кластерів. На рисунку 3.18 показані величини міжгрупових (Between SS) та внутрішньогрупових (Within SS) дисперсій вказаних ознак.

Якість такого типу кластеризації характеризується відповідними критеріями, а саме:

- максимізація величини міжгрупової дисперсії, а також мінімізація величини внутрішньо групової дисперсії. Дотримання вказаної умови показує якість характеристики стосовно кожного визначеного показника ступеня віднесення банківських установ до певного кластеру і , відповідно, якість здійсненої кластеризації;

- величина критерію Фішера (F) та ймовірності можливого відхилення нульової гіпотези (p), а саме недоцільність використання визначеного показника для описання ступеня віднесення банківських установ до певного кластеру. Як результат якісної кластеризації величина F максимізується, а величина p наближається до нульової відмітки.

	Analysis of Variance (Spreadsheet1.sta)					
Variable	Between SS	df	Within SS	df	F	signif. p
K1	0,15	7	1,343	57	0,9154	0,501452
K2	12270,79	7	1156,657	57	86,3863	0,000000
K3	37164,78	7	2713,438	57	111,5292	0,000000
K4	12093,98	7	748,569	57	131,5571	0,000000
K5	0,57	7	2,812	57	1,6458	0,141265
K6	0,60	7	2,391	57	2,0398	0,065501

Рисунок 3.18 – Аналіз адекватності кластеризації банків України на 8 груп станом на 2019 рік

Отже, здійснення аналізу результатів формування банківських установ України по групах у 2019 році по 8 кластерах, означає, що кластеризація виконана, так як величина p в частині характеристик частка фінансових операцій, зареєстрованих за ознаками внутрішнього фінансового моніторингу; частка надходжень готівкових коштів від загальної суми надходжень; частка видатків готівкових коштів від загальної суми видатків більша за допустиме для економічних досліджень значення 0,05. Одночасно з цим, для таких характеристик величина критерію Фішера не є статистично значущою, показник міжгрупової дисперсії набуває розміру від 0.15 до 0.60, а показник внутрішньогрупової дисперсії більше за тисячі. Так, процес групування банківських установ України на 8 кластерів є неадекватним, а це спричиняє необхідність аналізу 9-кластерного групування визначених об'єктів дослідження (рисунок 3.19).

	Analysis of Variance (Spreadsheet1.sta)					
Variable	Between SS	df	Within SS	df	F	signif. p
K1	0,28	8	1,211	56	1,6370	0,135080
K2	12229,96	8	1197,484	56	71,4913	0,000000
K3	37203,38	8	2674,840	56	97,3604	0,000000
K4	12207,68	8	634,874	56	134,5995	0,000000
K5	0,45	8	2,935	56	1,0623	0,402364
K6	0,53	8	2,461	56	1,5037	0,176795

Рисунок 3.19 – Аналіз адекватності кластеризації банків України на 9 груп станом на 2019 рік

Дослідження згрупування банківських установ України за 9-ма кластерами у 2019 році означає, що якість групування покращується в частині частка фінансових операцій, зареєстрованих за ознаками внутрішнього фінансового моніторингу, означає підвищення якості такої кластеризації.

Наступне групування банківських установ від 9 до 10 (рисунок 3.20) сприяють зниженню якості кластеризації, оскільки значення показника p для аналізованих характеристик частка фінансових операцій, зареєстрованих за ознаками внутрішнього фінансового моніторингу; частка надходжень готівкових

коштів від загальної суми надходжень; частка видатків готівкових коштів від загальної суми видатків стає більшою за допустиме для економічних досліджень значення 0,05. Подальше формування 10 кластерів спричиняє погіршення величин як міжгрупової дисперсії, так і внутрішньогрупової дисперсії, критерію Фішера. Цей факт означає, що наступне виокремлення кластерів більше 9 груп є недоцільним.

	Analysis of Variance (Spreadsheet1.sta)					
Variable	Between SS	df	Within SS	df	F	signif. p
K1	0,28	9	1,210	55	1,4367	0,195472
K2	12359,96	9	1067,483	55	70,7581	0,000000
K3	38800,88	9	1077,340	55	220,0943	0,000000
K4	12417,76	9	424,791	55	178,6439	0,000000
K5	0,46	9	2,916	55	0,9733	0,472015
K6	0,53	9	2,458	55	1,3217	0,247265

Рисунок 3.20 – Аналіз адекватності кластеризації банків України на 10 групи станом на 2019 рік

Переходячи до порівняльного аналізу виділених кластерів банків України, розглянемо співвідношення середніх значень вхідних показників (рисунок 3.21).

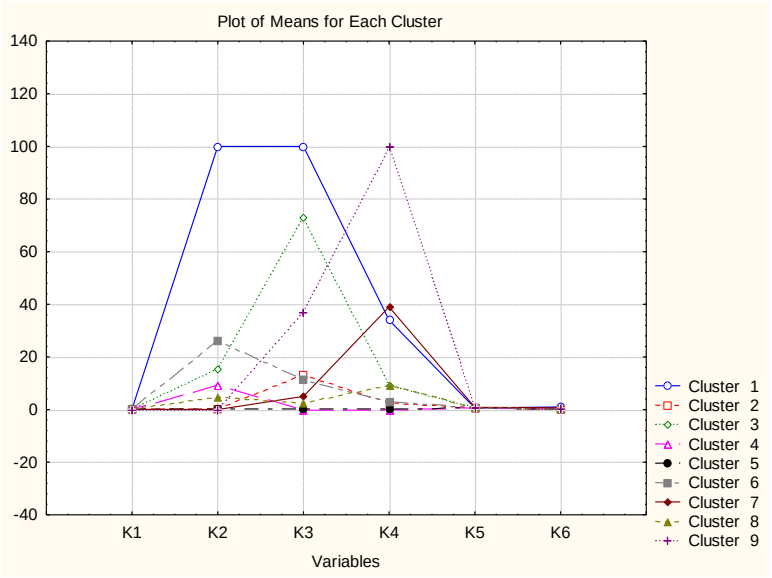


Рисунок 3.21 – Візуалізація співвідношення середніх значень вхідних показників в розрізі виділених кластерів

Аналізуючи виділені 9 кластерів за допомогою інструментарію Statistica, необхідно відзначити, що частину кластерів формує лише 1 банк. Така ситуація характерна для 1, 7 та 9 кластерів. На нашу думку така ситуація є недоцільною, враховуючи однорідність описових характеристик (евклідових відстаней між складовими) даних груп. Для нівелювання зазначеної проблематики пропонується подальше перегрупування 9 кластерів на 6 кластерів, представлених на рисунках 6 – 11.

Розглядаючи перший кластер (рисунок 3.22), встановимо склад банківських установ України, що його утворюють. Отже, за методом k-середніх до 1-го кластеру відносяться 5 банківських установ:

	Members of Cluster Number 2 (Spreadsheet1.sta) and Distances from Respective Cluster Center Cluster contains 5 cases
Case No.	Distance
C_8	6,536338
C_13	1,260224
C_16	2,312586
C_20	2,188678
C_50	2,308975

Рисунок 3.22 – Склад першої із шести умовних кластерів банків України в розрізі легалізації кримінальних доходів

Наступним, переходячи до здійснення аналізу описових статистик першого кластеру (рисунок 3.22, Г.11 в частині середньої величини, значення стандартного відхилення та показника дисперсії по кожному з 6 визначених показників, підсумуємо, що в розрізі такої групи банківських установ України визначальними є порушення ПП НБУ; порушення ЗУ "Про легалізацію"; порушення ЗУ "Про банки", у яких середні величини складають відповідно 100 од., 100 од., 34 од. відповідно. Мінімальні величини середньоквадратичних відхилень зустрічаються в розрізі усіх 6 показників, і означає те, що в частині таких характеристик поміж 5 банківських установ цього кластеру встановлена мінімальна варіація, тобто подібність розміру величин. Максимальний розкид

евклідових величин відстаней спостерігається в розрізі 8 банку у порівнянні з іншими банками.

Переходячи до другої із шести умовних кластерів банків України в розрізі легалізації кримінальних доходів, зазначимо, що дана група містить наступний склад: 1, 4, 9, 14, 22 і 31 банківська установа (рисунок 3.23). На основі рисунку Г.14 можна зробити висновок про визначальні особливості даної групи в розрізі таких показників як порушення ЗУ "Про легалізацію"; порушення ЗУ "Про банки".

	Members of Cluster Number 3 (Spreadsheet1.sta) and Distances from Respective Cluster Center Cluster contains 6 cases
Case No.	Distance
C_1	11,01400
C_4	10,69935
C_9	12,82663
C_14	7,54443
C_22	9,13011
C_31	5,91773

Рисунок 3.23 – Склад другої із шести умовних кластерів банків України в розрізі легалізації кримінальних доходів

Третю із шести умовних кластерів банків України в розрізі легалізації кримінальних доходів пропонується сформувати за рахунок 6 складових: 5,17, 65, 2, 18 та 10 (рисунок 3.24). В розрізі середніх величин обраних для аналізу показників зазначимо визначальний характер для формування даної групи таких напрямків як порушення ПП НБУ; порушення ЗУ "Про легалізацію"; порушення ЗУ "Про банки".

Найбільш чисельною за кількістю банків-учасників вступає четверта група, яка містить 43 складові (фрагмент представлений на рисунку 3.25, Г.17). Визначальною особливістю даного кластеру виступає однорідність значень усіх 6 показників характеристики легалізації кримінальних доходів як за середніми значеннями, так і за дисперсією та середньоквадратичними відхиленнями.

	Members of Cluster Number 4 (Spreadsheet1.sta) and Distances from Respective Cluster Center Cluster contains 3 cases
Case No.	Distance
C_5	0,960305
C_17	1,930919
C_65	0,993965

	Members of Cluster Number 1 (Spreadsheet1.sta) and Distances from Respective Cluster Center Cluster contains 1 cases
Case No.	Distance
C_2	0,00

	Members of Cluster Number 7 (Spreadsheet1.sta) and Distances from Respective Cluster Center Cluster contains 1 cases
Case No.	Distance
C_18	0,00

	Members of Cluster Number 9 (Spreadsheet1.sta) and Distances from Respective Cluster Center Cluster contains 1 cases
Case No.	Distance
C_10	0,00

Рисунок 3.24 – Склад третьої із шести умовних кластерів банків України в розрізі легалізації кримінальних доходів

	Members of Cluster Number 5 (Spreadsheet1.sta) and Distances from Respective Cluster Center Cluster contains 43 cases
Case No.	Distance
C_6	0,160823
C_7	0,356369
C_11	0,166931
C_12	0,219776
C_15	0,235676
C_19	0,291699
C_21	0,190505
C_23	0,744726
C_24	0,177889
C_25	0,371162
C_26	1,142137
C_27	0,203237
C_28	0,197443

Рисунок 3.25 – Склад четвертої із шести умовних кластерів банків України в розрізі легалізації кримінальних доходів

Нечисельними та в той же час специфічними виступають п’ята та шоста групи банків (рисунок 3.26, 3.27, Г.18, Г.20). Так, для п’ятої групи визначальними напрямками поведінки виступають порушення ПП НБУ та порушення ЗУ "Про легалізацію". Для шостої групи порушення ПП НБУ; порушення ЗУ "Про легалізацію"; порушення ЗУ "Про банки".

	Members of Cluster Number 6 (Spreadsheet1.sta) and Distances from Respective Cluster Center Cluster contains 3 cases
Case No.	Distance
C_3	7,336069
C_39	5,173688
C_44	3,364827

Рисунок 3.26 – Склад п’ятої із шести умовних кластерів банків України в розрізі легалізації кримінальних доходів

	Members of Cluster Number 8 (Spreadsheet1.sta) and Distances from Respective Cluster Center Cluster contains 2 cases
Case No.	Distance
C_36	2,115538
C_54	2,115538

Рисунок 3.27 – Склад шостої із шести умовних кластерів банків України в розрізі легалізації кримінальних доходів

2 етап. Введення базових даних. На даному етапі проводиться завантаження вхідних даних щодо оцінювання ефективності функціонування банків до програми Banxia Frontier Analyst 4 за допомогою використання базового користувацького інтерфейсу, проводиться попередній аналіз змінних та їх групування на умовно вхідні (контрольовані дискреційні та неконтрольовані екзогенно фіксовані або недискреційні змінні) та вихідні, ідентифікація релевантних показників та доцільність їх включення в модель, вибір способу інтерпретації даних (таблиця 3.4).

Для реалізації даного етапу обрано одну вихідну змінну: RLKD – кількісна оцінка ризику легалізації кримінальних доходів. В якості вхідних контрольованих дискреційних змінних пропонується обрати наступний перелік показників: К1 - частка фінансових операцій, зареєстрованих за ознаками внутрішнього фінансового моніторингу; К2 - порушення ПП НБУ; К3 - порушення ЗУ "Про легалізацію"; К4 - порушення ЗУ "Про банки"; К5 - частка надходжень готівкових коштів від загальної суми надходжень; К6 - частка видатків готівкових коштів від загальної суми видатків.

Таблиця 3.4 – Вхідні та вихідні показники дослідження ефективності банків України в розрізі протидії легалізації кримінальних доходів станом на 2019 рік

	1 група						
Bank	***K1***	***K2***	***K3***	***K4***	***K5***	***K6***	***RLKD***
Bank 8	0,1739	0	29	3	0,7715	0,4377	0,5276
Bank 13	0,0011	1	10	3	0,8906	0,3415	0,6019
Bank 16	0,0508	0	8	0	0,9269	0,8141	0,0254
Bank 20	0,0342	1	10	7	0,7968	0,2832	0,6489
Bank 50	0,0664	0	8	0	0,9624	0,1640	0,7000
	2 група						
Bank	***K1***	***K2***	***K3***	***K4***	***K5***	***K6***	***RLKD***
Bank 1	0,0760	20	48	0	0,6305	0,1815	0,4428
Bank 4	0,1107	38	86	7	0,5571	0,2163	0,4880
Bank 9	0,0514	6	97	27	0,9017	0,4259	0,5373
Banj 14	0,1181	1	83	3	0,8640	0,6472	0,6074
Bank 22	0,0785	24	54	1	0,8725	0,5823	0,6607
Bank 31	0,1121	3	70	16	0,6852	0,4528	0,6819
	3 група						
Bank	***K1***	***K2***	***K3***	***K4***	***K5***	***K6***	***RLKD***
Bank 5	0,1376	7	0	0	0,7043	0,2532	0,4945
Bank 17	1,0000	14	0	0	0,9009	0,5654	0,6428
Bank 65	0,0000	7	0	0	0,0000	0,0632	0,7266
Bank 2	0,2013	100	100	34	0,5588	1,0000	0,4603
Bank 18	0,0703	0	5	39	0,8460	0,7008	0,6465
Bank 10	0,0260	0	37	100	0,8243	0,4176	0,5457
	4 група						
Bank	***K1***	***K2***	***K3***	***K4***	***K5***	***K6***	***RLKD***
Bank 6	0,1239	0	0	0	0,7919	0,3932	0,4974
Bank 7	0,0525	1	0	0	0,8879	0,4456	0,5185
Bank 11	0,1169	0	0	0	0,6306	0,4507	0,5743
Bank 12	0,0061	0	0	0	0,4874	0,1357	0,5876
Bank 15	0,1960	0	0	0	0,3609	0,2130	0,6156
Bank 19	0,0000	0	0	0	0,1801	0,5801	0,6469
Bank 21	0,0000	0	0	0	0,7154	0,1586	0,6507
Bank 23	0,0173	0	2	0	0,6043	0,1075	0,6610
Banj 24	0,2434	0	0	0	0,8602	0,4569	0,6707
Bank 25	0,0916	1	0	0	0,8338	0,6797	0,6733
Bank 26	0,1195	0	0	3	0,7082	0,6535	0,6741
Bank27	0,1841	0	0	0	0,7403	0,0904	0,6767
	5 група						
Bank	***K1***	***K2***	***K3***	***K4***	***K5***	***K6***	***RLKD***
Bamk 3	0,0798	25	29	6	0,7306	0,2668	0,4873
Bank 39	0,0051	32	0	3	0,4501	0,2135	0,6909
Bank 41	0,3088	0	0	0	0,9087	0,6575	0,6929

Продовження таблиці 3.4

	6 група						
Bank	*K1*	*K2*	*K3*	*K4*	*K5*	*K6*	*RLKD*
Bank 36	0,4713	0	5	9	0,9318	0,5672	0,6900
Bank 54	0,0000	9	0	9	0,0000	0,0000	0,7051

Переходячи до ідентифікації релевантних показників, була проведена перевірка доцільності їх включення в модель за допомогою методу головних компонент у програмі Statistica 6.0. Так, за результатами факторних навантажень та графіку кам'янистого осипу було ідентифіковано, що серед переліку базових показників для оцінювання технічної ефективності банків України на основі проведення фронтірного DEA-аналізу середовища функціонування необхідно включити до розгляду усі вказані вище змінні.

Результати реалізації даного етапу науково-методичного підходу до оцінювання ефективності банків України на прикладі першої групи банків станом на 2019 рік представлено на рисунку 3.28.

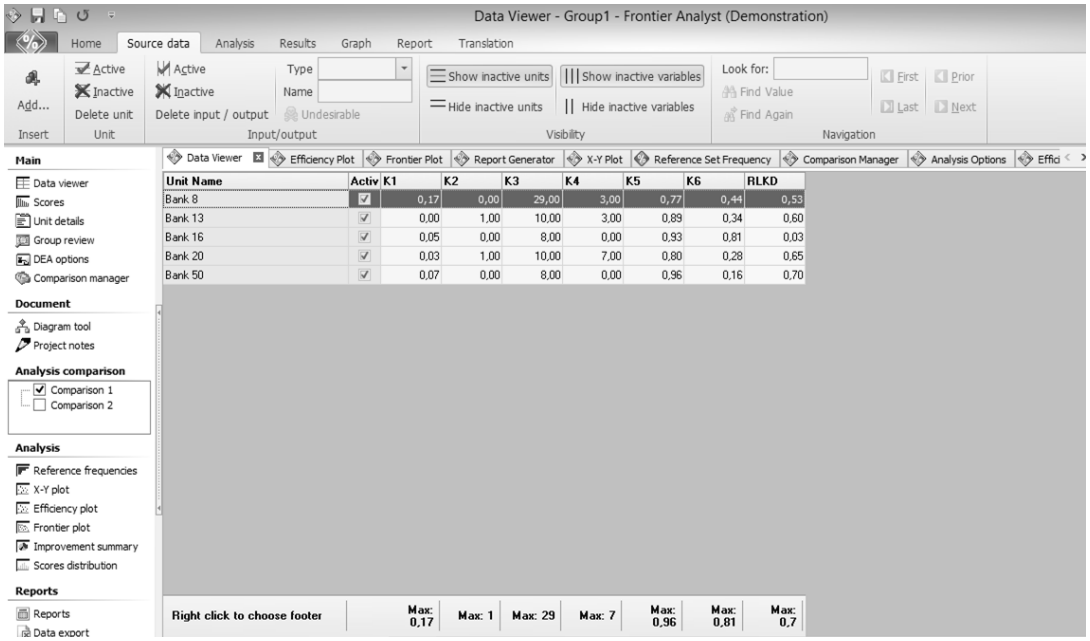


Рисунок 3.28 - Введення базових даних оцінювання ефективності банків України в розрізі протидії легалізації кримінальних доходів станом на 2019 рік

3 етап. Структурування проекту фронтірного DEA-аналізу середовища функціонування шляхом побудови вхідно-орієнтованої BCC-моделі задачі

дробно-лінійного програмування мінімізації умовних входів та вихідно-орієнтовної CCR-моделі задачі дробно-лінійного програмування максимізації відношення умовних виходів з постійною віддачею від масштабу (рисунок 3.29).

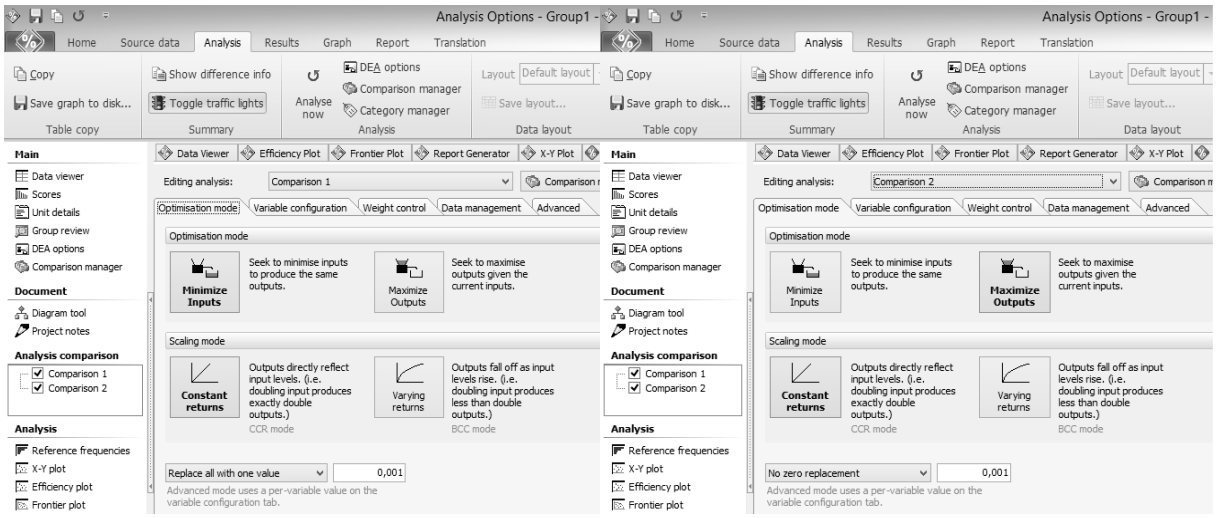


Рисунок 3.29 – Вікно вибору параметрів та вихідних умов побудови вхідно-орієнтованої BCC-моделі задачі дробно-лінійного програмування мінімізації умовних входів та CCR-моделі задачі дробно-лінійного програмування максимізації відношення умовних виходів з постійною віддачею від масштабу

Переходячи до математичної формалізації даного етапу, виникає необхідність, по-перше, визначення пріоритетності вхідних та вихідних змінних, що пропонується провести на основі використання методу головних компонент за допомогою програми Statistica (рисунок 3.30).

Аналіз рисунку 3.30 дозволяє зробити висновки. Беручи до увагу першу головну компоненту (Factor1) в розрізі усіх шести виділених кластерів, для першої групи банків найважливішими показниками є частка фінансових операцій, зареєстрованих за ознаками внутрішнього фінансового моніторингу (0,29); порушення ЗУ "Про легалізацію" (0,36); частка надходжень готівкових коштів від загальної суми надходжень (0,27), так як кожен з них складає орієнтовно по 30% від загальної ваги; показники . порушення ПП НБУ (0,02) та

частка надходжень готівкових коштів від загальної суми надходжень (0,04) є менш важливими, а не важливим є показник частка видатків готівкових коштів від загальної суми видатків, частка якого складає 0. Для другої групи банків найважливішими показниками є порушення ПП НБУ (0,23); частка надходжень готівкових коштів від загальної суми надходжень (0,28); частка видатків готівкових коштів від загальної суми видатків (0,20), так як кожен з них займає не менше 20% від загальної ваги; показники . порушення ЗУ "Про легалізацію" (0,10); порушення ЗУ "Про банки" (0,15) є менш важливими, а найменш важливим є показник частка фінансових операцій, зареєстрованих за ознаками внутрішнього фінансового моніторингу, частка якого складає 0,02. Для третьої групи банків найважливішими показниками є порушення ПП НБУ (0,27); порушення ЗУ "Про легалізацію" (0,32) ; частка видатків готівкових коштів від загальної суми видатків (0,30), так як кожен з них займає орієнтовно 30% від загальної ваги; показники . порушення ЗУ "Про банки" (0,05); частка надходжень готівкових коштів від загальної суми надходжень (0,03) є менш важливими, а майже не важливим є показник частка фінансових операцій, зареєстрованих за ознаками внутрішнього фінансового моніторингу (0,0007). Для четвертої групи банків найважливішими показником є частка видатків готівкових коштів від загальної суми видатків (0,30), так як його частка займає 30% від загальної ваги; показники . порушення ПП НБУ; порушення ЗУ "Про легалізацію"; частка надходжень готівкових коштів від загальної суми надходжень є середньо важливими, так як їх частка становить по 0,17 кожен, а найменш важливим є показники частка фінансових операцій, зареєстрованих за ознаками внутрішнього фінансового моніторингу ; порушення ЗУ "Про банки», частка яких складає по 0,08. Для п’ятої групи банків найбільш важливими показниками є частка фінансових операцій, зареєстрованих за ознаками внутрішнього фінансового моніторингу (0,21); порушення ПП НБУ (0,21); частка видатків готівкових коштів від загальної суми видатків (0,22), оскільки кожен з них займає не менше 20% від загальної ваги; показники . порушення ЗУ "Про банки"; частка надходжень готівкових коштів від загальної суми надходжень є менш

важливими і складають по 0,15 кожен, а найменш важливим є показник порушення ЗУ "Про легалізацію", частка якого складає 0,04 від загальної ваги. Для шостої групи банків всі показники є однаково важливими , а вага кожного складає по 0,16 від загальної ваги усіх показників.

	Variable contributions, based on correlations (Group1.sta			
Variable	Factor 1	Factor 2	Factor 3	Factor 4
Var1	0,298143	0,080795	0,033033	0,047681
Var2	0,022014	0,364335	0,022552	0,289749
Var3	0,360635	0,005985	0,002365	0,400983
Var4	0,045597	0,342923	0,020015	0,239949
Var5	0,273604	0,101922	0,051025	0,021453
Var6	0,000006	0,104039	0,871010	0,000184

	Variable contributions, based on correlations (Group2.sta				
Variable	Factor 1	Factor 2	Factor 3	Factor 4	Factor 5
Var1	0,025662	0,145184	0,609888	0,001612	0,027324
Var2	0,233504	0,028441	0,013952	0,566782	0,146140
Var3	0,109294	0,182608	0,255254	0,206774	0,207993
Var4	0,150368	0,332927	0,012568	0,047813	0,424392
Var5	0,281582	0,047058	0,104181	0,101229	0,020848
Var6	0,199589	0,263782	0,004157	0,075790	0,173302

	Variable contributions, based on correlations (Group3.sta				
Variable	Factor 1	Factor 2	Factor 3	Factor 4	Factor 5
Var1	0,000715	0,455570	0,122864	0,394816	0,025311
Var2	0,272722	0,025261	0,159528	0,000884	0,088198
Var3	0,326977	0,059660	0,001539	0,069957	0,092586
Var4	0,058858	0,015530	0,544029	0,240115	0,052088
Var5	0,031063	0,394160	0,171608	0,095757	0,306703
Var6	0,309665	0,049818	0,000432	0,198470	0,435114

	Variable contributions, based on correlations (Group4.sta					
Variable	Factor 1	Factor 2	Factor 3	Factor 4	Factor 5	Fact
Var1	0,080151	0,141599	0,463320	0,002660	0,239058	0,07
Var2	0,179717	0,409825	0,019699	0,007954	0,013379	0,36
Var3	0,171807	0,073508	0,010337	0,462954	0,280954	0,00
Var4	0,080900	0,253189	0,149238	0,297451	0,078140	0,14
Var5	0,177859	0,113360	0,171305	0,221432	0,146961	0,16
Var6	0,309565	0,008518	0,186101	0,007550	0,241508	0,24

	Variable contributions, based on correlations (Group5.sta	
Variable	Factor 1	Factor 2
Var1	0,213214	0,023333
Var2	0,215348	0,016764
Var3	0,045588	0,539502
Var4	0,155390	0,201391
Var5	0,150420	0,216695
Var6	0,220040	0,002315

	Variable contributions, based on correlations (Group6.sta
Variable	Factor 1
Var1	0,166667
Var2	0,166667
Var3	0,166667
Var4	0,166667
Var5	0,166667
Var6	0,166667

Рисунок 3.30 – Результати оцінювання пріоритетності показників характеристики ефективності протидії легалізації кримінальних доходів

Здійснюючи підбір певних параметрів та вихідних умов створення BCC-моделі задачі мінімізації умовних входів та CCR-моделі задачі максимізації відношення умовних виходів ефективності фінансового моніторингу банків України, визначимо мінімальні та максимальні значення пріоритетності показників, обрані на базі застосування формули Фішберна (на прикладі першої групи банків України станом на 2019 рік) (рисунок 3.31).

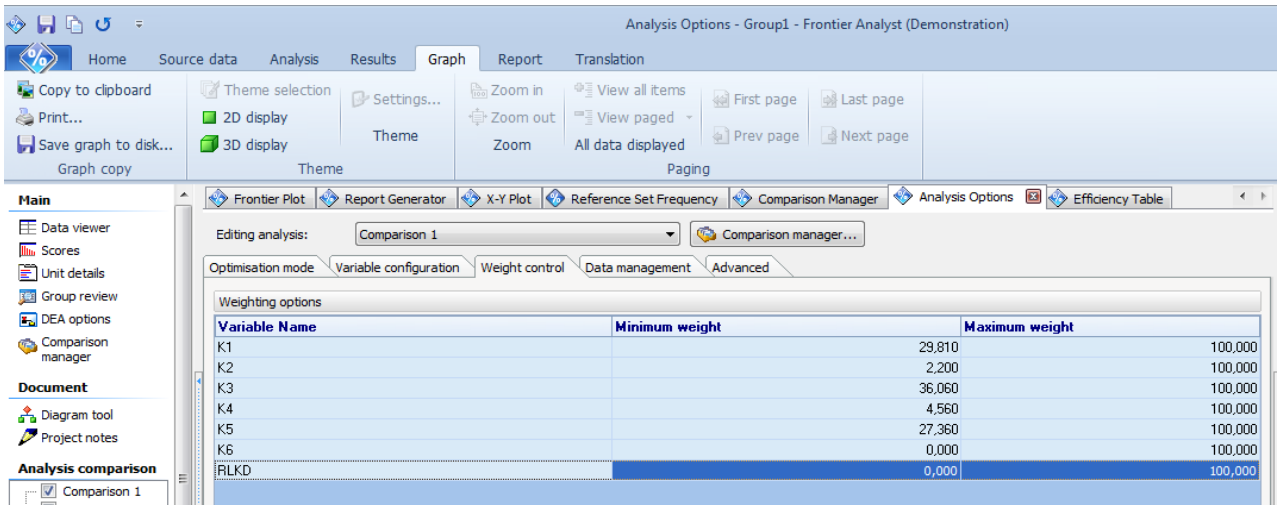


Рисунок 3.31 – Встановлення пріоритетності показників оцінювання ефективності банків України першої групи станом на 2019 рік

Наступний крок другого етапу запропонованого науково-методичного підходу до оцінювання ефективності фінансового моніторингу банківських установ України передбачає безпосередньо проведення математичної формалізації процесу побудови вхідно-орієнтованої BCC-моделі задачі дробно-лінійного програмування мінімізації умовних входів та вихідно-орієнтовної CCR-моделі задачі дробно-лінійного програмування максимізації відношення умовних виходів з постійною віддачею від масштабу:

$$\max \theta = \frac{\sum_i u_i w_i y_i}{\sum_i v_i w_i x_i}$$

$$\begin{cases} \dfrac{\sum_i u_i w_i y_i}{\sum_i v_i w_i x_i} \le 1, \\ \min w_i \le w_i \le 100\% \\ x_i \ge 0, y_i \ge 0 \end{cases} \qquad (3.21)$$

де θ - рівень технічної ефективності функціонування фінансового моніторингу обраної банківської установи;

u_i - характеристика економетричної моделі залежності технічної ефективності функціонування фінансового моніторингу обраної банківської установи від категорії умовних виходів;

y_i - і-та характеристика умовних виходів;

v_i - характеристика економетричної моделі залежності технічної ефективності функціонування фінансового моніторингу обраної банківської установи від категорії умовних входів;

x_i - і-та характеристика умовних входів.

3 етап. Проведення аналізу отриманих результатів застосування вхідно-орієнтованої BCC-моделі задачі дробно-лінійного програмування мінімізації умовних входів та вихідно-орієнтовної CCR-моделі задачі дробно-лінійного програмування максимізації відношення умовних виходів з постійною віддачею від масштабу для ефективності функціонування фінансового моніторингу банків України. Комплексний аналіз одержаних результатів дослідження показано на прикладі 34 банків шести груп банківських установ України станом на 2019 рік.

Переходячи до здійснення аналізу визначених результатів по першій групі банків України (рисунок 3.32), слід зазначити, що ефективною за 2019 рік виявилась робота Банку 13 та Банку 50 для BCC-моделі мінімізації умовних входів, а також - Банку 16 для CCR-моделі максимізації умовних виходів, про що свідчить розрахований показник технічної ефективності системи фінансового моніторингу на рівні 100%. При чому три банки першої групи – Банк 16 (4,0%%), Банк 20 (74,4%), Банк 8 (43,5%) для BCC-моделі, та чотири банки – Банк 13 (60,2%), Банк 20 (4,1%), Банк 50 (3,3%) та Банк 8 92,6%) для CCR-моделі, показали неефективну роботу.

Визначивши ефективно працюючі об’єкти дослідження в розрізі банків України першої групи згідно вхідно-орієнтованої BCC-моделі мінімізації умовних входів, встановимо наявний резерв та потенціал зростання ефективності фінансового моніторингу для групи в цілому (рисунок 3.33).

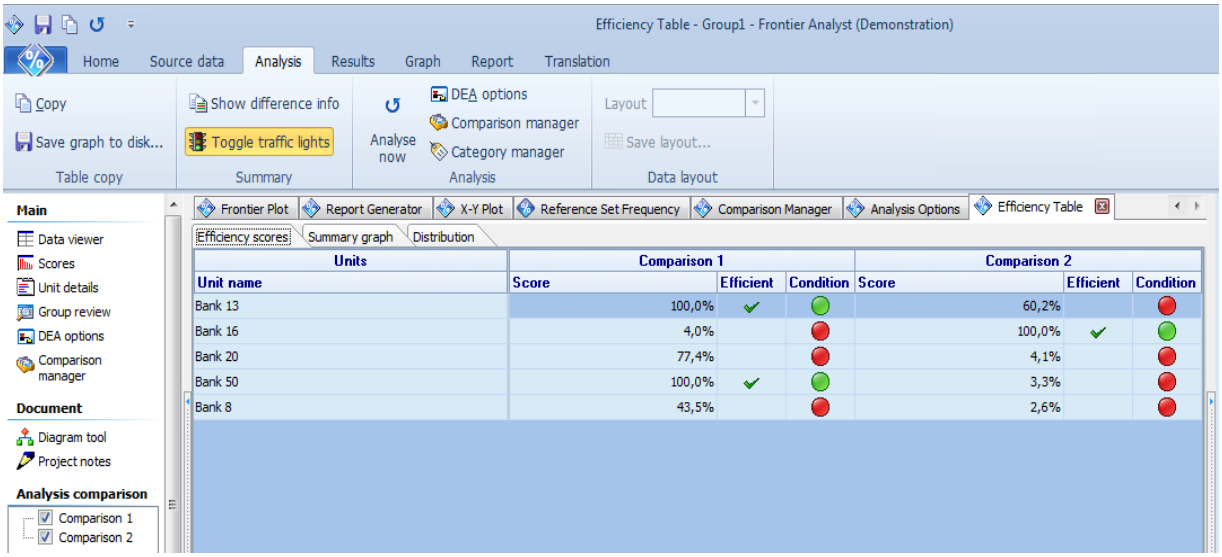


Рисунок 3.32 – Ефективність функціонування першої групи банків України станом на 2019 рік для ВСС-моделі та для CCR-моделі

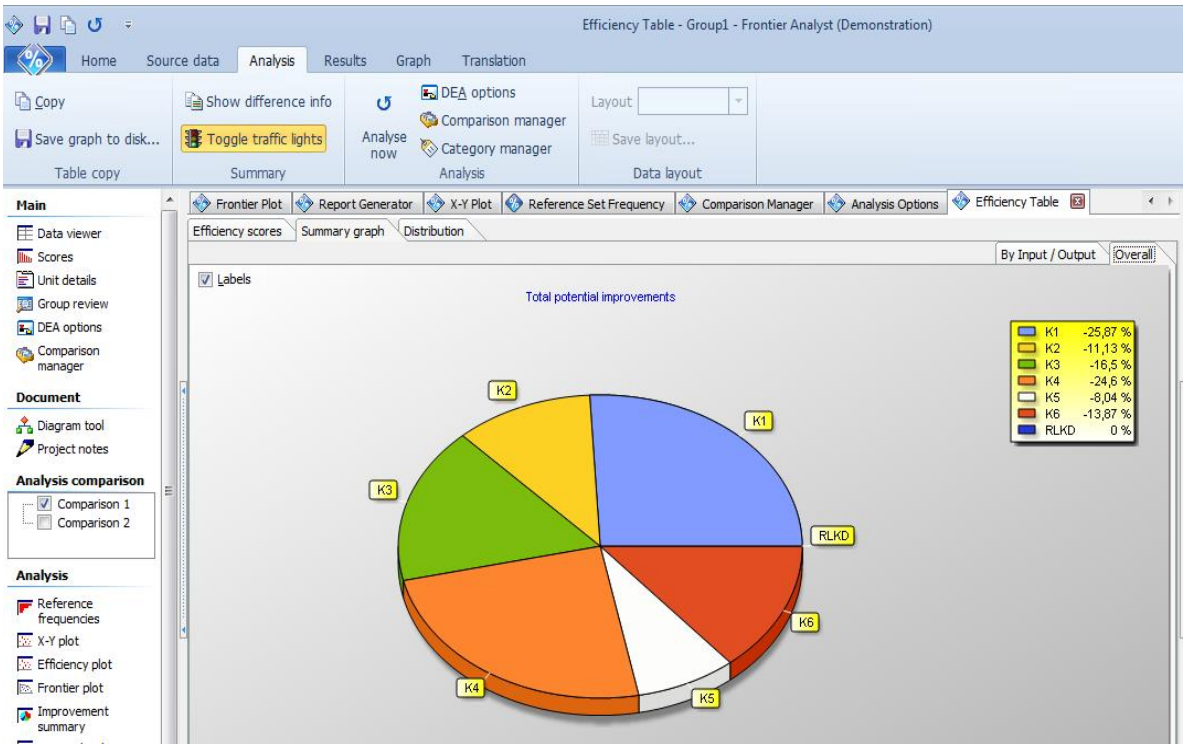


Рисунок 3.33 – Потенціал покращення ефективності функціонування фінансового моніторингу першої групи банків України станом на 2019 рік для ВСС-моделі

Отже, зроблено висновок щодо в цьому випадку зовсім не варто витрачати зусилля на змінні: К1 - частку фінансових операцій, зареєстрованих за ознаками

внутрішнього фінансового моніторингу, К2 - порушення ПП НБУ; К3 - порушення ЗУ "Про легалізацію", К4 - порушення ЗУ "Про банки", К5 - частку надходжень готівкових коштів від загальної суми надходжень, К6 - частку видатків готівкових коштів від загальної суми видатків, RLKD – кількісну оцінку ризику легалізації кримінальних доходів.

Графік розподілу (рисунок 3.34) наглядно відображає дані стосовно діапазон оцінок ефективності та подробиці кількості банків з їх балами у кожному діапазоні. Так 1 банк знаходиться в діапазоні 0-10, 1 в 41-50, 1 в 71-80, 1 банк в ефективному діапазоні, тобто є на 100% ефективними.

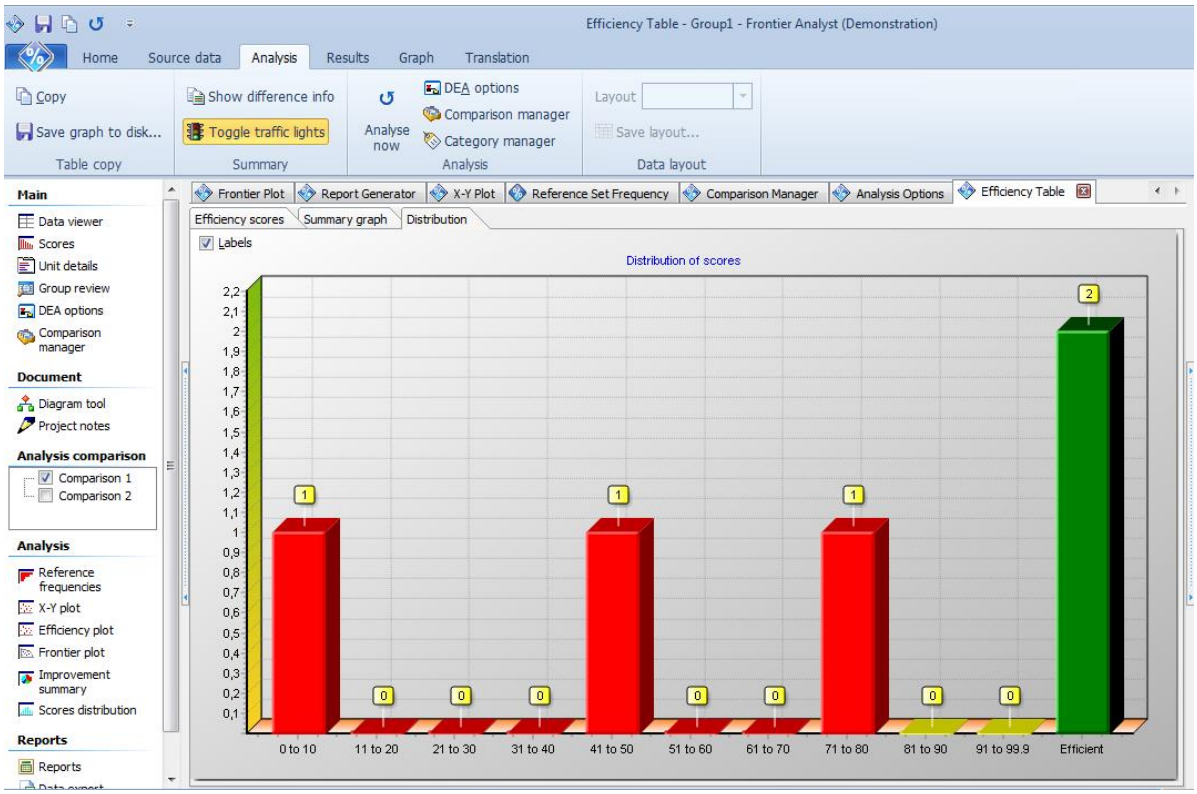


Рисунок 3.34 - Графік розподілу оцінок ефективності функціонування фінансового моніторингу першої групи банків України станом на 2019 рік для ВСС-моделі

Визначивши ефективно працюючі об’єкти дослідження в розрізі банків України першої групи згідно вихідно-орієнтовної CCR-моделі задачі дробно-лінійного програмування максимізації відношення умовних виходів,

встановлено наявний резерв та потенціал зростання ефективності фінансового моніторингу для групи в цілому (рисунок 3.35). Так, зроблено висновок щодо наявності резерву за всіма показниками вхідних індикаторів. Так, найбільші обсяги резервів встановлено за такими показниками як К6 - частка видатків готівкових коштів від загальної суми видатків 40,68%. Середні зусилля потрібно спрямувати на покращення змінної К1 - частка фінансових операцій, зареєстрованих за ознаками внутрішнього фінансового моніторингу 10,52%. В той же час найменший резерв даної групи банків спостерігається за показником К5 - частка надходжень готівкових коштів від загальної суми надходжень 2,43%. Не варто витрачати зусилля на змінні: К2, К3, К4, RLKD .

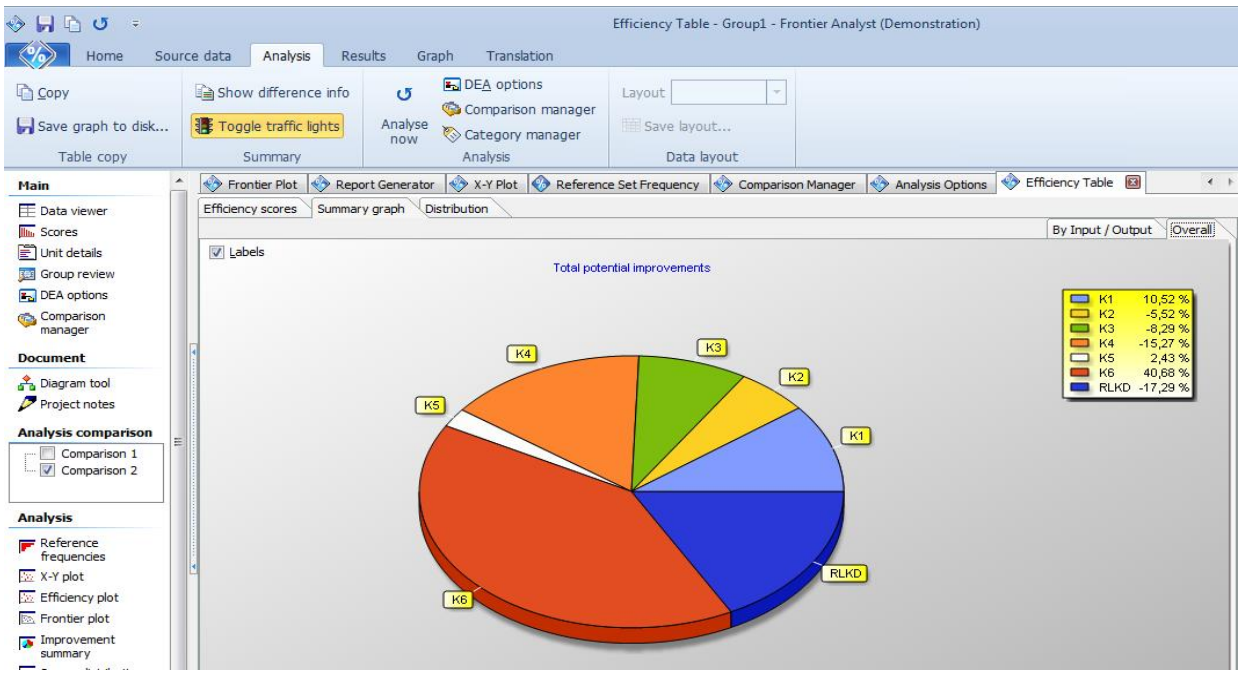


Рисунок 3.35 – Потенціал покращення ефективності функціонування фінансового моніторингу першої групи банків України станом на 2019 рік для CCR-моделі

Відповідно, графік розподілу (рисунок 3.36) зображує дані стосовно діапазон оцінок ефективності , тобто 3 банки знаходиться в діапазоні 0-10, 1 в 51-60, 1 банк в ефективному діапазоні і є на 100% ефективними.

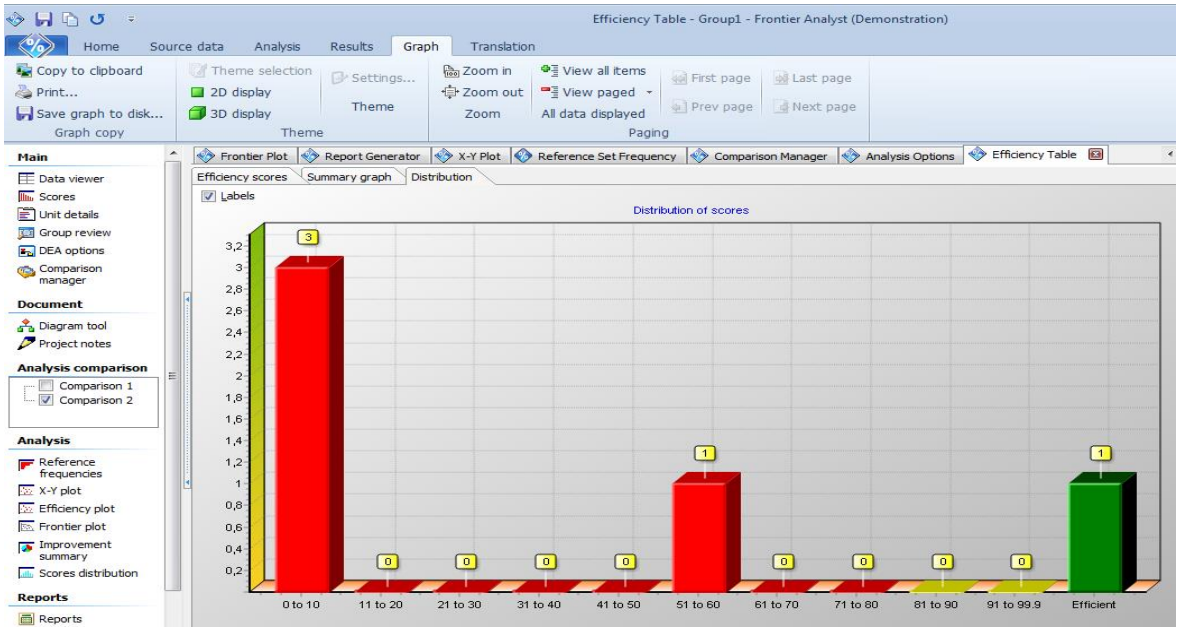


Рисунок 3.36 – Графік розподілу оцінок ефективності функціонування фінансового моніторингу першої групи банків України станом на 2019 рік для CCR-моделі

Аналогічно дослідженню першої групи банків встановлено, що по другій групі банків України (Додаток Д, рисунок Д.1) на 100% ефективними є за 2019 рік для BCC-моделі - Банк 14, Банк 1, Банк 31, а для CCR-моделі - Банк 14 та Банк 1. При чому банки другої групи – Банк 22 (86,9%) , Банк 4 (75,8%), Банк 9 (60,4%) для BCC-моделі, та банки – Банк 22 (39,0%), Банк 31 (80,4%), Банк 4 (62,4%) та Банк 9 (88,3%) для CCR-моделі, показали неефективну роботу. Аналогічно визначено ефективні та неефективні банки третьої, четвертої, п’ятої та шостої груп (Додаток Д, рисунок Д.6, рисунок Д.11, рисунок Д.16., рисунок Д.21).

Аналогічно аналізу першої групи банків, нижче для другої групи банків графічно показано кругову діаграму (Додаток Д, рисунок Д.2, рисунок Д.4) можливого покращення роботи фінансового моніторингу у вигляді відносних відсотків потенційного покращення для кожної з вхідних/вихідної змінних у окресленому діапазоні. Для BCC-моделі середні зусилля необхідно спрямувати на покращення змінної К1 (16,46%). Зовсім не потрібно витрачати зусилля на змінні К2, К3, К4, К5, К6, RLKD. Для CCR -моделі середні зусилля необхідно

спрямувати на покращення змінної К1 (22,19%), К5 (12,1%), К6 (10,29%). Незначні зусилля можна спрямувати на покращення змінну К3 (5,99%). Не варто витрачати зусилля на змінні К2, К4, RLKD. Аналогічно проаналізовано і графічно зображено банки третьої, четвертої, п’ятої та шостої груп (Додаток Д, рисунок Д.7, рисунок Д.9, рисунок Д.12, рисунок Д.14, рисунок Д.17, рисунок Д.19, рисунок Д.22, рисунок Д.24).

Також, аналогічно аналізу першої групи банків, графік розподілу (Додаток Д, рисунок Д.3, рисунок Д.5) банків другої групи показує , що для ВСС-моделі 1 банк знаходиться в діапазоні 51-60, 1 в 71-80, 1 в 51-60, 1 в 71-80, 1 в 81-90 та 3 банки в ефективному діапазоні; для CCR -моделі 1 банк знаходиться в діапазоні 31-40, 1 в 61-70, 1 в 71-80, 1 в 81-90 та 2 банки в ефективному діапазоні. Аналогічно по графіках розподілу зображено та проаналізовано банки третьої, четвертої, п’ятої та шостої груп (Додаток Д, рисунок Д.8, рисунок Д.10, рисунок Д.13, рисунок Д.15, рисунок Д.18, рисунок Д.20, рисунок Д.23, рисунок Д.25).

Детальніше зупинимося на аналізі неефективних банківських установ за допомогою інформаційних даних, що міститься у вкладці деталей банківських установ щодо потенційних покращень їх роботи, еталонного порівняння, довідкових матеріалів, а також вхідні чи вихідні данні по окремо взятим банкам.

Графік потенційних покращень (рисунок 3.37) показує процентні зміни по кожному окремому показнику, що банк повинен зробити для досягнення ефективності фінансового моніторингу. Графік показує, що для Банку 8 є місце для покращення по змінним, тобто для CCR-моделі К2 на 86,08%, К5 на 123,57%, К6 на 246,10 % , а для для ВСС-моделі покращення змінних не потрібні.. Також спостерігаються можливість скорочення по деяким змінним, а саме: для CCR-моделі К1 на 45,68%, К3 на 48,67%, К4 на 99,99 %, RLKD на 97,42% , а для для ВСС-моделі по всім показникам, крім RLKD , тобто К1 на 71,23%, К2 на 24,63%, К3 на 73,21%, К4 на 100,0%, К5 на 5,98%, К6 на 71,76%

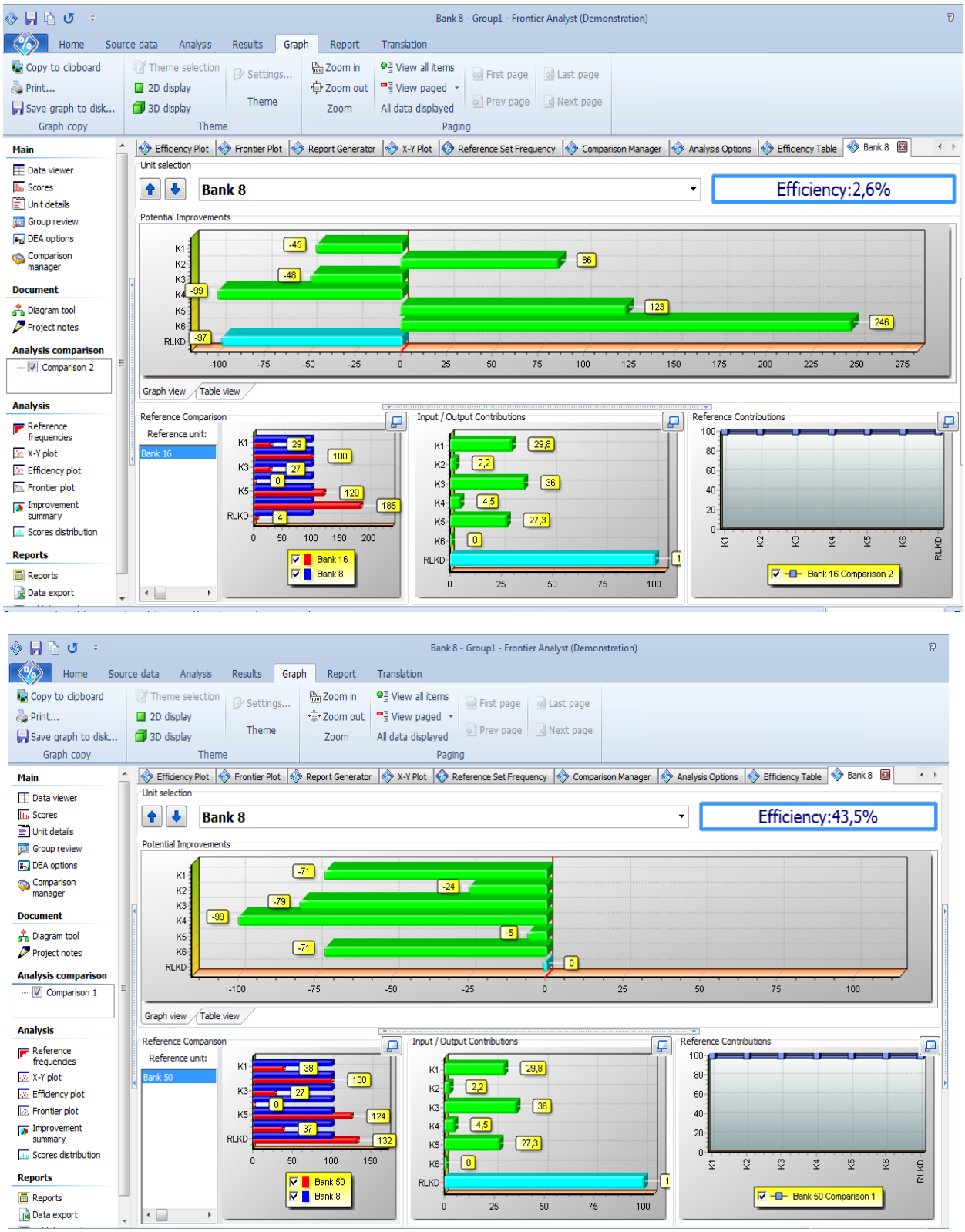


Рисунок 3.37 – Аналіз результативності та потенціалу покращення фінансового моніторингу Банку8 станом на 2019 рік для CCR-моделі та для BCC-моделі

Потенційні зміни можливо також розглянути у табличній формі (рисунок 3.38). У стовбці факт зображені досягнуті в даний момент значення. У цільовому стовбці значення, що повинні бути досягнуті для ефективної роботи фінансового моніторингу банку. У стовпці потенційних покращень зображена різниця між фактом та планом у процентному вираженні.

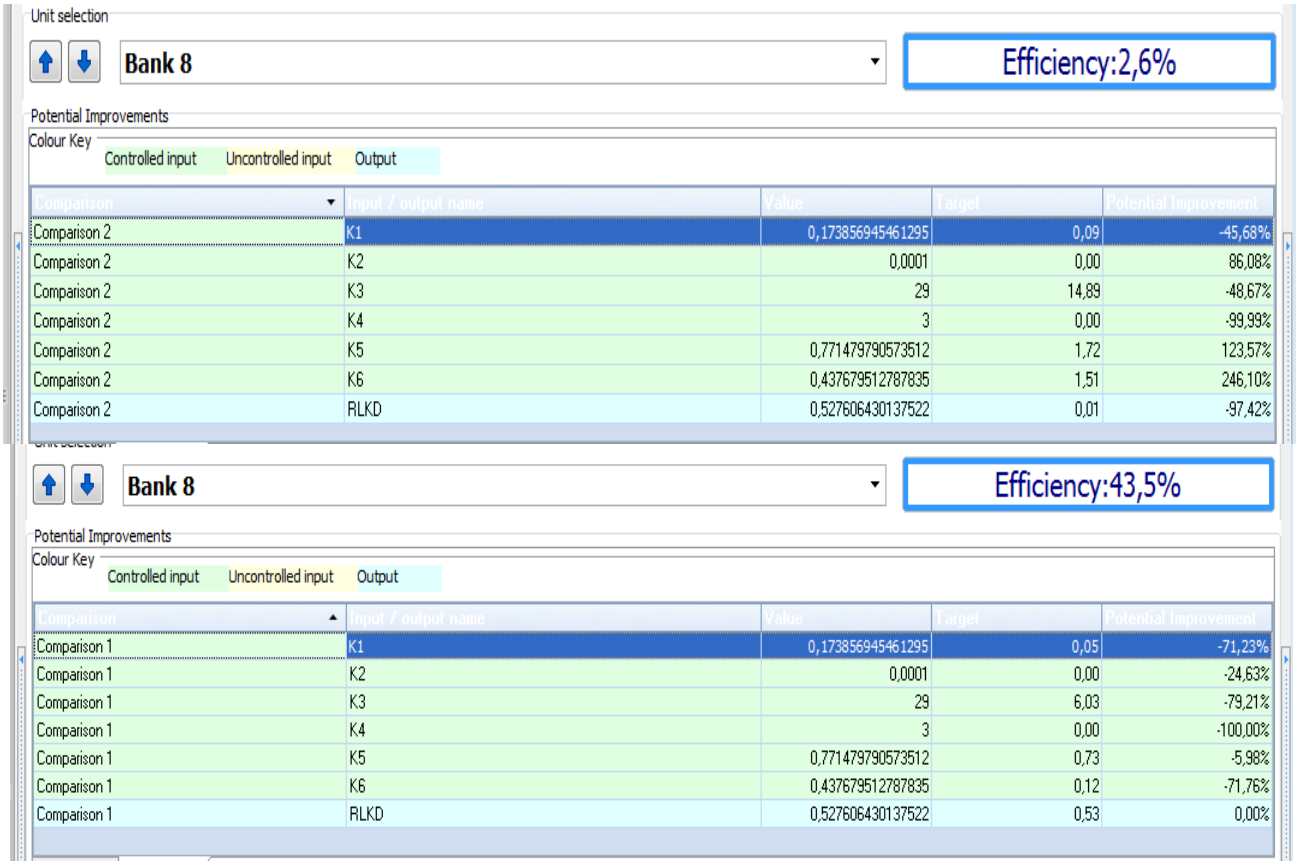


Рисунок 3.38 – Потенціал покращення фінансового моніторингу Банку8 станом на 2019 рік для CCR-моделі та для BCC-моделі

Вищеописані резюме у графічному та табличному вигляді можна надати по всім неефективним банкам, що нас цікавлять при дослідженні, аналогічно аналізу Банку 8. Так, для Банку 13 графік потенційних покращень (Додаток Е, рисунок Е.1 та Е.2) показує можливість покращення по зміним такі для BCC-моделі: К1 на 221,87%. Є можливість скорочення по наступних змінних для BCC-моделі: К2 на 100,00%, К3 на 94,39%, К4 на 100,0%, К5 на 92,71%, К6 на 83,3%, RLKD на 39,84%.

Аналогічно по графіках потенційних покращень у графічному та табличному вигляді зображено та проаналізовано кожен неефективний банк по першої групи (Додаток Е, рисунок Е.3-Е.8) та можна проаналізувати всі неефективні банки по усім шести групам..

4 етап. Проведення систематизації отриманих результатів та створення практичних рекомендацій стосовно покращення певних напрямків стратегічного управління банківськими установами в розрізі фінансового моніторингу. На даному етапі спочатку утворюються групи ефективно та неефективно працюючих банківських установ. Отже, на базі ґрунтовного аналізу таблиці 3.5 зроблено висновок для:

- вхідно-орієнтованої ВСС-моделі задачі дробно-лінійного програмування мінімізації умовних входів з постійною віддачею від масштабу про стабільну ефективну діяльність таких 14 банківських установ як: Банк 13, Банк 50, Банк 14, Банк 1, Банк 31, Банк 18, Банк 65, Банк 19, Банк 21, Банк 27, Банк 39, Банк 41, Банк 36, Банк 54; 3 банки: Банк12, Банк 15, Банк23 є дещо проблемними; найпроблемнішими банками в розрізі оцінювання технічної ефективності фінансового моніторингу визначено 17 банків: Банк 16, Банк 20, Банк 8, Банк 22, Банк 4, Банк 9, Банк 10, Банк 17, Банк 2, Банк 5, Банк 24, Банк 11, Банк 25, Банк 26, Банк 6, Банк 7, Банк 27.

- вихідно-орієнтовної CCR-моделі задачі дробно-лінійного програмування максимізації відношення умовних виходів з постійною віддачею від масштабу про стабільну ефективну діяльність таких 14 банківських установ як: Банк 16, Банк 14, Банк 1, Банк 10, Банк 18,Банк 5, Банк 65, Банк 12, Банк 19, Банк 21, Банк 39, Банк 41, Банк 36, Банк 54; 1 банк: Банк3 є дещо проблемним; найпроблемнішими банками в розрізі оцінювання технічної ефективності фінансового моніторингу визначено 19 банків: Банк 13, Банк 20, Банк 50, Банк 8, Банк 22, Банк 31, Банк 4, Банк 9, Банк 17, Банк 2, Банк 2, Банк 24, Банк 11, Банк15, Банк 23, Банк 25, Банк 26, Банк 6, Банк 7, Банк 27.

Таблиця 3.5 – Ефективність фінансового моніторингу банків України у 2019р.

Bank	BCC-модель	CCR-модель
1 група		
Bank 8	43,5%	2,6%
Bank 13	100,0%	60,2%
Bank 16	4,0%	100,0%
Bank 20	77,4%	4,1%
Bank 50	100,0%	3,3%
2 група		
Bank 1	100,0%	100,0%
Bank 4	75,8%	62,4%
Bank 9	60,4%	88,3%
Banj 14	100,0%	100,0%
Bank 22	86,9%	39,0%
Bank 31	100,0%	80,4%
3 група		
Bank 5	50,1%	100,0%
Bank 17	49,3%	52,7%
Bank 65	100,0%	100,0%
Bank 2	2,4%	6,1%
Bank 18	100,0%	100,0%
Bank 10	75,4%	100,0%
4 група		
Bank 6	54,9%	77,1%
Bank 7	40,1%	51,5%
Bank 11	65,2%	68,3%
Bank 12	95,4%	100,0%
Bank 15	91,3%	100,0%
Bank 19	100,0%	100,0%
Bank 21	100,0%	100,0%
Bank 23	94,3%	73,2%
Banj 24	70,1%	55,0%
Bank 25	49,4%	37,0%
Bank 26	62,8%	47,3%
Bank27	100,0%	88,3%
5 група		
Bamk 3	44,8%	90,1%
Bank 39	100,0%	100,0%
Bank 41	100,0%	100,0%
6 група		
Bank 36	100,0%	100,0%
Bank 54	100,0%	100,0%

Ефективною є робота фінансового моніторингу по обох моделях у 10 банків: Банк 14 (ВАТ "КРЕДОБАНК"), Банк 1 (КБ "ПРИВАТБАНК"), Банк 18 (ВАТ "ПІРЕУС БАНК МКБ"), Банк 65 (УКР.БАНК РЕКОНСТР.ТА РОЗВ.), Банк 19 (ВАТ "БАНК РУСКИЙ СТАНДАРТ"), Банк 21 (ЗАТ "КРЕДИТ ЄВРОПА БАНК"), Банк 39 (АБ "КЛІРИНГОВИЙ ДІМ"), Банк 41 (АКБ "АРКАДА"), Банк 36 (АКБ "АЛЬЯНС"), Банк 54 ("ПРИВАТІНВЕСТ").

Другою частиною цього етапу визначається наявний резерв та потенціал зростання ефективності фінансового моніторингу для групи в цілому, так і для кожного окремо взятого банку. Так, представлено наочну інтерпретацію доцільності активізації тих чи інших напрямків стратегічного управління банківських установ в частині фінансового моніторингу (таблиці 3.6 – 3.12).

Таблиця 3.6 – Потенціал зростання ефективності фінансового моніторингу для груп банків України у 2019р.

Показник	1 група банків		2 група банків		3 група банків	
	BCC-модель	CCR-модель	BCC-модель	CCR-модель	BCC-модель	CCR-модель
K1	-25,87%	10,52%	16,46%	22,19%	-1,99%	-21,48%
K2	-11,13%	-5,52%	-14,05%-	-9,78%	2,46%	-17,07%
K3	-16,5%	-8,29%	-8,8%	5,99%	-1,44%	-13,96%
K4	-24,6%	15,27%	-45,46%	-29,25%	-0,84%	-13,96%
K5	-8,04%	2,43%	-1,36%	12,1%	-5,89%	-15,86%
K6	-13,87%	40,68%	-13,87%	10,29%	0,11%	-17,65%
RLKD	0%	-17,29%	0%	-10,4%	87,28%	0%

Продовження таблиці 3.6

Показник	4 група банків		5 група банків		6 група банків	
	BCC-модель	CCR-модель	BCC-модель	CCR-модель	BCC-модель	CCR-модель
K1	-41,84%	-34,22%	-25,81%	-25,61%	15,96%	-10,67%
K2	-13,92%	3,56%	-2,63%	28,83%	18,36%	-12,27%
K3	-8,7%	18,22%	-27,02%	-28,45%	12,03%	-16,09%
K4	-8,82%	15,47%	-17,49%	-6,08%	13,36%	-17,88%
K5	0,65%	4,54%	-15,28%	-0,88%	16,14%	-10,79%
K6	-26,07%	-10%	-11,77%	7,35%	13,25%	-17,73%
RLKD	0%	-13,98%	0%	-2,8%	10,9%	-14,57%

Таблиця 3.7 – Потенціал зростання ефективності фінансового моніторингу для 1 групи банків України у 2019р.

Показник	1 група банків							
	Банк8		Банк13		Банк16		Банк20	
	BCC-модель	CCR-модель	BCC-модель	CCR-модель	BCC-модель	CCR-модель	BCC-модель	CCR-модель
К1	-71,23%	-45,68%	0,00%	221,87%	-95,26%	0,00%	-96,52%	41,44%
К2	-24,63%	86,08%	0,00%	-100,0%	-96,37%	0,00%	7,81%	-99,99%
К3	-79,21%	-48,67%	0,00%	-94,39%	-96,37%	0,00%	7,81%	-23,78%
К4	-100,0%	-99,99%	0,00%	-100,0%	-96,37%	0,00%	-53,79%	-100,0%
К5	-5,98%	123,57%	0,00%	-92,71%	-96,24%	0,00%	20,51%	10,83%
К6	-71,76%	246,10%	0,00%	-83,30%	-99,27%	0,00%	30,03%	173,91%
RLKD	0,00%	-97,42%	0,00%	-39,84%	0,00%	0,00%	0,00%	-95,90%

Продовження таблиці 3.7

Показник	1 група банків	
	Банк50	
	BCC-модель	CCR-модель
К1	0,00%	-16,88%
К2	0,00%	8,67%
К3	0,00%	8,67%
К4	0,00%	8,67%
К5	0,00%	4,67%
К6	0,00%	439,52%
RLKD	0,00%	-96,66%

Таблиця 3.8 – Потенціал зростання ефективності фінансового моніторингу для 2 групи банків України у 2019р.

Показник	2 група банків							
	Банк1		Банк4		Банк9		Банк14	
	BCC-модель	CCR-модель	BCC-модель	CCR-модель	BCC-модель	CCR-модель	BCC-модель	CCR-модель
К1	0,00%	0,00%	-24,35%	-0,17%	71,76%	194,13%	0,00%	0,00%
К2	0,00%	0,00%	-42,00%	-23,46%	-60,60%	-78,67%	0,00%	0,00%
К3	0,00%	0,00%	-38,49%	-18,83%	-43,14%	9,53%	0,00%	0,00%
К4	0,00%	0,00%	-100,0%	-100,0%	-53,31%	-85,78%	0,00%	0,00%
К5	0,00%	0,00%	24,72%	64,59%	-40,13%	22,64%	0,00%	0,00%
К6	0,00%	0,00%	-7,55%	22,00%	-16,24%	94,51%	0,00%	0,00%
RLKD	0,00%	0,00%	0,00%	-37,60%	0,00%	-11,68%	0,00%	0,00%

Продовження таблиці 3.8

Показник	2 група банків			
	Банк22		Банк31	
	BCC-модель	CCR-модель	BCC-модель	CCR-модель
K1	44,32%	66,13%	0,00%	16,73%
K2	44,32%	43,13%	0,00%	-63,09%
K3	44,32%	52,67%	0,00%	31,31%
K4	44,32%	-99,98%	0,00%	-79,24%
K5	44,32%	24,12%	0,00%	39,63%
K6	44,32%	-46,48%	0,00%	58,30%
RLKD	44,32%	-60,98%	0,00%	-19,56%

Таблиця 3.9 – Потенціал зростання ефективності фінансового моніторингу для 3 групи банків України у 2019р.

Показник	3 група банків							
	Банк5		Банк17		Банк65		Банк2	
	BCC-модель	CCR-модель	BCC-модель	CCR-модель	BCC-модель	CCR-модель	BCC-модель	CCR-модель
K1	-99,90%	0,00%	-99,98%	-89,41%	0,00%	0,00%	-98,72%	-99,92%
K2	35,91%	0,00%	-10,20%	-61,54%	0,00%	0,00%	81,02%	-88,95%
K3	35,91%	0,00%	79,61%	-23,07%	0,00%	0,00%	-100,00%	-100,0%
K4	35,91%	0,00%	79,61%	-23,07%	0,00%	0,00%	-99,99%	-100,0%
K5	-99,98%	0,00%	-99,98%	-39,85%	0,00%	0,00%	-99,54%	-99,97%
K6	-66,08%	0,00%	-79,93%	-65,55%	0,00%	0,00%	63,39%	-90,03%
RLKD	99,70%	0,00%	103,03%	0,00%	0,00%	0,00%	3982,41%	0,00%

Продовження таблиці 3.9

Показник	3 група банків			
	Банк18		Банк10	
	BCC-модель	CCR-модель	BCC-модель	CCR-модель
K1	0,00%	0,00%	202,41%	0,00%
K2	0,00%	0,00%	11,91%	0,00%
K3	0,00%	0,00%	-84,88%	0,00%
K4	0,00%	0,00%	-56,35%	0,00%
K5	0,00%	0,00%	14,86%	0,00%
K6	0,00%	0,00%	87,79%	0,00%
RLKD	0,00%	0,00%	32,58%	0,00%

Таблиця 3.10 – Потенціал зростання ефективності фінансового моніторингу для 4 групи банків України у 2019р.

Показник	4 група банків							
	Банк6		Банк7		Банк11		Банк12	
	BCC-модель	CCR-модель	BCC-модель	CCR-модель	BCC-модель	CCR-модель	BCC-модель	CCR-модель
К1	-99,94%	-92,51%	-89,82%	-74,58%	-94,94%	-92,24%	-98,51%	0,00%
К2	-23,56%	53,20%	-99,99%	-99,98%	-2,26%	49,84%	-9,69%	0,00%
К3	-23,56%	53,20%	-11,76%	120,26%	-2,26%	49,84%	-9,69%	0,00%
К4	-23,56%	53,20%	-11,76%	120,26%	-2,26%	49,84%	-9,69%	0,00%
К5	-30,95%	-5,71%	-51,56%	20,91%	-24,45%	15,83%	32,55%	0,00%
К6	-69,17%	-47,14%	-73,13%	-32,93%	-70,58%	-54,89%	5,57%	0,00%
RLKD	0,00%	-22,88%	0,00%	-48,55%	0,00%	-31,72%	0,00%	0,00%

Продовження таблиці 3.10

Показник	4 група банків							
	Банк15		Банк19		Банк21		Банк23	
	BCC-модель	CCR-модель	BCC-модель	CCR-модель	BCC-модель	CCR-модель	BCC-модель	CCR-модель
К1	-14,59%	-96,46%	0,00%	0,00%	0,00%	0,00%	-99,41%	-57,51%
К2	-9,03%	14,63%	0,00%	0,00%	0,00%	0,00%	1,58%	21,53%
К3	-9,03%	14,63%	0,00%	0,00%	0,00%	0,00%	-99,99%	-99,99%
К4	-9,03%	14,63%	0,00%	0,00%	0,00%	0,00%	1,58%	21,53%
К5	86,58%	54,80%	0,00%	0,00%	0,00%	0,00%	20,26%	-1,98%
К6	-61,41%	-27,00%	0,00%	0,00%	0,00%	0,00%	49,85%	53,37%
RLKD	0,00%	-16,73%	0,00%	0,00%	0,00%	0,00%	0,00%	-26,84%

Продовження таблиці 3.10

Показник	4 група банків							
	Банк24		Банк25		Банк26		Банк27	
	BCC-модель	CCR-модель	BCC-модель	CCR-модель	BCC-модель	CCR-модель	BCC-модель	CCR-модель
К1	-25,07%	-96,03%	-99,89%	-84,40%	-99,91%	-90,65%	0,00%	-96,76%
К2	-0,90%	59,43%	-99,99%	-99,98%	3,60%	84,36%	0,00%	-1,67%
К3	-0,90%	59,43%	3,47%	135,89%	3,60%	84,36%	0,00%	-1,67%
К4	-0,90%	59,43%	3,47%	135,89%	-100,0%	-99,99%	0,00%	-1,67%
К5	-14,71%	-9,66%	-11,22%	37,89%	4,65%	26,90%	0,00%	-35,26%
К6	-80,40%	-52,66%	-75,86%	-52,91%	-74,86%	-61,72%	0,00%	47,61%
RLKD	0,00%	-45,04%	0,00%	-63,00%	0,00%	-52,71%	0,00%	-11,69%

Таблиця 3.11 – Потенціал зростання ефективності фінансового моніторингу для 5 групи банків України у 2019р.

Показник	5 група банків					
	Банк3		Банк39		Банк41	
	BCC-модель	CCR-модель	BCC-модель	CCR-модель	BCC-модель	CCR-модель
К1	-95,52%	-90,01%	0,00%	0,00%	0,00%	0,00%
К2	-9,72%	101,31%	0,00%	0,00%	0,00%	0,00%
К3	-100,0%	-100,0%	0,00%	0,00%	0,00%	0,00%
К4	-64,73%	-21,36%	0,00%	0,00%	0,00%	0,00%
К5	-56,55%	-3,11%	0,00%	0,00%	0,00%	0,00%
К6	-43,57%	25,82%	0,00%	0,00%	0,00%	0,00%
RLKD	0,00%	-9,86%	0,00%	0,00%	0,00%	0,00%

Таблиця 3.12 – Потенціал зростання ефективності фінансового моніторингу для 6 групи банків України у 2019р.

Показник	6 група банків			
	Банк36		Банк54	
	BCC-модель	CCR-модель	BCC-модель	CCR-модель
К1	0,00%	0,00%	0,00%	0,00%
К2	0,00%	0,00%	0,00%	0,00%
К3	0,00%	0,00%	0,00%	0,00%
К4	0,00%	0,00%	0,00%	0,00%
К5	0,00%	0,00%	0,00%	0,00%
К6	0,00%	0,00%	0,00%	0,00%
RLKD	0,00%	0,00%	0,00%	0,00%

Отже, аналізуючи проведене дослідження, зазначимо, що в даній роботі було здійснена розробку економіко-математичної, структурно-логічної моделі ефективності фінансового моніторингу банків України в частині національної системи оцінки ризиків легалізації коштів, одержаних злочинним шляхом, фінансування тероризму та розповсюдження зброї масового знищення на основі проведення Data Envelpment Analysis з використанням середовища Frontier Analyst.

На базі виконання фронтірного DEA-аналізу середовища було побудовано вхідно-орієнтовану BCC-модель задачі дробно-лінійного програмування

мінімізації умовних входів та вихідно-орієнтовну CCR-модель задачі дробно-лінійного програмування максимізації умовних виходів з постійною віддачею від масштабу. При чому умовні входи розраховано на основі адитивної згортки зважених методом першої головної компоненти показників характеристики ефективності функціонування банків України.

Під час дослідження було сформовано групи ефективно та неефективно працюючих банків в розрізі фінансового моніторингу, визначено існуючий резерв та можливий потенціал покращення ефективності і для групи відібраних банків в цілому, і для окремо взятого банку. Кластеризацію банків проведено шляхом застосування методу k-середніх. Далі проілюстровано графічну інтерпретацію поточної позиції конкретних банків відносно конкурентів-конкурентів в середовищі діяльності на банківському ринку в розрізі різних напрямків стратегічного управління.

Запропоновану модель можна використовувати при введенні нагляду на базі оцінки ефективності банківських установ України у розрізі виконання ними вимог нормативно-законодавчих актів з питань фінансового моніторингу. Описаний підхід з використанням Frontier Analyst надає можливість провести порівняльний аналіз ефективності; побудувати візуалізацію вагомої для подальшої діяльності інформації; здійснювати ефективніший розподіл наявних ресурсів; знаходити інформацію, потрібну при розробленні стратегії планування; визначати найгірші та найкращі одиниці дослідження; глибше вивчати показники, характеристики та одиниці дослідження.

Підрозділ 3.2 даного звіту було виконано із використанням матеріалів публікацій виконавців [229, 230, 231, 232].

3.3 Розробка методологічного підґрунтя підвищення ефективності організації системи кіберзахисту в банках

3.3.1 Шляхи підвищення ефективності забезпечення кібербезпеки банку

Цифрова економіка представляє значну частину світової економіки і за оцінками Конференції ООН по торгівлі та розвитку (UNCTAD) досягне на початку третього десятиріччя XXI століття 15,5% світового ВВП. Фінансовий сектор, більша частина якого припадає на банківський сегмент, має значний потенціал щодо цифровізації, яку найбільш активно впроваджують банківські установи [233]. В першу чергу це стосується мобільного банкінгу. Проведене Juniper Research дослідження Digital Banking: Banking-as-a-Service, Open Banking & Digital Transformation 2020-2024 показує, що до 2024 року кількість користувачів цифрового банкінгу досягне 3,6 млрд, що на 54 % більше, ніж у 2020 році.

В той же час банки є об’єктами критичної інфраструктури України [234]. Через велику кількість грошових коштів, сконцентрованих на банківських рахунках, різноманітність електронних банківських послуг і значну кількість клієнтів, які користуються цими послугами, саме банківські установи найбільше приваблюють кіберзлочинців. Кількість кіберінцидентів у фінансовому секторі постійно збільшується, а їх наслідки призводять до значних фінансових втрат, витоку важливої інформації, погіршення репутації фінансових установ, втрати довіри населення [235]. Вплив цифровізації поширюється на весь ландшафт операційних ризиків, головним серед яких, на думку топ-менеджерів, є ризик кібершахрайства [236]. Майже 80 відсотків фінансових установ впроваджують цифрові технології швидше, ніж забезпечують їх кіберзахист [237]. Як зазначено в роботі [238], до ключових загроз цифрової економіки відносяться несправності IT-систем, що спричинені кібератаками, а також недооцінка ризиків, пов’язаних з цифровими технологіями, і, як наслідок, ризик стати жертвою кібершахрайства.

Згідно звіту про глобальні ризики Всесвітнього економічного форуму кібератаки та кібершахрайства входять до топової п’ятірки глобальних ризиків за частотою появи [239]. Тільки в Україні за 9 місяців 2020 року було зафіксовано 1,2 млн. кіберінцидентів, серед яких – поширення шкідливого програмного забезпечення, фішинг, DDOS-атаки [240].

Цифровізація фінансового сектору збільшує кількість кіберінцидентів, яким не можна повністю запобігти [241]. Сьогодні в світі протидія кіберзлочинності визнана пріоритетною проблемою, вирішення якої потребує проведення ґрунтовних наукових досліджень. Актуальною є проблема забезпечення кіберстійкості фінансового сектору до шахрайських дій і, як наслідок, виконання фінансовим сектором покладених на нього функцій в непередбачуваних несприятливих умовах. Як зазначено в роботі [241], цілями кіберстійкості є попередження кіберзагроз, протистояння кібератакам, відновлення (подолання шкоди, заподіяної кіберінцидентами) та адаптація до кіберризиків. Слід відмітити, що сьогодні в сфері кібербезпеки домінують два міжнародних стандарти, які хоч і не декларують кіберстійкість своєю метою, але включають заходи, що можуть бути використані для досягнення цілей кіберстійкості: серія міжнародних стандартів ISO 27000 і Cybersecurity Framework від NIST (Національний інститут стандартів і технологій США). Серія міжнародних стандартів ISO 27000 містить наступні заходи, що сприяють кіберстійкості [242]: поінформованість про інформаційну безпеку, освіта та навчання; резервне копіювання інформації; навчання на інцидентах інформаційної безпеки тощо. NIST Cybersecurity Framework описує такі функції кіберзахисту, як ідентифікація, захист, виявлення та відновлення [243].

Ефективність захисту інформаційних активів банківської установи (матеріальних або нематеріальних об’єктів, що є інформацією або містять інформацію, слугують для обробки, зберігання або передачі інформації та мають цінність для банку [93]) безпосередньо впливає на конкурентоспроможність банківської установи. На державному рівні основним суб’єктом забезпечення кібербезпеки в банківському секторі є Національний банк України. Водночас на

рівні бізнесу за кібербезпеку банківської установи відповідає її власник. Тому одним із шляхів протидії кіберзлочинності є впровадження внутрішньобанківської системи кібербезпеки та оцінка ефективності її роботи.

Дослідження [244] показало, що менеджмент банку в першу чергу піклується про цілісність даних, втрату або розкриття даних (особливо персональних даних клієнтів банку), вразливості (кібератаки на аутсорсингові компанії, внутрішні загрози, а також кібернетичні ризики, пов'язані з використанням банком хмарних технологій), операційну стійкість банку (його спроможність відновити операційну діяльність після кібератаки та надати клієнтам доступ до банківських сервісів). Інструменти для здійснення кібератак невпинно розвиваються та стають доступнішими. У багатьох випадках кіберзлочини здійснюються за участі персоналу банку, а також із використанням методів соціальної інженерії. Спостерігається сплеск нових загроз у сфері соціальних мереж, мобільних пристроїв, а також хмарних технологій. Дослідження компанії EPG виявило такі слабкі сторони в забезпеченні кібербезпеки банків, як відсутність форензік-аналізу для визначення першопричин інцидентів інформаційної безпеки, відсутність необхідних даних для точного усвідомлення ситуації, відсутність ретроспективного аналізу та оперативної адаптації системи кіберзахисту для запобігання подібних атак в майбутньому [245].

Аналіз наукових публікацій в сфері кібербезпеки дозволяє виділити організаційний та технологічний аспекти забезпечення кіберстійкості банківської установи. Організаційне забезпечення має поєднати всіх суб'єктів банківського менеджменту, долучених до процесів забезпечення кібербезпеки, управління кіберризиками та безперервності банківського бізнесу. Існують фундаментальні принципи, властиві організаціям, що ефективно функціонують. У середовищі фахівців з організаційного управління добре відома кібернетична модель життєздатної системи VSM (Viable Systems Model), розроблена С. Біром [246]. Принципами VSM є керованість, здатність до навчання, адаптації та розвитку, що відповідають наведеним вище цілям кіберстійкості.

VSM має п’ять базових управлінських функцій (підсистем): операційної діяльності, координації, контролю, розвитку, формування політики. Постулюється принцип: кожна життєздатна система містить в собі життєздатну систему і сама є елементом життєздатної системи. Така самоподібність вважається запорукою життєздатності. Кожній з п’яти підсистем, які включає в себе життєздатна система, повинно бути надано стільки автономії, наскільки це можливо без порушення цілісності системи.

В основу моделі життєздатної системи С. Біра покладено «закон необхідної різноманітності», сформульований Р. Ешбі, який вимагає, щоб набір управлінських впливів був не менш різноманітним, ніж набір можливих станів системи. Згідно цього закону управління полягає в такому перетворенні множини станів керованої системи, в результаті якого ймовірності небажаних станів зменшуються, а ймовірності бажаних станів збільшуються. Управління складністю системи здійснюється за допомогою самоорганізації (рис. 3.39).

Рис. 3.39 – Система взаємовідносин в процесі управління складністю системи відповідно до концепції VSM

Згідно Закону України «Про основні засади забезпечення кібербезпеки України», кіберпростір – це середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з’єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі

Інтернет та/або інших глобальних мереж передачі даних. У фінансовому секторі кіберризики відносяться до операційних ризиків. Різноманітність середовища більша за різноманітність технологічних операцій бізнес-підрозділів, яка, в свою чергу, перевищує різноманітність керування. В структурі правильно організованої системи відбувається спрямоване звуження різноманітності середовища (аттенюація) з одночасним збільшенням різноманітності управління (підсилення).

Розглянемо побудовану нами з використанням принципів теорії життєздатних систем С. Біра узагальнену модель механізму забезпечення кіберстійкості фінансового сектору, представлену в наочному вигляді на рис. 3.40.

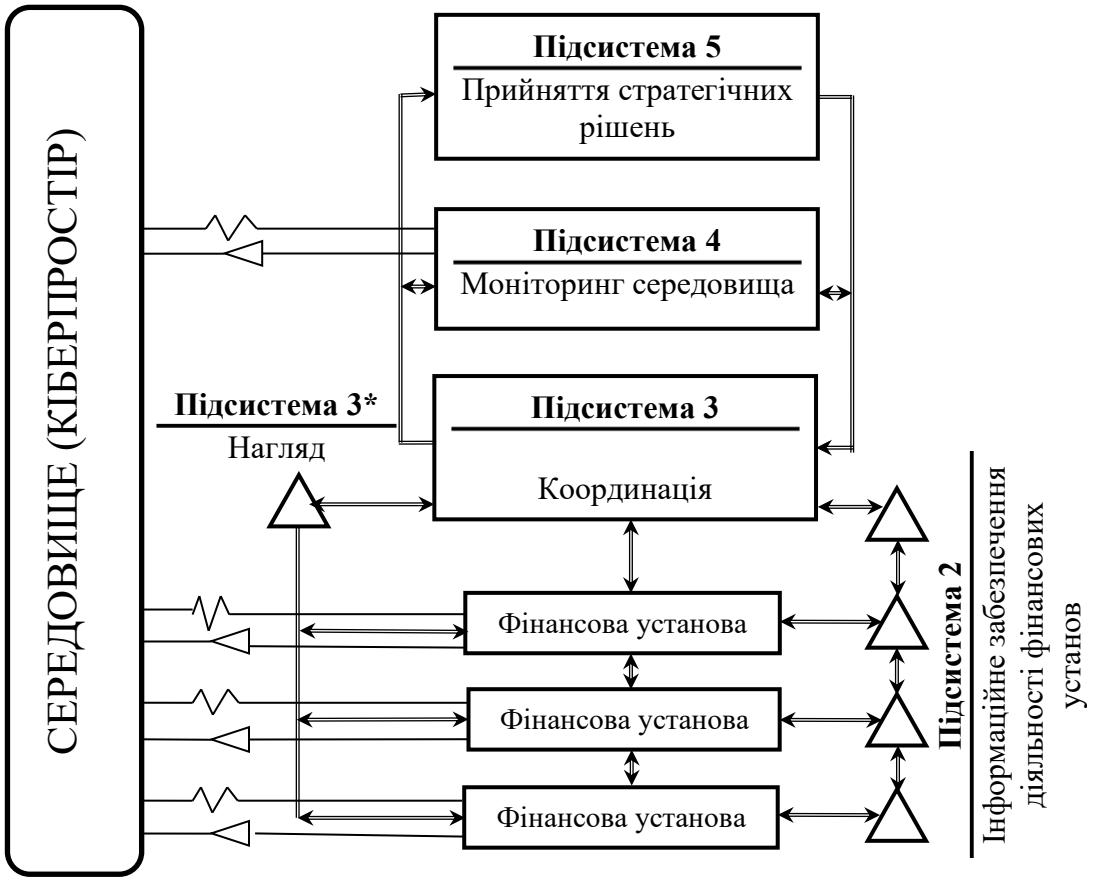


Рис. 3.40 – Модель механізму забезпечення кіберстійкості фінансового сектору

Підсистема 1 представлена у вигляді фінансової установи, яка здійснює свою діяльність у відповідності з отриманими ліцензіями. Кожна Підсистема 1

виконує свої функції в рамках горизонтальної площини, взаємодіючи в кіберпросторі та підкоряючись власній системі управління кіберризиками. Кожна фінансова установа самостійно обирає модель організаційної побудови системи управління кіберризиками. При цьому враховуються особливості діяльності фінансової установи, рівень цифровізації фінансових послуг, інформаційна інфраструктура, а також наявні можливості та потреби у сфері забезпечення кіберстійкості та управління кіберризиками. Один з можливих варіантів такої моделі представлено на рис. 3.41.

Рис. 3.41 – Модель організаційної побудови системи управління кіберризиками фінансової установи

Першу лінію захисту від кіберризиків утворюють бізнес-підрозділи та підрозділ інформаційної безпеки. Другу лінію захисту утворює підрозділ з управління операційними ризиками, який здійснює комплаєнс-контроль бізнес-підрозділів. Третю лінію захисту утворює підрозділ внутрішнього аудиту, який

не бере безпосередньої участі в управлінні кіберризиками. Його роль полягає в оцінці загальної ефективності дій, що виконуються першою та другою лініями захисту. Внутрішній аудит кібербезпеки є важливою складовою забезпечення кібербезпеки. Він дозволяє об'єктивно оцінити рівень кібербезпеки банку в умовах постійного впливу зовнішніх і внутрішніх загроз, а також дотримання вимог національного законодавства, нормативних вимог регулятора та міжнародних стандартів інформаційної безпеки. В банку повинна бути передбачена можливість аудиту кібербезпеки аутсорсингових організацій, яким передана частина операційних процесів банку, бо таким чином банк потрапляє у залежність від стану кібербезпеки цих організацій [93]. Для актуалізації плану роботи підрозділу внутрішнього аудиту його керівник повинен бути підзвітним безпосередньо члену наглядової ради, що очолює аудиторський комітет, щоб знати, управління якими ризиками є наразі пріоритетним.

Важливо також періодично проводити незалежне зовнішнє оцінювання якості методичного забезпечення та інструментарію внутрішнього аудиту кібербезпеки, кваліфікації персоналу підрозділу внутрішнього аудиту, результатів роботи та якості звітності внутрішнього аудиту. Одним із результатів незалежного зовнішнього оцінювання є дорожна карта з поліпшення якості роботи підрозділу внутрішнього аудиту в напрямі забезпечення кібербезпеки банку. Згідно Постанови НБУ «Про затвердження Положення про організацію внутрішнього аудиту в банках України» №311 від 10.05.2016 у 2020 році завершується п'ятирічний етап, протягом якого вітчизняні банки зобов'язані пройти зовнішнє оцінювання функції внутрішнього аудиту. Зауважимо, що з 01.07.2020 року в Україні Національний банк України є регулятором як ринку банківських фінансових послуг, так і ринків небанківських фінансових послуг. Комітет кіберстійкості бізнесу (див. рис. 3.41) є колегіальним органом з ключовими повноваженнями в цій сфері. До його складу доцільно включити членів Правління, які відповідають за безперервність банківського бізнесу, управління кіберризиками та якість інформаційної інфраструктури.

Підсистема 1 (фінансова установа) сама є життєздатною системою відповідно до рекурсивного характеру моделі життєздатної системи. Вона автономно утримує свої параметри кіберстійкості на цільовому рівні шляхом активного реагування на кіберзагрози. В роботі [247] запропоновано оцінювати кіберстійкість за наступними рівнями:

- нормальний рівень кіберстійкості, що характеризується цільовим рівнем всіх параметрів кіберстійкості, контрольованим рівнем кіберризиків, безперервністю та стійкістю бізнесу;
- низький рівень кіберстійкості, що характеризується стійким погіршенням всіх параметрів кіберстійкості, зростанням рівня кіберризиків, зростанням термінів, необхідних для відновлення безперервності бізнесу;
- критичний рівень кіберстійкості, що характеризується зниженням параметрів кіберстійкості до критичного рівня, невиконанням державних регуляторних вимог, значними порушеннями в безперебійності бізнесу.

Мета Підсистеми 2 – запобігання некерованим коливанням, що виникають між різними підсистемами життєздатної системи. Вона забезпечує обмін інформацією між Підсистемами 1 та Підсистемою 3 для контролю і координації діяльності Підсистем 1. В концепції механізму забезпечення кіберстійкості фінансового сектору Підсистема 2 представлена законами, підзаконними актами, постановами Національного банку України та іншими нормативними документами у сфері кібербезпеки, які регулюють діяльність фінансових установ. Функції Підсистеми 2 відносяться до функцій Департаменту безпеки Національного банку України та Управління фінансових та операційних ризиків. Однією з основних функцій Департаменту безпеки є розроблення та реалізація стратегії і політики інформаційної безпеки Національного банку України, впровадження новітніх технологій у частині забезпечення ефективного і цілеспрямованого захисту інформації в інформаційній інфраструктурі Національного банку України та банківської системи України.

Для покращення стану кібербезпеки банку необхідно привести у відповідність міжнародним стандартам систему управління інформаційною

безпекою банку [242]. Запровадження у банку міжнародних стандартів інформаційної безпеки дозволяє оптимізувати витрати на забезпечення кібербезпеки, знизити ймовірність реалізації кіберризиків, здійснювати їх моніторинг та оцінку, розробити ефективну політику інформаційної безпеки та забезпечити її якісне виконання. Постанова НБУ «Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України» №95 від 28.09.2017 року передбачає впровадження банками системи управління інформаційною безпекою згідно з Національними стандартами ДСТУ ISO/IEC 27001:2015 «Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Вимоги» та ДСТУ ISO/IEC 27002:2015 «Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Звід практик щодо заходів інформаційної безпеки», розробленими на основі міжнародних стандартів серії ISO 27k, які забезпечують відповідність вимогам Базельського комітету Basel II щодо зменшення операційних ризиків банків.

Згідно зі стандартом ДСТУ ISO/IEC 27001:2015 реалізація заходів інформаційної безпеки повинна відбуватись за допомогою політики інформаційної безпеки, яка визначає організаційні засади, напрями і цілі цих заходів, а також принципи діяльності у галузі інформаційної безпеки та кіберзахисту. Незважаючи на загальні принципи забезпечення інформаційної безпеки та кіберзахисту у банківській сфері, кожен з банків розробляє власну політику інформаційної безпеки, яка базується на результатах аудиту інформаційної інфраструктури та засобів кіберзахисту банку. Метою впровадження політики інформаційної безпеки банку є забезпечення надійного функціонування інформаційних систем банку та зниження збитків, що можуть наступити внаслідок реалізації інцидентів інформаційної безпеки. Політику інформаційної безпеки необхідно періодично переглядати з метою приведення у відповідність потребам бізнесу та стратегії розвитку банку.

Підсистема 3 є системою координації. Вона виконує роль арбітра при виникненні нетипових проблем і забезпечує взаємодію з Підсистемами 4 і 5. Підистема 3* здійснює аудит і виявляє неусвідомлені системами 1 проблеми.

Підсистема 4 – система моніторингу внутрішнього та зовнішнього середовища. Функції моніторингу відносяться до функцій Центру кіберзахисту, що входить до складу Департаменту безпеки НБУ, який співпрацює з Державним центром кіберзахисту Державної служби спеціального зв'язку та захисту інформації України, підрозділом якого є урядова команда реагування на комп'ютерні надзвичайні події України (CERT-UA). НБУ співпрацює також із Національним координаційним центром кібербезпеки, який є робочим органом РНБО, та Департаментом кіберполіції Національної поліції України. Згідно Закону України «Про основні засади забезпечення кібербезпеки України» суб'єкти забезпечення кібербезпеки в межах своєї компетенції:

– здійснюють виявлення і реагування на кіберінциденти та кібератаки, усунення їх наслідків;

– здійснюють інформаційний обмін щодо реалізованих та потенційних кіберзагроз;

– розробляють і реалізують запобіжні, організаційні, освітні та інші заходи у сфері кібербезпеки;

– забезпечують проведення аудиту інформаційної безпеки, у тому числі на підпорядкованих об'єктах та об'єктах, що належать до сфери їх управління.

Одним з основних шляхів підвищення ефективності забезпечення кібербезпеки банку в організаційному аспекті, на нашу думку, є покращення взаємодії суб'єктів забезпечення кібербезпеки в банківській сфері. Система моніторингу повинна здійснювати оцінку діяльності фінансових установ з точки зору кіберстійкості, проведення регулярних сканувань для визначення уразливостей в технологіях і бізнес-процесах фінансових установ, тестування на проникнення. Результати такого моніторингу використовуються при плануванні розвитку кіберстійкості фінансового сектору.

У провідній компанії в галузі бізнес-аналітики SAS Institute вважають, що новими викликами у сфері кібербезпеки є зростаюче розмаїття кіберзагроз, необхідність швидкої обробки даних про кібератаки, велика кількість повідомлень, що генеруються системою кіберзахисту та вимагають оперативного реагування, управління великими масивами даних, аналіз і модернізація системи кіберзахисту на підставі нових відомостей [248]. Тому для підвищення ефективності протидії кібератакам важливо забезпечити обмін інформацією про інциденти інформаційної безпеки. Покращення взаємодії суб'єктів забезпечення кібербезпеки в банківській сфері ми вбачаємо у впровадженні Security Operations Center (центру моніторингу та реагування на інциденти інформаційної безпеки), архітектура якого складається з двох основних компонентів:

1) розподіленої системи збору подій інформаційної безпеки, розгорнутої в рамках інформаційної інфраструктури банку, яка відповідає за збір і первинну обробку подій інформаційної безпеки з підключених джерел (серверів, що забезпечують обробку пластикових карт, міжмережевих екранів, мережевого обладнання, системи автентифікації, контролю цілісності, антивірусів тощо);

2) центрального ядра, що відповідає за автоматичне виявлення інцидентів інформаційної безпеки на підставі даних, отриманих від розподіленої системи збору подій інформаційної безпеки, а також зберігання подій інформаційної безпеки для їх ретроспективного аналізу.

Такий підхід надає можливість застосовувати для аналізу даних щодо реалізованих та потенційних кіберзагроз технології штучного інтелекту, машинного навчання та аналітики великих даних, виявляти та попереджувати кібершахрайства.

Підсистема 5 – система прийняття рішень. При ухваленні рішень на цьому рівні використовується інформація про стан автономного управління, що йде нагору від Підсистеми 3, та результати моніторингу, надані Підсистемою 4. Основні функції по прийняттю рішень лежать на регуляторі. Згідно з Законами

України «Про Національний банк України» та «Про основні засади забезпечення кібербезпеки України», а також Стратегією кібербезпеки України на Національний банк України покладено завдання із встановлення правил захисту інформації, визначення порядку, вимог і заходів із забезпечення кіберзахисту та інформаційної безпеки в банківській системі України та здійснення контролю за їх виконанням.

Стійкість фінансового кіберпростору забезпечуватиметься шляхом виконання двох основних умов: кіберстійкості Підсистем 1 та існування й ефективній взаємодії Підсистем 2-5.

У технологічному аспекті основним шляхом підвищення ефективності забезпечення кібербезпеки банку ми вбачаємо впровадження інноваційних технологій у сфері кіберзахисту. Для протидії кіберзагрозам в усьому світі традиційно використовують системи виявлення вторгнень IDS (Intrusion Detection System), що інформують про можливі порушення, та системи запобігання вторгненням IPS (Intrusion Prevention System), що відстежують трафік і здатні виявляти та блокувати потенційні небезпеки. Обмеженням у використанні цих систем є той факт, що вони засновані на виконанні певних правил реагування, які технічно неможливо неперервно поновлювати, і тому не здатні реагувати на нові кіберзагрози. Інноваційними у сфері кіберзахисту є системи управління інформацією про безпеку та поточні події SIEM (Security Information and Event Management), здатні обробляти дані в реальному часі та вчасно виявляти спроби вторгнення, хоча й вони мають певні недоліки, наведені, наприклад, у [245]. Популярною в банківській сфері стає біометрична ідентифікація, зокрема ідентифікація клієнта по відбитку пальця та розпізнавання його по голосу при звертанні до call-центру. Банки все частіше використовують аналітичні технології великих даних (BigData Analytics) для захисту від шахрайств із грошовими транзакціями та пластиковими картками. Інноваційною є технологія блокчейн, яка дозволяє зберігати інформацію у відкритому доступі для зацікавлених осіб, які не можуть змінювати раніше

внесені дані. Її використовують такі провідні банки, як CreditSuisse, GoldmanSachs, JP Morgan, Barclays.

З аналізу сучасних досліджень і відкритих наукових публікацій встановлено, що на теперішній час не існує єдиного підходу до оцінки ефективності внутрішньобанківської системи кібербезпеки. Слід враховувати, що якщо для інфраструктурної кібербезпеки більш важлива доступність до інформаційного активу, то у випадку кібербезпеки банківського бізнесу більш важливе значення має конфіденційність і цілісність інформації.

У роботі [249] наведена наступна класифікація моделей, що лежать в основі практично всіх відомих методик оцінювання ефективності комплексних систем захисту інформації (СЗІ):

– за цільовою спрямованістю (оціночні);
– за ієрархічною структурою (однорівневі);
– за способом опису функціональних зв’язків (аналітичні);
– за способом урахування випадкових факторів (комбіновані);
– з точки зору врахування стохастичної невизначеності (ймовірнісні).

В роботі [250] наведена класифікація існуючих підходів до оцінки ефективності комплексних СЗІ:

– статистичний (базується на статистичній обробці загроз і їх наслідків);
– імовірнісний (базується на розрахунку сумарних середніх втрат, використовує імовірність відмови системи в результаті реалізації загроз);
– частотний (базується на визначенні очікуваного збитку від реалізації загрози, використовує показник частоти виникнення загрози);
– експертний (базується на визначенні ступеня забезпечення безпеки системи, використовує суб’єктивні оцінки експертів);
– інформаційно-ентропійний (базується на обчисленні інформаційної ентропії системи, використовує поняття згортки функції);
– нечітко-множинний (базується на поданні показників захищеності інформаційної системи у вигляді лінгвістичних змінних);

– мінімізації ризиків (базується на розрахунку показників, що характеризують ризики, та економічного ефекту від управління ризиками);

– матричний (формальні моделі захисту);

– багаторівневий (стан системи захисту описується сукупністю рівнів конфіденційності та набором категорій конфіденційності);

– оптимізаційний (комбінаторний).

Наголошується, що рівень захищеності об’єкта може характеризуватися ефективністю СЗІ.

В роботі [251] для оцінки ефективності СЗІ використовується метод порівняльного багатовимірного аналізу. Він передбачає побудову матриці відстаней між показниками захищеності, що оцінюються, на основі матриці їх нормованих ознак. Матриця відстаней дає можливість впорядкувати показники захищеності за ступенем важливості, встановити залежності між ними та оцінити ступінь їх взаємного впливу. На нашу думку, даний метод може бути застосований і для оцінки ефективності захисту інформаційних активів банку системою кібербезпеки.

У роботі [252] зазначено, що на сьогоднішній день найбільш розповсюдженим на практиці підходом для оцінювання захищеності системи є використання критерію ризику, що вимірюється потенційними втратами від реалізації загроз. Згідно міжнародного стандарту ISO/IEC 27005:2011 «Інформаційні технології. Методи забезпечення безпеки. Управління ризиками інформаційної безпеки» ризик інформаційної безпеки визначається як потенційна можливість використання вразливості активу або групи активів конкретною загрозою для нанесення збитку організації. У роботі [253] оцінка рівня ефективності впровадження системи інформаційної безпеки передбачає розрахунок показника очікуваних фінансових втрат від реалізації загроз, який визначається на підставі ступеня тяжкості потенційної загрози, і зіставлення його з витратами на захист інформації з подальшою градацією ефективності витрат за якісними рівнями. Автор використовує суб’єктивні оцінки, але не зазначає принципи їх розрахунку, через що, на нашу думку, даний

метод має обмежене застосування. Зауважимо також, що в наукових публікаціях відсутній єдиний підхід до розрахунку витрат на захист інформації (проектування та функціонування СЗІ).

У роботі [254] для оцінки ефективності СЗІ запропоновано використовувати економічний критерій виду «ефективність-вартість» у вигляді суми очікуваного можливого збитку від реалізації загроз і витрат на побудову СЗІ, де значення очікуваного збитку від реалізації конкретної загрози розраховується як добуток величини збитку від реалізації загрози та ймовірності її реалізації. На нашу думку, оцінку ефективності за цим критерієм найкраще проводити в динаміці, щоб побачити, чи зростає значення критерію при постійних витратах на СЗІ, а може залишається на досягнутому рівні при зниженні витрат на СЗІ. Недоліком даного підходу є оцінка ймовірності реалізації загрози. Статистика появи загроз та реалізованих кібератак на інформаційні активи накопичується, по-перше, в банківській установі з уже впровадженою системою кібербезпеки та, по-друге, на протязі певного часу і потребує відповідної статистичної обробки.

Відомо, що в переважній більшості випадків на безпеку інформаційного активу впливає декілька загроз, які можуть бути спрямовані на різні його властивості (конфіденційність, цілісність, доступність та спостережність). У роботі [255] запропоновано метод оцінки ефективності системи захисту інформації, перший етап якого передбачає визначення важливості кожного ресурсу системи, що захищається, як середньоарифметичного значення оцінок рівнів його властивостей. У роботі [254] важливість ресурсу системи, що захищається, запропоновано визначати як наслідки втрати інформації в разі реалізації загрози. Другий етап методу оцінки ефективності системи захисту інформації передбачає визначення експертним шляхом бальної оцінки рівня реалізації загрози в залежності від її частоти та рівня складності. Третій етап передбачає визначення остаточного рівня загрози після проходження механізму захисту. Далі визначається рівень ризику, що створюється загрозою для ресурсу системи, як добуток важливості ресурсу та остаточного рівня загрози після

проходження механізму захисту. На цій основі робиться експертний висновок щодо ефективності роботи системи захисту інформації. Розглянутий метод використовує суб'єктивні оцінки експертів, а також положення теорії нечіткої логіки при визначенні рівня зниження загрози механізмом захисту [256].

У роботі [257] зазначено, що оцінка рівня кібербезпеки відноситься до класу багатокритеріальних задач, а для її вирішення в умовах невизначеності найбільш раціональними є експертні методи, зокрема, метод анкетування [258]. Перший етап запропонованої в [257] методики розрахунку кіберзахищеності включає визначення компонентів системи (інформаційно-телекомунікаційного вузла), які необхідно захищати (зокрема, телекомунікаційне обладнання, засоби IP-телефонії, сервери та автоматизовані робочі місця, міжмережеві екрани, мережеві сервіси, операційні системи, застосунки користувачів тощо), та обчислення їх вагових коефіцієнтів із використанням рангових оцінок і методу парних порівнянь Сааті [259]. Чим більше ранг, тим більша важливість компонента, яка оцінюється експертами з позицій впливу компонента на працездатність, кіберзахищеність та безпечний стан системи в цілому. Оцінка кіберзахищеності кожного компонента здійснюється за критеріями кіберзахищеності згідно вимог нормативних документів технічного захисту інформації та індикаторів міжнародних стандартів захисту NIST SP 800-53 [260] або DOD 8530.01 [261]. Показник кожного критерія кіберзахищеності розраховується як середньоарифметичне значення оцінок експертів, отриманих за формулою нормованої суми бальних оцінок рівня кіберзахищеності згідно критерію, що розглядається, та вірогідності виникнення кіберзагрози. На цій основі формується матриця показників кіберзахищеності для кожного компонента системи, яку необхідно захищати, та розраховується підсумковий показник кіберзахищеності як зважена та нормована оцінка індикаторів стану кіберзахищеності компонентів. У свою чергу індикатор стану кіберзахищеності кожного компонента розраховується як середньоарифметичне значення показників кіберзахищеності цього компонента. На нашу думку, розглянутий підхід є універсальним по своїй суті та після відповідного доопрацювання може

може бути застосований для оцінки ефективності внутрішньобанківської системи кібербезпеки.

У роботі [262] в основу моделі оцінювання рівня захищеності системи покладена декомпозиція комплексної СЗІ на ієрархічні рівні, для кожного з яких обчислюється інтегральний показник рівня захищеності інформації як послідовна згортка часткових для нього показників нижнього рівня з використанням математичного апарату нечітких множин. У роботі [263] для розрахунку загального показника якості СЗІ використовувалась адитивна згортка часткових показників захищеності, отриманих як адитивна згортка характеристик часткового показника захищеності. Значення характеристик були подані у вигляді нечітких термів із трапецієподібними функціями належності, з ваговими коефіцієнтами, значення яких були подані у вигляді нечітких термів із трикутними функціями належності. Дефазифікація отриманого нечіткого значення часткового показника здійснювалась із використанням центроїдного методу з наступною природною нормалізацією отриманого чіткого значення часткового показника. Економічний ефект від впровадження СЗІ розраховувався як різниця між вартістю інформації та приведеною вартістю проекта СЗІ (NPV). На нашу думку, подання часткових показників як у числовому, так і в лінгвістичному вигляді, уможливлює аналіз значної кількості якісної інформації, отриманої від експертів і доповненої кількісними даними.

У роботі [264] запропоновано підхід до оцінки інформаційної безпеки організації на основі критерію впевненості в тому, що в організації реалізується прийнята політика безпеки. Цей підхід використовує вербально-числову шкалу та функцію бажаності Харингтона.

Ми погоджуємося з думкою автора роботи [265], що багато ідей, які лежать в основі кількісних методів оцінювання ефективності впровадження проектів інформатизації, можуть бути використані і для оцінювання економічної ефективності комплексної СЗІ: фінансові (метод окупності інвестицій ROI, метод визначення економічної добавленої вартості EVA, метод визначення сукупної вартості володіння TCO, метод визначення чистої приведеної вартості

NPV, метод визначення сукупного економічного ефекта TEI, метод швидкого економічного обгрунтування REJ), імовірнісні (метод справедливої оцінки опціонів ROV, метод прикладного інформаційного аналізу AIE). Вважаємо, що ці методи можуть бути використані також і для оцінювання ефективності кібербезпеки банківського бізнесу але потребують суттєвого переосмислення та вдосконалення.

Підсумовуючи вищенаведене, можемо представити результати порівняльного аналізу типових методів оцінки ефективності внутрішньобанківської системи кібербезпеки як складної системи з невизначеністю у вигляді наступної таблиці 3.13.

Таблиця 3.13 – Порівняльний аналіз методів оцінки ефективності внутрішньобанківської системи кібербезпеки

Група методів оцінки ефективності внутрішньобанківської системи кібербезпеки	Основні характеристики	Урахування невизначеності
Кількісні (метод порівняльного багатовимірного аналізу, метод зіставлення очікуваних втрат від потенційних загроз із витратами на захист інформації, критерій «ефективність-вартість», фінансові, ймовірнісні)	Базуються на традиційному математичному апараті	Невизначеність враховується за допомогою засобів статистики, теорії ймовірностей і експертних оцінок із використанням бальних шкал
Якісні (нечіткі множини)	Базуються на експертних оцінках	Невизначеність враховується за допомогою лінгвістичних експертних оцінок і теорії нечітких множин
Комбіновані (використовують критерій ризику, критерій впевненості, багатокритеріальне оцінювання)	Базуються на синергетичному підході (використовуються сильні сторони різних методів)	Невизначеність враховується за допомогою кількісного та якісного математичного апарату

За результатами проведеного дослідження можна зробити такі висновки та рекомендації. Підтверджено, що кібербезпека є головним пріоритетом у

банківській сфері в усьому світі. Виділено організаційний та технологічний аспекти забезпечення кібербезпеки банку. Організаційне забезпечення повинно поєднувати суб'єктів банківського менеджменту, долучених до забезпечення кіберстійкості та безперервності бізнесу. Виявлено недоліки в сучасному стані кібербезпеки банків і запропоновано заходи, реалізація яких дасть змогу підвищити ефективність забезпечення кібербезпеки банку, а відтак і ефективність банківського бізнесу. В організаційному аспекті необхідно покращувати взаємодію суб'єктів забезпечення кібербезпеки в банківській сфері, внутрішній аудит кібербезпеки, політику інформаційної безпеки та відповідність системи забезпечення кібербезпеки банку міжнародним стандартам. Наведена модель організаційної побудови системи управління кіберризиками фінансової установи передбачає три лінії захисту від кіберризиків (на рівні бізнес-підрозділів, підрозділу з управління операційними ризиками та підрозділу внутрішнього аудиту). Запропонована модель механізму забезпечення кіберстійкості фінансового сектору передбачає моніторинг і координацію фінансових установ, засновані на принципах теорії життєздатних систем. У технологічному аспекті основним шляхом підвищення ефективності забезпечення кібербезпеки банку визначено впровадження інноваційних технологій у сфері кіберзахисту. Підтверджено, що не існує єдиного підходу до оцінки ефективності системи кібербезпеки як складної системи з невизначеністю. Якісні методи враховують невизначеність за допомогою лінгвістичних експертних оцінок і теорії нечітких множин. Кількісні методи враховують невизначеність за допомогою засобів статистики, теорії ймовірностей і експертних оцінок із використанням бальних шкал. Оптимальними для врахування невизначеності при оцінюванні ефективності внутрішньобанківської системи кібербезпеки є комбіновані методи, що використовують сильні сторони різних підходів.

Пункт 3.3.1 даного звіту було виконано із використанням матеріалів публікацій виконавців [266, 267, 268, 269].

3.3.2 Формування механізму забезпечення кіберстійкості банків

Банки відіграють надважливу роль у забезпеченні сталого розвитку економіки, адже саме вони є тими фінансовими посередниками, що забезпечують постачання ліквідності на фінансовий ринок та забезпечують кредитування реального сектору економіки.

Зважаючи на це, особливої уваги набуває забезпечення їх кібербезпеки з урахуванням впливу всього комплексу факторів зовнішніх та внутрішніх факторів, у тому числі технологічного та інформаційного характеру.

Однією з нових загроз втрати кібербезпеки банків в умовах переходу на шостий технологічний уклад та пов’язаного з цим застосування технологій Індустрії 4.0, таких як штучний інтелект, «хмарні» та «туманні» обчислення, IoT / IIoT, Big Data, Blockchain, VR / AR, є кіберзагрози, ландшафт який постійно трансформується та оновлюється.

Так, в останньому Звіті про глобальні ризики Всесвітнього економічного форуму кібератаки включені до складу основних ризиків, з якими світ зіткнеться в наступні десять років [270]. У Звіті Accenture State of Cyber Resilience (Accenture) за 2019 рік зазначено, що протягом останніх п’яти років кількість порушень кібербезпеки зросла більш ніж на 65 % [235]. У результаті розвитку цифрової інфраструктури, за оцінками експертів, негативні фінансові наслідки від реалізації кіберзагроз зростуть з 3 трлн доларів США до більше ніж 5 трлн доларів США у 2024 році [271].

На сучасному етапі в умовах переходу на шостий технологічний уклад та пов’язаного з цим застосування в банківській індустрії технологій Індустрії 4.0 (штучний інтелект, «хмарні» та «туманні» обчислення, IoT / IIoT, Big Data, Blockchain, VR / AR тощо) з’являються нові види загроз безпеки, що умовно формують групу кіберзагроз, ландшафт яких постійно трансформується та оновлюється. У банківській індустрії проблема ускладняється наступним:

- банківські установи є елементами критичної інфраструктури;

- мотивація кіберзловмисників зміщується від досягнення прямих фінансових вигід до руйнування критичної інфраструктури, що становить загрозу для національної та міжнародної стабільності фінансових систем та вимагає координації дій в сфері забезпечення кіберстійкості та кібербезпеки з боку як фінансових посередників, так і фінансових регуляторів на національному та наднаціональному рівнях;

- приваблива сфера для реалізації кібератак, зважаючи на можливі обсяги потенційних прямих фінансових вигід у разі їх успішної реалізації. У [272] шляхом проведення актуарних розрахунків визначено, що сукупні збитки від кібератак на 7947 банків у світі складають 97 млрд доларів на рік (9 % чистого прибутку), а вартість ризику (VaR) коливається від 147 до 201 млрд доларів (14 % - 19 % від чистого прибутку). Зазначене призводитиме до зростання кількості кібератак, що будуть відбуватись у фінансовому секторі з постійним збільшенням кількості клієнтів, які зазнаватимуть втрат від реалізації кіберзагроз;

- модуляризація фінансових та банківських послуг, що пов’язує між собою фінансові установи та різноманітні організації (клієнти, контрагенти, постачальники ресурсів та послуг), рівень зрілості яких у здатності протистояти кіберзагрозам сильно відрізняється. Це формує слабкі елементи в механізмі забезпечення кібербезпеки фінансових посередників та ускладнює задачі банківських менеджерів щодо формування ефективного інструментарію протистояння кіберзагрозам та абсорбції їх наслідків в разі реалізації;

- наявна інфраструктура інформаційних та комунікаційних технологій не була розроблена з пріоритетом кібербезпеки, що потребуватиме її адаптації до нових умов діяльності, вимагатиме значних витрат та формуватиме внутрішні вразливості фінансових посередників до кіберризиків;

- значні непрямі наслідки кібератак, що мають різноманітні негативні прояви: репутаційні (наприклад, втрата ключових клієнтів та персоналу, знецінення банківського бренду); соціальні (наприклад, порушення повсякденного життя споживачів банківських послуг через наслідки кібератак,

наприклад втрату коштів з банківського рахунка, негативне сприйняття споживачами банківських послуг цифрових технологій); фізичні (наприклад, пошкодження банківської інфраструктури).

Зважаючи на зазначене вище, банки мають формувати комплекс заходів, інструментів та механізмів для забезпечення кібербезпеки на основі кіберстійкості як здатності протистояти зовнішнім та внутрішнім загрозам, спричинених кіберризиками, адаптуватися до них та / або відновлюватися після них. При цьому це є окремим завданням в забезпеченні безпеки банка в цілому, що має концентруватись на виявленні та протидії кібератакам, мінімізації та швидкому подоланні їх наслідків.

Дослідження кібербезпеки на основі належного забезпечення кіберстійкості банків є відносно новим напрямом у науковій літературі, як вітчизняній, так і закордонній, а системні дослідження в цій сфері практично відсутні. У фінансовій сфері кібератаки належать до складу операційних ризиків, опосередковано призводячи до підвищення інших ризиків насамперед ризику ліквідності та кредитного ризику, тому при дослідженні цієї теми доцільно використовувати науковий доробок у сфері управління операційними ризиками.

Фундаментальні основи забезпечення стійкості та безпеки банків сформовано в працях вітчизняних (О. Барановський, В. Вербенський, О. Дзюблюк та Р. Михайлюк, Ж. Довгань, В. Зінченко, О. Іващук, В. Коваль, В. Коваленко, В. Лавренюк, Д. Хоружий, С. Шумська) та закордонних (Е. Дж. Долан, Р. Дж. Кемпбелл, Р. Л. Міллер, П. С. Роуз, Дж. Ф. Сінкі, Дж. К. Ван Хорн) науковців. Базуючись на отриманих ними результатах, можливо сформувати базові постулати формування механізму забезпечення кібербезпеки банків на основі кіберстійкості.

Ґрунтовне дослідження концепції кіберстійкості фінансових посередників зроблено Б. Дюпоном [241]. Ним обґрунтовується необхідність забезпечення кіберстійкості в фінансовому секторі, систематизуються типи загроз та різноманітні прояви їх негативного впливу на діяльність фінансових посередників. Автором досліджується еволюція концепції «стійкість», що дало

йому змогу визначити поняття «кіберстійкість» та виокремити п’ять основних її параметрів: динамічний, мережевий, практичний, адаптивний та заперечуваний.

На підставі цього автор зробив висновок про те, що базова парадигма «запобігати та захищати» є неадекватною, і що для забезпечення ефективного функціонування фінансових посередників слід орієнтуватись на активне забезпечення кіберстійкості. Також вченим систематизовано інституційні підходи, що використовуються для підвищення кіберстійкості в фінансовому секторі: фінансові посередники здійснюють просування кіберстійкості як майбутнього кібербезпеки; органи стандартизації включають кіберстійкість до стандартів кібербезпеки; регуляторні органи розробляють широкий спектр інструментів відповідності, спрямованих на підвищення кіберстійкості.

Висновки Б. Дюпона щодо неефективності базової парадигми кібербезпеки «запобігати та захищати» підтверджено висновками, наведеними у звіті Accenture за 2019 рік. За результатами опитування виявлено дві окремі групи фінансових посередників, що мають значні відмінності у показниках кібербезпеки: група лідерів з високим рівнем (15 % фінансових посередників) та група наслідувачів (75 % фінансових посередників) з середнім рівнем. Індикатором для виділення групи лідерів у сфері забезпечення кіберстійкості та безпеки є швидкість, з якою останні виявляють та усувають кіберзагрози, перш ніж буде завдано значних фінансових та нефінансових втрат. Ці фінансові посередники виявляють аномалії, ініціюють розслідування та оперативно усувають кіберзагрозу. Решта 75 % фінансових посередників, навпаки, надлишково витрачають кошти на оборону від кіберзагроз та занижують витрати та час на створення можливостей виявлення та реагування на них [235].

Т. Шугунов, А. Жуков, Ф. Хочуєва у [273] визначили основні проблеми забезпечення кібербезпеки банківського сектора Російської Федерації у правовому та методологічному аспектах. Також ними проведеного поглиблений аналіз стану системи забезпечення кіберстійкості кредитно-фінансової системи в умовах становлення та розвитку цифрової економіки.

Важливі висновки щодо необхідності забезпечення кібербезпеки та кіберстійкості індустрії 4.0 зроблені С. Петренком у [274]. Він визначив, що якщо «…забезпечення кібербезпеки …, в основному, орієнтоване на оцінку ймовірності виникнення інцидентів та запобігання можливих загроз безпеки, то забезпечення кіберстійкості … спрямоване на збереження цільової поведінки та працездатності кіберсистем в умовах як відомих (приблизно 45 %), так і невідомих кібератак (решта 55 %).

М. Дубина, І. Середюк, Н. Білоус у [275] акцентують увагу на тому, що «…виникнення кібератак … зумовлюють створення нових кіберризиків для роботи банків. Це … вимагає пошуку нових механізмів, інструментів для їх попередження та протидії», тобто посилювати заходи щодо забезпечення кібербезпеки банку.

За результатами дослідження визначено, що рекомендовані підходи для забезпечення кібербезпеки на основі кіберстійкості значно різняться, але, як правило, більшість наукових наголошують на цілісному системному уявленні про кіберризики [276]. Також науковці акцентують увагу на необхідності розвитку можливостей реагування на кібератаки та відновлення після них, а не виключно на виявленні та підготовці до них для підвищення кіберстійкості [277].

М. Богославський у [278] досліджував ступінь протидії банківським кібератакам на світовому та вітчизняному рівнях, в результаті чого виявив базові постулати забезпечення кібербезпеки на основі кіберстійкості банків: обмін інформацією за поточними кіберзагрозами у реальному часі; постійна фінансова підтримка для забезпечення найліпшого результату боротьби з кіберзагрозами; взаємодія органів банківського нагляду та регулювання інформаційних технологій; протидія кібератакам на глобальному рівні з міжвідомчою кооперацією; розширення спектру дій банків при кібератаках для оперативної допомоги клієнтам.

Зважаючи на початковий етап наукових розробок, присвячених забезпеченню кібербезпеки на основі кіберстійкості банків на сучасному етапі розвитку цифрової економіки, подальшого розвитку потребує комплекс питань

щодо теоретико-методологічного підґрунтя та практичного впровадження механізму забезпечення кібербезпеки на основі кіберстійкості, що дозволяє здійснити формалізацію ландшафту реальних та потенційних кіберзагроз; забезпечує узгодженість механізмів та інструментів для протистояння загрозам, спричинених кібератаками, адаптації та / або відновлення після них; дозволяє не лише адекватно реагувати на наявні кіберзагрози, а й ідентифікувати негативні фактори, що можуть призвести до виникнення та реалізації нових кіберзагроз та кібератак.

При формуванні механізму забезпечення кібербезпеки на основі кіберстійкості банків слід розуміти, що вона є складовою банківської безпеки, під в умовах розвитку інформаційної економіки розуміємо «…стан, що забезпечує: … фінансову стійкість та захищеність від зовнішніх та внутрішніх загроз, у тому числі, пов’язаних із активним розвитком ІТ технологій, підвищення ефективності виконання у штатному режимі базових функцій, пов’язаних з безпосереднім (контактним) або дистанційний (безконтактним) розрахунково-касовим, кредитним, депозитним, валютним обслуговуванням клієнтів юридичних та фізичних осіб завдяки інтенсивному використанню зазначених технологій» [279].

Виходячи з наведеного, кібербезпека є складовою банківської безпеки банку та, поряд з фінансовою стійкістю, визначає стійкий стан банку.

При розгляді питання щодо сутності поняття «кіберстійкість банку» як основи кібербезпеки застосовуються якісний та оцінювальний підходи.

За результатами проведеного дослідження з’ясовано, що у визначенні поняття «кіберстійкість» за якісним підходом спостерігається неоднозначність трактувань, що демонструє таблиця 3.14.

Таблиця 3.14 – Підходи до трактування поняття «кіберстійкість»

№	Джерело	Визначення
1	Європейський центральний банк	здатність продовжувати виконувати свою місію, прогнозуючи кіберзагрози та інші відповідні зміни в операційному середовищі та адаптуючись до них, а також витримуючи, стримуючи кіберінциденти та швидко відновлюючись після них.
2	Комітет з питань платежів та ринкової інфраструктури	здатність прогнозувати, протистояти, стримувати та швидко відновлюватися після кібератак
3	Д. Бодо, Р. Граубарт	здатність підтримувати свої основні функції і цілісність при впливі потенційних атак з загрозою її інформаційної безпеки. Кіберстійка організація – … здатна запобігати, виявляти, стримувати кібератаки та відновлюватися після них, мінімізуючи вразливість до атаки та її вплив на бізнес
		здатність передбачати, витримувати, відновлюватись та пристосовуватися до несприятливих умов, стресів, атак або компромісів щодо кіберресурсів
4	Комісія з цінних паперів та інвестицій Австралії	здатність підготуватися до кібератак, відреагувати на них і відновитися після них. .. це більше, ніж просто запобігання кібератаки або реагування на неї – вона також бере до уваги здатність функціонувати під час такої події, а також адаптуватися та відновлюватися після неї
5	Рада з фінансової стабільності	здатність продовжувати виконувати свою місію, передбачаючи та пристосовуючись до кіберзагроз та інших відповідних змін в операційному середовищі, витримуючи, стримуючи та швидко відновлюючись від кіберінцидентів.
6	Р.Коллінз; К.О'Коннор-Клоуз; А.Чжан	здатність протистояти, стримувати кіберінциденти та швидко відновлюватися після них шляхом прогнозування кіберзагроз та інших змін в операційному середовищі та адаптації до них.
7	Комітет «Кіберстійкості бізнесу»	здатність зберігати працездатність до кібератаки (підготуватися до неї і зробити її максимально дорогою для кіберзлочинців), ефективно реагувати на дії «чорних» хакерів під час кібератаки, а також швидко і з мінімальними втратами відновитися після неї
8	NIST	здатність передбачати, витримати, відновитися і адаптуватися до несприятливих умов, атак або компрометації систем, що використовують або активують різні компоненти незалежно від їх джерела
9	Колосок І. Н., Гуріна Л. А.	здатність стримувати локальний вплив кібератак, ідентифікувати та затримувати потік спотворених даних в межах сфери, чутливої до кібератаки, без подальшої передачі і використання цих даних при управлінні фізичною підсистемою, щоб не привести до виникнення аварійних ситуацій, зокрема великих системних

Джерело: систематизовано автором на основі [280-288]

Результати дослідження щодо визначення сутності поняття «кіберстійкість банку», враховуючи необхідність її розгляду в якісному та оцінювальному розрізах, систематизовано та схематично зображено на рисунку 3.42.

Рисунок 3.42 – Підходи до визначення сутності поняття «кіберстійкість банку»

На основі узагальнення напрацювань щодо визначення сутності поняття «кіберстійкість» пропонуємо визначати кіберстійкість як основу кібербезпеки банку за якісним підходом як здатність безперебійно виконувати покладені на нього функції, протистояти та / або адаптуватись до дії внутрішніх та зовнішніх кіберзагроз за умови максимальної ефективності та мінімальних кіберризиків шляхом прогнозування, ідентифікації, попередження кібератак та відновлення після них.

Відповідно до оцінювального підходу пропонуємо розглядати кіберстійкість у розрізі якісного та кількісного оцінювання.

Якісне оцінювання передбачає визначення відповідності та якості або ступеня застосування принципів, механізмів та інструментів забезпечення кіберстійкості в банку. Вона базується на деталізованих даних щодо типів, рівнів та частоти кібератак, типи атакованих активів та профілів кіберзловмисників. Отримані значення також можуть доповнюватися експертними судженнями.

Кількісне оцінювання кіберстійкості банку здійснюється за допомогою аналізу різних наборів показників, що дають змогу оцінити параметри кіберстійкості: фізичні, інформаційні / технічні, управлінські, організаційні, галузеві, регіональні, національні або транснаціональні.

При цьому в контексті кількісного оцінювання кіберстійкості банку важливим є визначення її видів за рівнями, а саме:

- нормальний рівень кіберстійкості банку, що характеризується цільовим рівнем всіх параметрів кіберстійкості, контрольованим рівнем кіберризиків, безперервністю та стійкістю банківського бізнесу;

- низький рівень кіберстійкості банку, що характеризується стійким погіршенням всіх її параметрів, зростанням рівня кіберризиків, зростанням строків, необхідних для відновлення безперервності банківського бізнесу;

- критичний рівень кіберстійкості банку, що характеризується зниженням параметрів до критично низького рівня, невиконанням державних регуляторних вимог, значними порушеннями в безперебійності банківського бізнесу.

При характеристиці кіберстійкості вважаємо за доцільне базуватись на підході Б. Дюпона [241], який зазначив, що кіберстійкість має:

- динамічний характер: формування механізму забезпечення кіберстійкості вимагає її вивчення через часовий аспект з аналізом заходів, реалізованих до, під час і після кібератаки. Забезпечення кіберстійкості має передбачати постійний циклічний процес підготовки до кібератак, нівелювання їх наслідків та адаптації для запобігання зниженню її рівня до катастрофічного значення;

- мережевий характер: забезпечення кіберстійкості базується на мережі внутрішньоорганізаційних та міжорганізаційних зв’язків, що можуть бути активовані в короткі терміни в надзвичайній ситуації для надання додаткових ресурсів та досвіду;

- постійний характер: забезпечення кіберстійкості має передбачати регулярні репетиції кризових сценаріїв реалізації кіберзагроз. Це дозволить

сформувати інструментарій та навички персоналу, необхідні для роботи в умовах постійного зростання кібератак;

- адаптивний характер: забезпечення кіберстійкості має базуватись на ретельному аналізі реалізованих кібератак, їх причин та наслідків, що дозволить банку підвищувати рівень готовності до кіберзагроз, що можуть виникнути в майбутньому;

- суперечливий характер: мета забезпечення необхідного рівня кіберстійкості може вступати в розбіжність з іншими цільовими показниками діяльності банку, зокрема такими як прибутковість, що вимагає компромісу між ефективністю та адаптованістю до кіберзагроз при формуванні механізму забезпечення кіберстійкості банку.

Механізм забезпечення кібербезпеки банку на основі кіберстійкості є складовою механізму забезпечення банківської безпеки та розглядається як цілісна система взаємопов'язаних елементів, що відбивають відповідні заходи з забезпечення кіберстійкості банків на макро- та мікрорівнях (рис. 3.43).

Особливість кіберстійкості банку в механізмі її забезпечення полягає в тому, що, з одного боку, вона є об'єктом застосування регуляторних та управлінських впливів (керівна підсистема), з іншого – є системним параметром функціонування, без якої банк не матиме змогу продовжувати виконувати свою місію та здійснювати безперервну діяльність. Відповідно до цього, показники кіберстійкості мають включатись до загальної стратегії банку та узгоджуватись з цільовими кількісними та якісними параметрами стратегічних планів в сфері забезпечення кібербезпеки.

Зовнішні рамки механізму забезпечення кібербезпеки банків на основі кіберстійкості формують органи банківського регулювання та нагляду національного та наднаціонального рівнів. Зокрема, ними сформовано широкий спектр інструментів оцінки та відповідності, спрямованих на підвищення рівня кібербезпеки та кіберстійкості.

Банк міжнародних розрахунків, Європейський центральний банк і національні регулятори в Великобританії, США, Нідерландах, Данії, Австралії

та Канаді підвищили свої вимоги до рівня кібербезпеки та кіберстійкості фінансових посередників.

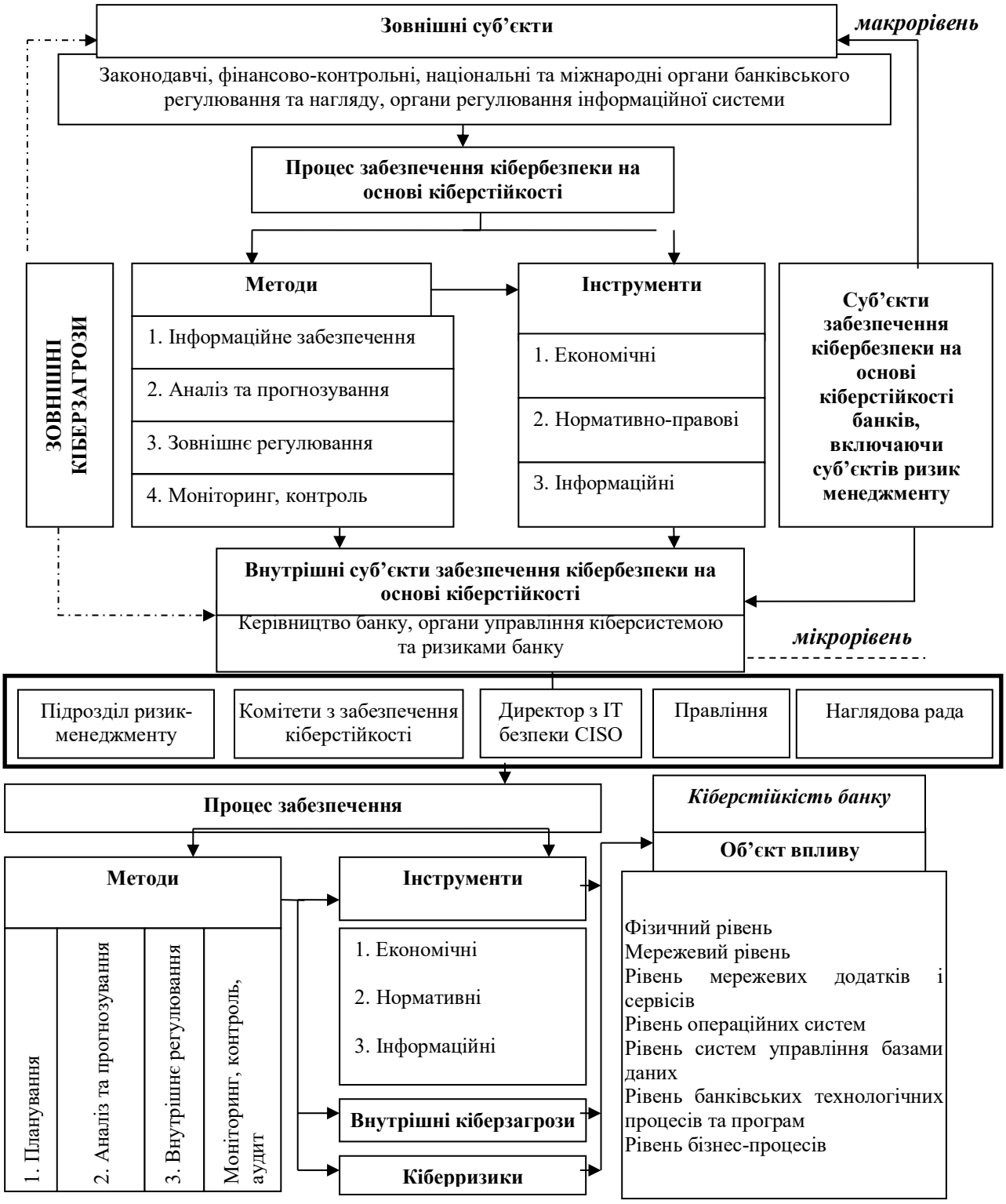


Рисунок 3.43 – Механізм забезпечення кібербезпеки на основі кіберстійкості банку

При цьому в більшості випадків вважається за доцільне застосовувати диференційований підхід з ескалацією регуляторного та наглядового впливу залежно від рівня кіберзагроз, що створюються фінансовим посередником для безпеки фінансової системи в цілому. Базова стратегія регулювання та нагляду в цьому випадку – це делеговане регулювання, що сприятиме співпраці між фінансовими посередниками та саморегулюванню, дозволяючи їм самостійно визначати шляхи досягнення регуляторних цілей у сфері підвищення кіберстійкості. У тому випадку, коли фінансові посередники не бажають або не можуть реалізовувати ефективні стратегії кібербезпеки, суб'єкти регулювання та нагляду здійснюючи посилення рівня інтервенціонізму, переходячи до жорсткіших норм регулювання та контролю, в тому числі штрафних санкцій.

Важливим напрямом при формуванні механізму забезпечення кібербезпеки банків на макрорівні формування регуляторної та рекомендаційної бази та стандартів.

У [290] визначено, що більшість наглядових органів використовують раніше розроблені національні або міжнародні стандарти: рамки кібербезпеки Національного інституту стандартів і технологій США (NIST), серію стандартів ISO 27000 та керівництво CPMI-IOSCO 2016 (Committee on Payments and Market Infrastructures- International Organisation of Securities Commissions) для забезпечення кіберстійкості інфраструктури фінансового ринку.

Групою Світового банку підготовлено збірник нормативних документів, що систематизує наявні нормативні та наглядові практики з кібербезпеки для фінансового сектора [291] та документ про регулювання й нагляд кібербезпеки фінансового сектора [292].

Європейський центральний банк (ЄЦБ) у 2018 році опублікував документ «Очікування щодо нагляду за кіберстійкістю» (CROE) [289], що наразі застосовується практично всіма операторами фінансової інфраструктури в Європі. Світовий банк офіційно прийняв CROE, щоб забезпечити кіберстійкість інфраструктур фінансових ринків та сприяти глобальної гармонізації в рамках Глобальної ініціативи фінансової доступності (FIGI) [292].

Також ЄЦБ розробив стандарт для перевірки стійкості фінансового сектора до кібератак шляхом симуляції їх наслідків на критичні системи в банківській системі Європейського союзу (Threat Intelligence-based Ethical Red Teaming, TIBER-EU). Він передбачає, що за допомогою «етичного злому» так звана «червона команда» допомагає оцінити здатність фінансової установи протистояти кібератаці [293].

Для забезпечення кіберстійкості на макрорівні важливим є формування відповідного інформаційного забезпечення, а саме збору даних щодо кіберінцидентів та їх наслідків, належного обміну інформацією між зацікавленими сторонами з державного та приватного секторів, включаючи фінансовий. У цьому відношенні такі ініціативи, як FS ISAC (Центр обміну інформацією та аналізу фінансових послуг), FSARC (Центр фінансового системного аналізу та стійкості) і SABRIC (Південноафриканський центр інформації про банківські ризики), вже грають важливу роль у полегшенні збору даних та обміну інформацією в різних юрисдикціях по всьому світу.

Але при цьому слід наголосити на тому, що не в усіх країнах та не всіма фінансовими посередниками визнано необхідність обміну інформацією щодо реалізації кіберзагроз, кібератак та їх наслідків. Це зумовлено значною кількістю факторів, одним з яких є відсутність довіри між всіма учасниками обміну інформацією. Зважаючи на це, органам банківського регулювання та нагляду спільно з іншими організаціями, долученими до протидії кіберзагрозам, необхідно реалізувати комплекс заходів, що мотивуватимуть всіх організацій та установ державного та приватного секторів, включаючи фінансовий, здійснювати обмін інформацією щодо кіберзагроз, кіберінцидентів, стратегій та інструментів їх виявлення, попередження та подолання їх негативних наслідків.

За результатами вивчення теоретичних підходів до забезпечення кібербезпеки банків ми розробили модель механізму забезпечення на мікрорівні, адекватну сучасному стану та умовам, в яких працюють банки України, у наочному вигляді представлену на рисунку 3.44.

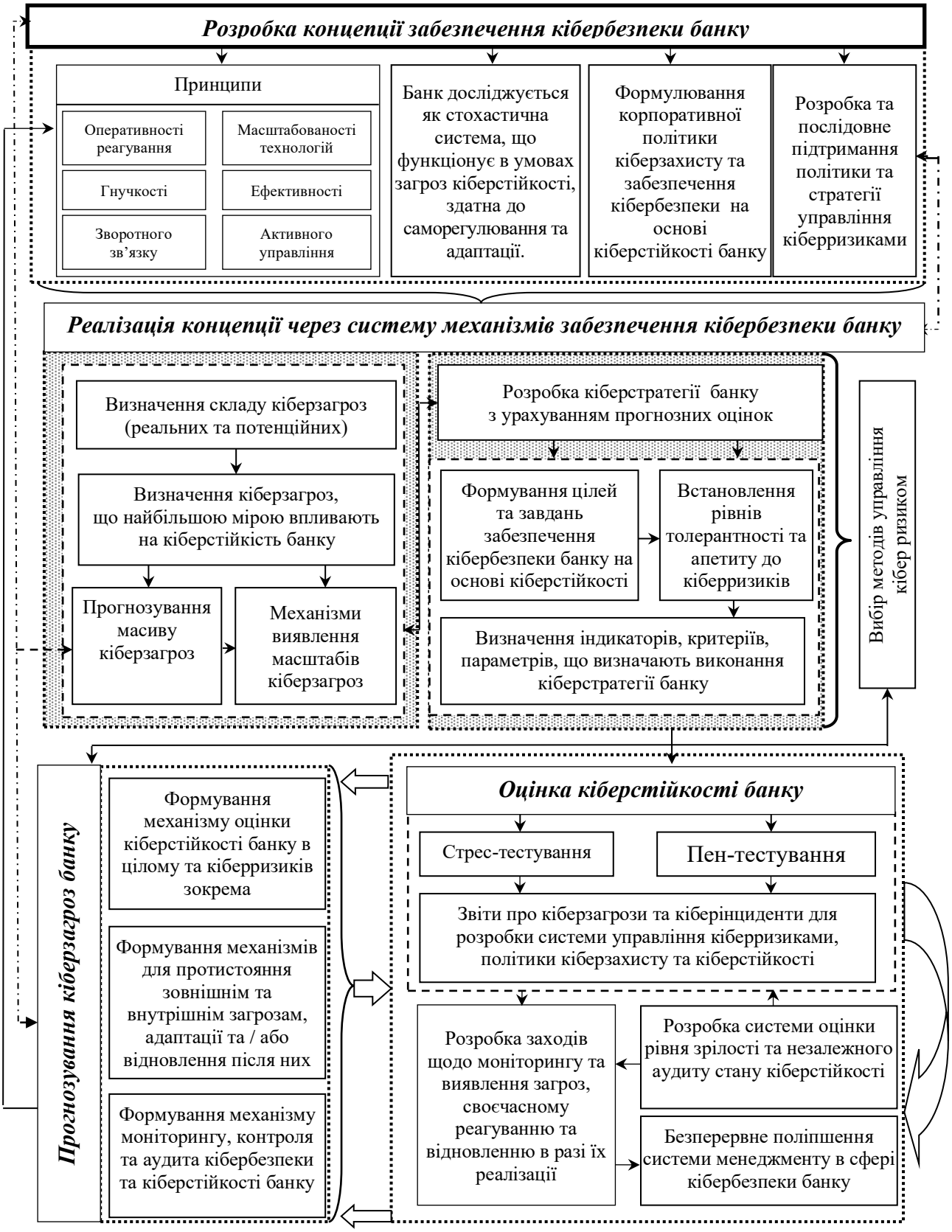


Рисунок 3.44 – Концептуальна модель механізму забезпечення кібербезпеки на основі кіберстійкості банку на мікрорівні

Розроблена концептуальна модель механізму забезпечення кібербезпеки на основі кіберстійкості на мікрорівні забезпечує цілісний підхід до захисту від кібератак. Замість того, щоб зосередитись лише на запобіганні кібератакам, механізм забезпечення кібербезпеки має зосереджуватися на адаптивних та компенсаційних інструментах, що дозволять забезпечити безперервність банківського бізнесу в разі реалізованої кібератаки. Цей механізм у найбільш загальному вигляді включає комплекс заходів, що банки реалізують для запобігання зовнішнім загрозам та виникненню внутрішніх кіберврaзливостей, заходи реагування, що дозволяють пом'якшити наслідки реалізації кіберзагроз, та збільшують можливості відновлення безперебійності після кібератаки.

Розроблений дозволяє: ідентифікувати ландшафт реальних кіберзагроз та прогнозувати потенційні кіберзагрози; забезпечує узгодженість механізмів та інструментів їх попередження, адаптації та / або відновлення від кібератак; дозволяє не тільки адекватно реагувати на наявні кіберзагрози, а й виявляти негативні фактори, що можуть призвести до появи та реалізації нових кіберзагроз та кібератак.

Ми визначили, що важливим для забезпечення кібербезпеки банку є належне організаційне забезпечення. Воно має поєднати всіх суб'єктів банківського менеджменту, долучених до процесів забезпечення кібербезпеки, управління кіберризиками та безперервності банківського бізнесу. При цьому слід наголосити на тому, що кожен банк обирає таку модель організаційної будови, що найкращим чином відповідає особливостям його діяльності, характеру та обсягу банківських послуг, їх цифровізації, рівню розвитку та структурі інформаційних систем, а також наявним можливостям та потребам у сфері забезпечення кібербезпеки банку та кібер-ризик-менеджменту.

За результатами дослідження вважаємо за необхідне створювати в банках спеціалізований комітет забезпечення кібербезпеки як колегіальний орган з ключовими повноваженнями у цій сфері, до складу якого доцільно включити представників підрозділів, які відповідають за безперервність банківського бізнесу, кібербезпеку, управління кіберризиками та якість IT-систем. Це

дозволить домогтися синергетичного ефекту та об’єднати зусилля всіх суб’єктів банківського менеджменту різних бізнес-напрямів, центрів інфраструктури та забезпечення бізнес-процесів шляхом створення єдиної взаємозалежної процесно-орієнтованої моделі, включаючи метрики кіберстійкості та KPI, а також інструменти для моніторингу, контролю та протидії зовнішнім та внутрішнім кіберзагрозам, адаптації та / або відновлення після кібератак.

До функцій цього спеціалізованого підрозділу доцільно віднести:

- інтеграцію процесів безперервності банківського бізнесу, якості IT, управління кіберризиками та кібербезпеки в єдиний механізм;
- нормативне, методологічне та інформаційне забезпечення механізму кібербезпеки та кіберстійкості банку;
- розробка звітних форм та створення бази даних щодо кіберінцидентів, їх фінансових та нефінансових наслідків;
- розробка багатоетапних та багатофакторних сценаріїв реагування на кіберінциденти;
- координація підрозділів банку у сфері реагування на кіберінциденти, прийняття рішення про ескалацію реагування на кіберінциденти на рівень топменеджменту банку;
- формування інструментів прогнозування, ідентифікації, попередження кібератак та відновлення після них;
- розробка планів розвитку механізму забезпечення кібербезпеки, моніторинг та аудит їх виконання.

Також важливим є брати участь в обміні надійною та дієвою інформацією про кіберзагрози та кіберінциденти з ключовими внутрішніми та зовнішніми зацікавленими сторонами (включаючи інші фінансові установи та державні органи банківського регулювання та нагляду) [294]. При цьому суб’єкти забезпечення кібербезпеки банку мають відстежувати актуальні оновлення інформації про кіберзагрози, кібервразливості, кіберінциденти, що відбувались в інших організаціях приватного та державного секторів, та заходи, що вживались для їх попередження та подолання наслідків [294].

Встановлено, що на сучасному етапі розвитку світової економіки в умовах переходу на шостий технологічний уклад та пов'язаного з цим застосування технологій Індустрії 4.0 (штучний інтелект, «хмарні» та «туманні» обчислення, IoT / IIoT, Big Data, Blockchain, VR / AR тощо) з'являються нові види загроз безпеки економічних агентів, що умовно формують групу кіберзагроз, ландшафт яких постійно трансформується та оновлюється.

Обґрунтовано, що у фінансовому секторі проблема забезпечення кібербезпеки ускладняється: переорієнтацією кіберзловмисників на руйнацію критичної інфраструктури країни; можливістю отримання значних фінансових вигід у разі успішної реалізації кібератак; модуляризацією фінансових та банківських послуг, що пов'язує між собою фінансові установи та різноманітні організації (клієнти, контрагенти, постачальники ресурсів та послуг), рівень зрілості яких у здатності протистояти кіберзагрозам відрізняється; необхідністю адаптації інформаційно-комунікаційної інфраструктури до потреб кібербезпеки; значними прямими фінансовими та непрямими репутаційними, соціальними, фізичними втратами фінансових посередників. Зазначені вище тригери формують необхідність забезпечувати кібербезпеку на основі кіберстійкості як комплекс заходів, інструментів та механізмів, що мають забезпечити протистояння зовнішнім та внутрішнім загрозам, спричинених кіберризиками, адаптуватися до них та / або відновлюватися після них.

Встановлено, що забезпечення кібербезпеки є окремим завданням в забезпеченні банківської безпеки, і має концентруватись на виявленні та протидії кібератакам, мінімізації та швидкому подоланні їх наслідків. Визначено, що кіберстійкість як основу кібербезпеки банку доцільно розглядати за якісним та оцінювальним підходами. За якісним підходом кіберстійкість банку – це здатність безперебійно виконувати покладені на нього функції, протистояти та / або адаптуватись до дії внутрішніх та зовнішніх кіберзагроз за умови максимальної ефективності та мінімальних кіберризиків шляхом прогнозування, ідентифікації, попередження кібератак та відновлення після них.

Відповідно до оцінювального підходу кіберстійкість запропоновано розглядати в розрізі якісного (визначення відповідності та якості або ступеня застосування принципів, механізмів та інструментів забезпечення кіберстійкості в банку) та кількісного (формування наборів показників, що дають змогу оцінити параметри кіберстійкості: фізичні, інформаційні / технічні, управлінські, організаційні, галузеві, регіональні, національні або транснаціональні) оцінювань. При цьому в контексті кількісного оцінювання кіберстійкості банку важливим є визначення її видів за рівнями (нормальний, низький, критичний).

Розроблена концептуальна модель механізму забезпечення кібербезпеки банку на мікрорівні забезпечує цілісний підхід до захисту від кібератак. Замість того, щоб зосередитись лише на запобіганні кібератакам, розроблений механізм зосереджується на адаптивних та компенсаційних інструментах, що дозволять забезпечити безперервність банківського бізнесу в разі реалізованої кібератаки.

Розроблений механізм забезпечення кібербезпеки на основі кіберстійкості дозволяє: ідентифікувати ландшафт реальних кіберзагроз та прогнозувати потенційні кіберзагрози; забезпечує узгодженість механізмів та інструментів їх попередження, адаптації та / або відновлення від кібератак; дозволяє не тільки адекватно реагувати на наявні кіберзагрози, а й виявляти негативні фактори, що можуть призвести до появи та реалізації нових кіберзагроз та кібератак.

Встановлено, що важливим для забезпечення кібербезпеки банку є належне організаційне забезпечення, зокрема створення спеціалізованого комітету забезпечення кібербезпеки як ключового колегіального органу в цій сфері. Це дозволить домогтися синергетичного ефекту та об’єднати зусилля всіх суб’єктів банківського менеджменту різних бізнес-напрямів, центрів інфраструктури та забезпечення бізнес-процесів шляхом створення єдиної взаємозалежної процесно-орієнтованої моделі, включаючи метрики кіберстійкості та KPI, а також інструменти для моніторингу, контролю та протидії зовнішнім та внутрішнім кіберзагрозам, адаптації та / або відновлення після кібератак.

Пункт 3.3.2 даного звіту було виконано із використанням матеріалів публікацій виконавців [186, 247, 295].

3.4 Розробка концепції реформування фінансового кіберпростору

3.4.1 Моделювання інтегрального індексу загрози як одного із векторів стратегії забезпечення стійкості фінансового кіберпростору

В останні 35-40 років на макроекономічному рівні спостерігається активне вивчення та розвиток питань економічної небезпеки, що супроводжується безперервними змінами сутності, понять та методик забезпечення відповідних показників безпеки економіки. Основні матеріали цих досліджень в більшій частині ґрунтуються на розрахунку загального рівня економічної безпеки країн та відповідного ранжування держав згідно визначеного рівня. Паралельно з цим формуються основні відмінності таких досліджень, що полягають у різних наборах факторів та чинників, що впливають на рівень безпеки кожної країни, визначення сили впливу та розміру вагомості таких факторів загрози національним економікам держав. Відомі сучасні методики визначення рівня загрози економіки країн світу, наразі враховують основні тенденції функціонування та розвитку світової економічної системи, сучасних інформаційних технологій, останні досягнення в напряму економічної теорії. У сучасних умовах розвитку кожна окремо взята держава піддається впливу всіх цих процесів, що визначають тенденції сьогодення, визначаючи, диверсифікуючи та ускладнюючи проблеми економічної небезпеки. Так, аналіз існуючих методик оцінки загрози національної економіки вказує на відсутність в економічній літературі досконалого дієвого та якісного підходу до визначення загроз економіці країни, що викликає гостру необхідність розробки ефективної методології забезпечення національної економічної безпеки країни.

Для вивчення категорії індексу загрози національної економіки проведено аналіз наявної літератури шляхом побудови карти наукової бібліографії терміну «threatindex» (індекс загрози) [296, 297, 298, 299,300] за період 2016 - 2020 рр. у частині таких галузей як економіка, економетрика, фінанси та бізнес, управління та бухгалтерський облік за допомогою програми VOSViewerv.1.6.10. Відповідні результати аналізу зображено у вигляді графіку (рисунок 3.45). Формування карти наукової бібліографії зазначеного поняття базується на даних трактатів [301, 302, 303], знайдених, відібраних та побудованих у архіві зібрань Scopus.

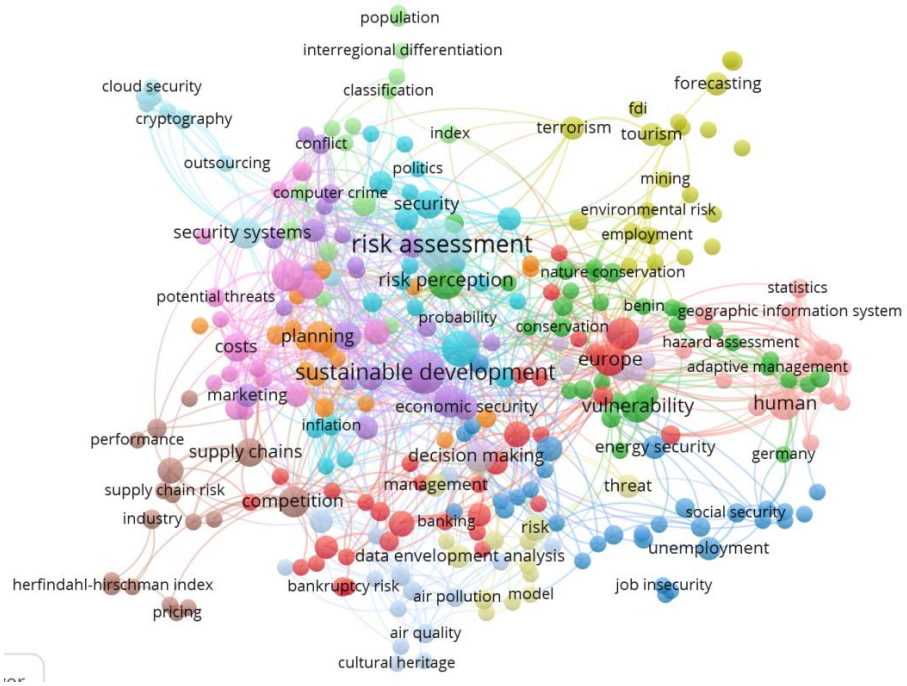


Рисунок 3.45 – Карта наукового бібліографічного поняття «threatindex»

Аналіз рисунку 3.45 надає можливість здійснити висновки про те, що дослідження теми визначення індексу загрози національної економіки, наразі доволі актуальне та затребуване, а доказом цього є велика чисельність робіт вчених за напрямком цієї сфери [304, 305, 306, 307]. На карті зображено кластери видань, сформованих по ключовими словам, що також групуються з даними. Таким чином було виділено 14 певних кластерів, включаючи ключові слова, що різняться між собою відмінними кольорами. Особливо великими є кластери, що

мають зв’язок з такими поняттями як оцінювання ризику, стабільний розвиток, економічна безпека, прийняття рішень, системи безпеки, банкрутство, інфляція, безробіття тощо [308, 309, 310, 311, 312].

З метою здійснення оцінки індексу загрози національної економіки пропонується побудувати структурно-логічну математичну модель, що включає відповідну послідовність певних етапів дослідження.

Етап 1. Створення інформаційної бази вхідних предикторів за період з 2008 по 2019 рр. у динаміці, а саме: Дефіцит державного бюджету, % до ВВП; Обсяг загального боргу, % до ВВП; Частки іноземного капіталу у статутному капіталі банків; Міжнародні резерви країни в місяцях імпорту; Рівень доларизації, частка іноземної валюти у грошовій масі, %; Контроль корупції; Політична стабільність та відсутність насильства / тероризму; Верховенство права; Рівень інфляції, %; Рівень безробіття,%; Індекс GINI; Рівень тіньової економіки, % ВВП; таблиця 3.15, Ж.1)

Таблиця 3.15 – Макет таблиці відображення динаміки показників оцінювання індексу загрози національної економіки

Індикатор	Порогове значення	Рік				
		1	…	t	…	T
Дефіцит державного бюджету, % до ВВП	не більше 3-4					
Обсяг загального боргу, % до ВВП	не більше 60					
Частки іноземного капіталу у статутному капіталі банків	не більше 30					
Міжнародні резерви країни в місяцях імпорту	не меньше 3					
Рівень доларизації, частка іноземної валюти у грошовій масі, %	не більше 10					
Контроль корупції						
Політична стабільність та відсутність насильства / тероризму						
Верховенство права						
Рівень інфляції, %	не більше 7					
Рівень безробіття,%	не більше 7,6					
Індекс GINI						
Рівень тіньової економіки, % ВВП						

2 етап. Приведення показників вхідної інформаційної бази дослідження до співставного вигляду шляхом проведення нелінійної нормалізації за наступною формулою 3.22:

$$I_{ij} = \left(1 + e^{\frac{\overline{x_j} - x_{ij}}{\sigma(x_j)}}\right)^{-1} \quad (3.22)$$

де I_{ij}– нормалізоване значення j-го показника характеристики загрози національної економіки за і-ий рік;

$\overline{x_j}$– середнє значення j-го показника характеристики загрози національної економіки за досліджуваний часовий діапазон;

x_{ij} – фактичне значення j-го показника характеристики загрози національної економіки за і-ий рік;

$\sigma(x_j)$ – середнє квадратичне відхилення j-го показника характеристики загрози національної економіки за досліджуваний часовий діапазон.

Розрахунки нормалізованих значень показників вхідної інформаційної бази дослідження на основі застосування формули (3.22) представимо в таблиці 3.16.

3 етап. Відбір релевантних показників оцінювання індексу загрози національної економіки на базі комбінації методів Парето та діаграми розсіювання. Переходячи до реалізації даного етапу побудови структурно-логічної математичної моделі оцінювання індексу загрози національної економіки, розглянемо теоретичні аспекти застосування зазначених методів до фільтрації релевантних предикторів вхідної інформаційної бази дослідження. Так, діаграма Парето використовується для відображення відносної важливості всіх можливих проблемних аспектів з метою знаходження початкової точки для подальшого спостереження за результатами, пошуку головної причини проблеми, результативного розв’язання питання.

Таблиця 3.16 –Нормалізовані значення показників характеристики індексу загрози національної економіки

Показник	Рік					
	2008	2009	2010	2011	2012	2013
Дефіцит державного бюджету, % до ВВП	0,28	0,66	0,88	0,32	0,62	0,72
Обсяг загального боргу, % до ВВП	0,16	0,28	0,35	0,31	0,31	0,35
Частки іноземного капіталу у статутному капіталі банків	0,48	0,45	0,62	0,67	0,58	0,38
Міжнародні резерви країни в місяцях імпорту	0,91	0,64	0,74	0,50	0,37	0,29
Рівень доларизації, частка іноземної валюти у грошовій масі, %	0,50	0,64	0,30	0,44	0,69	0,11
Контроль корупції	0,74	0,33	0,35	0,31	0,26	0,18
Політична стабільність та відсутність насильства / тероризму	0,63	0,57	0,63	0,61	0,61	0,48
Верховенство права	0,86	0,53	0,28	0,24	0,40	0,30
Рівень інфляції, %	0,71	0,54	0,41	0,39	0,26	0,25
Рівень безробіття,%	0,11	0,60	0,42	0,36	0,29	0,22
Індекс GINI	0,84	0,51	0,35	0,30	0,33	0,30
Рівень тіньової економіки, % ВВП	0,41	0,71	0,66	0,41	0,41	0,54

Продовження таблиці 3.16

Показник	Рік					
	2014	2015	2016	2017	2018	2019
Дефіцит державного бюджету, % до ВВП	0,75	0,29	0,40	0,27	0,34	0,35
Обсяг загального боргу, % до ВВП	0,69	0,78	0,79	0,71	0,59	0,67
Частки іноземного капіталу у статутному капіталі банків	0,33	0,71	0,89	0,45	0,20	0,19
Міжнародні резерви країни в місяцях імпорту	0,15	0,42	0,52	0,50	0,46	0,42
Рівень доларизації, частка іноземної валюти у грошовій масі, %	0,70	0,70	0,78	0,66	0,30	0,28
Контроль корупції	0,42	0,45	0,78	0,82	0,67	0,67
Політична стабільність та відсутність насильства / тероризму	0,27	0,28	0,29	0,29	0,30	0,92
Верховенство права	0,36	0,26	0,49	0,76	0,73	0,72
Рівень інфляції, %	0,46	0,94	0,50	0,51	0,44	0,39
Рівень безробіття,%	0,70	0,67	0,72	0,75	0,59	0,66
Індекс GINI	0,17	0,57	0,41	0,72	0,74	0,73
Рівень тіньової економіки, % ВВП	0,87	0,76	0,48	0,30	0,21	0,19

Досить цікавими є історичне становлення та застосування діаграми Парето. Так, італійським вченим Парето В. у 1897 р. сформульовано закон розподілення доходів, що передбачає нерівномірний розподіл усіх наявних благ. Американським науковцем Лоренцом М. зображено таку теорію у вигляді діаграми. Економіст Джуран Д. вивчав особливості якості, та використав діаграму з метою класифікації певних проблем якості, а саме: небагаточисленні, але є суттєво важливими, та багаточисленні, але не суттєво важливі. Він назвав свій метод аналіз Паретто.

Отже, передбачається, що зосередження уваги на найбільш важливих проблемах сильніше впливає на отримання бажаних результатів. Відомим є правило з назвою 20/80, що означає: зосередження 20% зусиль на найважливіших питаннях призводить до можливості отримати 80% результатів. А решта 80% зусиль дозволяють отримати тільки решту 20% від усіх результатів.

Слід зазначити, що діаграма Парето виступає особливим типом вертикального стовпчикового графіка, що дозволяє знайти порядок вирішення виникаючих проблем. В цьому випадку є можливість досягти значно більших результатів, опрацьовуючи найвищий стовпчик, а не розподіляючи увагу ще й на менші стовпчики .

Побудова діаграми Парето передбачає використання наступної методики: спочатку здійснити відбір проблемних питань, що необхідно між собою порівняти та розмістити за ступенями важливості; визначити певний єдиний стандартний масштаб для можливості здійснити порівняння одиниць виміру; визначити період часу для дослідження; зібрати всі необхідні дані; визначити та порівняти частоти появи відповідних категорій; перерахувати категорії проблем на горизонтальній осі графіка зліва направо в порядку спадання ознаки критерію; відмітити на вертикальній осі графіку зазначеного масштабу від 0% до 100%, за якого 100% включає загальна сумарна частота виникнення всіх можливих категорій проблем.

Таким чином, переходячи до побудови діаграми Парето з метою вибору релевантних предикторів оцінювання індексу загрози національної економіки

проведемо ряд проміжних кроків, а саме: 1) діапазон можливих нормалізованих значень вхідних предикторів розіб'ємо на 10 рівномірних інтервалів (від 0 до 0,1; від 0,1 до 0,2; від 0,2 до 0,3; від 0,3 до 0,4; від 0,4 до 0,5; від 0,5 до 0,6; від 0,6 до 0,7; від 0,7 до 0,8; від 0,8 до 0,9; від 0,9 до 1,0); 2) обчислимо кількість випадків протягом досліджуваного часового діапазону попадання нормалізованих значень предикторів характеристики рівня загрози національної економіки визначеним інтервальним межам (таблиця 3.15); 3) обчислимо частоти використання предикторів (графа «Сума всього» таблиці 3.17); 4) визначимо частоти попадання нормалізованих значень предикторів у кожен з визначених на першому кроці інтервалів, результати представимо у рядку «Сума» таблиці 3.17. На основі аналізу розрахованих на даному кроці частот визначимо 20% інтервалів, якими можна знехтувати при визначенні пріоритетності вхідних предикторів – тобто інтервали від 0 до 0,1 та від 0,1 до 0,2, оскільки саме не них припадає найменша кількість частот; 5) обчислимо 80% значущих частот використання предикторів (графа «Сума 80%» таблиці 3.17). Так, на основі результатів проведення даного кроку визначимо, що найменші значення частот за сумою 80%, тобто значення в розмірі 30 одиниць, мають 2 предиктори: Рівень доларизації, частка іноземної валюти у грошовій масі, % та Рівень тіньової економіки, % ВВП. Саме ці два предиктори пропонується вилучити з подальших розрахунків індексу загрози національної економіки.

На основі даних таблиці 3.17 (графи «Сума всього» та «Сума 80%») побудуємо діаграму Парето (рисунок 3.46), яка візуально дозволяє визначити 80% релевантних і 20% нерелевантних предикторів вхідної бази дослідження. Для побудови даної діаграми обчислимо відносний показник структури в розрізі зазначених граф таблиці 3.17. Діаграма Парето виступає підтвердженням доцільності вилучення таких пре дикторів, як Рівень доларизації, частка іноземної валюти у грошовій масі, % та Рівень тіньової економіки, % ВВП.

Таблиця 3.17 – Частота попадання нормалізованих значень показників предикторів характеристики рівня загрози національної економіки інтервальним межам від 0 до 1

Показник\Інтервал можливих значень	0,1	0,2	0,3	0,4	0,5	0,6	0,7	0,8	0,9	1	Сума всього	Сума 80%
Дефіцит державного бюджету, % до ВВП	0	0	3	2	4	2	6	4	7	4	32	32
Обсяг загального боргу, % до ВВП	0	1	1	5	1	6	2	9	2	9	36	35
Частки іноземного капіталу у статутному капіталі банків	0	0	1	2	4	3	6	4	7	4	31	31
Міжнародні резерви країни в місяцях імпорту	0	1	1	2	5	3	6	4	6	5	33	32
Рівень доларизації, частка іноземної валюти у грошовій масі, %	0	1	2	1	3	2	8	3	8	3	31	30
Контроль корупції	0	1	1	4	3	4	4	6	5	6	34	33
Політична стабільність та відсутність насильства / тероризму	0	0	5	0	6	1	10	1	10	1	34	34
Верховенство права	0	0	4	1	6	2	6	4	7	4	34	34
Рівень інфляції, %	0	0	2	1	5	4	5	5	5	6	33	33
Рівень безробіття,%	0	1	2	2	3	3	5	6	5	6	33	32
Індекс GINI	0	1	2	3	3	5	3	7	4	7	35	34
Рівень тіньової економіки, % ВВП	0	0	1	1	5	2	6	4	7	4	30	30
Сума	0	6	25	24	48	37	67	57	73	59		

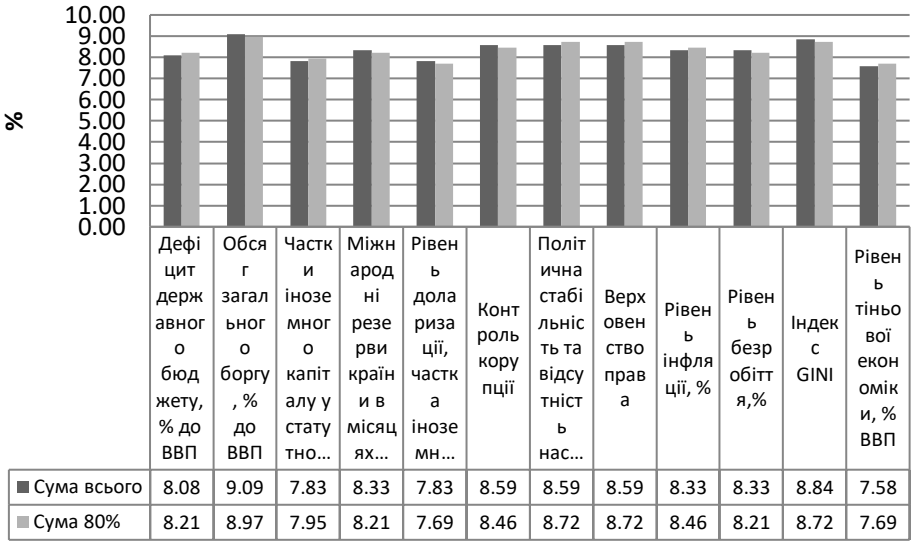


Рисунок 3.46 – Діаграма Парето вибору релевантних предикторів оцінювання індексу загрози національної економіки

В розрізі дослідження окресленої проблематики визначення релевантності предикторів окрема увага віддається діаграмі розсіювання (розкиду)., яка використовується для зображення тих процесів, що відбуваються з однією з аналізованих змінних категорій, у випадку за якого інша змінна категорія також змінюється; проведення перевірки припущення щодо взаємозв'язку двох аналізованих змінних категорій, оцінювання величини сили такого взаємозв'язку. При цьому діаграма розкиду не дозволяє встановити причинно-наслідковий взаємозв'язок. Аналіз побудованої діаграми (рисунок 3.47) дозволяє підтвердити висновок про доцільність акцентування уваги при виборі релевантних предикторів саме інтервалів нормалізованих значень від 0,2 до 1.

4 етап. Оцінювання інтегрального індексу загрози національної економіки за допомогою функції Кернела, яка являє собою новий метод- концепція регресії Кернела [313, 314]. Така концепція дозволяє ефективно моделювати періодичні явища та процеси, враховуючи та долаючи при цьому обмеження певних методів. Функція Кернела застосовується при вимірюванні подібності між парами певних показників. При цьому метою такого дослідження є моделювання періодичних процесів та явищ у визначених часових рядах.

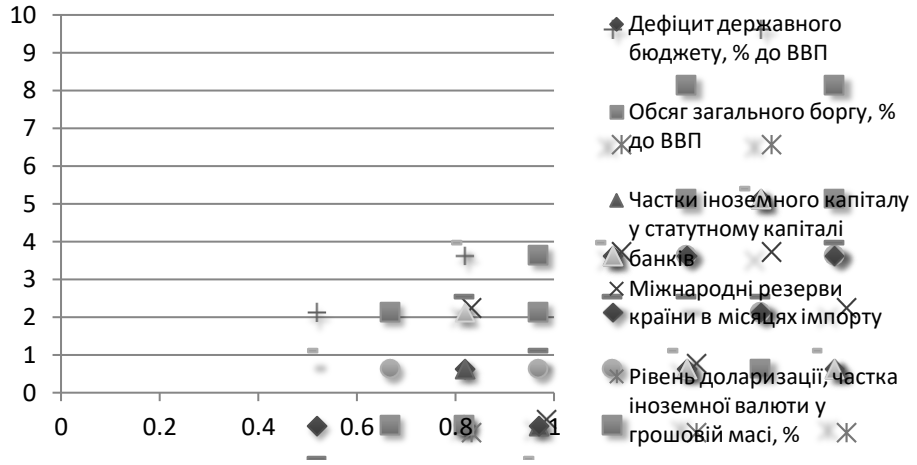


Рисунок 3.47 – Діаграма розсіювання вибору релевантних предикторів оцінювання індексу загрози національної економіки

Функцію Кернела [315] можна представити у вигляді формули 3.23:

$$k(t_i, t_j) = exp\left[-\frac{2}{l^2} sin\left(\pi \frac{t_i - t_j}{\rho}\right)^2\right] \tag{3.23}$$

де t – показник часу;

$k(t_i, t_j) \in (0, 1)$ – вихідний результат функції Кернела. Він вимірює відповідну схожість двох часових показників t_i і t_j, у вигляді функції відстані, що є між ними, а також функції двох певних параметрів;

$\theta = \{p, \ell\}$ - період і довжина функції Кернела.

Переходячи до застосування функції Кернела в розрізі оцінювання складових індексу загрози національної економіки за предикторами, представимо пару показників - з одного боку, нормалізованого значення j-го показника характеристики загрози національної економіки за і-ий рік та, з іншого боку, середнього нормалізованого значення $\overline{I_J}$ даного показника:

$$k\left(I_{ij},\overline{I_J}\right) = exp\left[-\frac{2}{l^2}sin\left(\pi\frac{I_{ij}-\overline{I_J}}{\rho}\right)^2\right] \qquad (3.24)$$

$$\overline{I_J} = \frac{\sum_{i=1}^{m} I_{ij}}{m}$$

де $k\left(I_{ij},\overline{I_J}\right)$ – функція Кернела залежності від нормалізованого значення j-го показника характеристики загрози національної економіки за і-ий рік та середнього нормалізованого значення $\overline{I_J}$;

$\overline{I_J}$ – середнє арифметичне значення j-го нормалізованого показника характеристики загрози національної економіки за проміжок часу;

m – кількість показників характеристики загрози національної економіки;

l,ρ – параметри функції Кернела.

Обчисливши значення функції Кернела в розрізі кожного відібраного на попередньому етапі предиктора індексу загрози національної економіки за кожен рік досліджуваного часового діапазону, виникає необхідність їх згортки до єдиного узагальнюючого індикатора за допомогою мультиплікативної форми згортки на основі методики середнього геометричного. В той же час, індекс загрози інтерпретується як індекс-дестимулятор національної економіки, саме тому для відображення даного негативного аспекту характеристики розрахункового індексу, виникає необхідність розгляду її величини як одиниці мінус середнє геометричне функцій Кендела кожного релевантного предиктора:

$$D_i = 1 - \sqrt[n-1]{\prod_{j=1}^{n} k(I_{ij},\overline{I_{iJ}})} \qquad (3.25)$$

де D_i – інтегральний індекс загрози національної економіки за і-тий рік;

n – кількість років досліджуваного часового діапазону;

m – кількість показників характеристики загрози національної економіки;

Формула (3.25) з урахуванням умовних позначень набуває вигляду 3.26:

$$D_i = 1 - \sqrt[n-1]{\prod_{j=1}^{n} k\left(I_{ij}, \overline{I_{ij}}\right)} = 1 - \sqrt[n-1]{\prod_{j=1}^{n} exp\left[-\frac{2}{l^2} sin\left(\pi \frac{I_{ij} - \overline{I_J}}{\rho}\right)^2\right]} \qquad (3.26)$$

Обираючи в якості параметрів функції Кернела $l = 0{,}2, \rho = 5$, результати розрахунків за формулою (5) та усі проведені проміжні обчислення систематизуємо в таблиці 3.18.

Таблиця 3.18 – Динаміка проміжних розрахунків та інтегрального індексу загрози національної економіки з 2008 по 2019 рр.

Показник	порогове значення	Рік					
		2008	2009	2010	2011	2012	2013
Дефіцит державного бюджету, % до ВВП	не більше 3-4	0,40	0,56	0,05	0,58	0,74	0,36
Обсяг загального боргу, % до ВВП	не більше 60	0,11	0,39	0,64	0,49	0,51	0,63
Частки іноземного капіталу у статутному капіталі банків	не більше 30	0,99	0,95	0,72	0,56	0,86	0,77
Міжнародні резерви країни в місяцях імпорту	не меньше 3	0,04	0,64	0,31	1,00	0,74	0,44
Контроль корупції		0,32	0,57	0,66	0,49	0,33	0,14
Політична стабільність та відсутність насильства / тероризму		0,68	0,88	0,70	0,75	0,76	1,00
Верховенство права		0,08	0,97	0,42	0,27	0,85	0,47
Рівень інфляції, %	не більше 7	0,38	0,94	0,91	0,83	0,38	0,35
Рівень безробіття,%	не більше 7,6	0,05	0,84	0,86	0,66	0,40	0,20
Індекс GINI		0,10	1,00	0,67	0,46	0,56	0,46
Integralindex		0,81	0,26	0,51	0,42	0,42	0,58

Продовження таблиці 3.18

Показник	порогове значення	Рік					
		2014	2015	2016	2017	2018	2019
Дефіцит державного бюджету, % до ВВП	не більше 3-4	0,28	0,46	0,86	0,40	0,65	0,68
Обсяг загального боргу, % до ВВП	не більше 60	0,50	0,22	0,19	0,42	0,84	0,57
Частки іноземного капіталу у статутному капіталі банків	не більше 30	0,58	0,39	0,05	0,95	0,19	0,16
Міжнародні резерви країни в місяцях імпорту	не меньше 3	0,10	0,91	0,99	1,00	0,98	0,91
Контроль корупції		0,89	0,96	0,22	0,13	0,54	0,57
Політична стабільність та відсутність насильства / тероризму		0,39	0,42	0,47	0,47	0,49	0,03
Верховенство права		0,71	0,34	1,00	0,25	0,33	0,37
Рівень інфляції, %	не більше 7	0,99	0,02	0,99	0,99	0,97	0,83
Рівень безробіття,%	не більше 7,6	0,49	0,59	0,43	0,32	0,87	0,65
Індекс GINI		0,12	0,90	0,87	0,39	0,31	0,35
Integralindex		0,60	0,63	0,56	0,55	0,46	0,62

Розрахувавши значення інтегрального показника за формулою (8) як індикатора загрози національної економіки в динаміці з 2008 по 2019 рр., виникає необхідність візуалізації як загальної тенденції поведінки даного індексу в часі, так і варіації в межах від мінімально та максимально можливих рівнів. Для цього побудуємо рисунок 3.48.

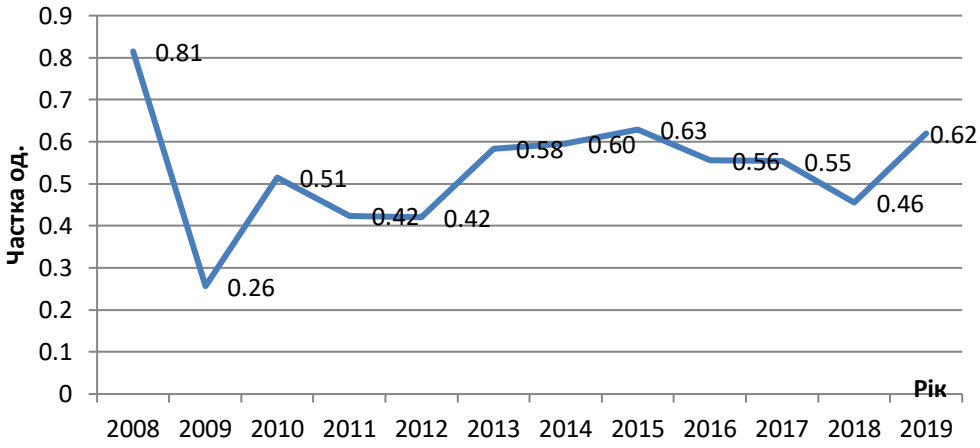


Рисунок 3.48 – Динаміка індексу загрози національної економіки з 2008 по 2019 рр.

Аналіз рисунку 3.48 дозволяє стверджувати, що загальна тенденція індексу загрози національної економіки характеризується як зростаюча.

Усі країни в більшому чи меншому ступені прагнуть забезпечити довготривалі вигідні стратегічні переваги в напрямку економічних стабільності. А процеси, що відбуваються в глобальному світовому співтоваристві, гостро впливають на становлення та розвиток світового господарства, політичні та економічні відносини у суспільстві. Все це спричиняє формування нових загроз і ризиків для розвитку національної економіки та забезпечення безпечного функціонування держави. Забезпечення економічної безпеки передбачає , передусім, створення оптимального, ефективного механізму та методології формування національної економічної безпеки країни на основі побудови структурно-логічної математичної моделі, що включає відповідну послідовність певних етапів дослідження факторів та показників загроз національної економіки.

Так , формування, розрахунок , оцінка та аналіз узагальненого показника індексу загрози національної економіки, дозволить допомогти у вирішенні основних поставлених цілей ефективного, стабільного, а головне безпечного функціонування національної економіки, таких як: стабільне зростання обсягів національного виробництва; стабілізація рівня цін; забезпечення стабільно о

високого рівня зайнятості населення; підтримка рівноваги у зовнішньоторговельному балансі. Запропонована методологія дозволить своєчасно та оперативно забезпечувати підтримку необхідних організаційних, інституційних, нормативно-правових умов, що передбачають спроможність системи національної економіки до протистояння зовнішніх та внутрішніх загроз та навантажень, подальшої якісної адаптації до проблем та дестабілізуючих факторів, і як результат швидкому відновленню після впливу негативних чинників.

Пункт 3.4.1 даного звіту було виконано із використанням матеріалів публікацій виконавців [186, 316, 317, 318, 319].

3.4.2 Ігромоделювання стратегій державного регулювання економічної безпеки національної економіки з метою формування внутрішньобанківських інструкцій щодо організації системи кіберзахисту

В сучасних умовах організації світових макроекономічних процесів, з урахуванням виникаючих фінансових криз, під час розроблення та впровадження середньо та довгострокової стратегії економічного, фінансового, соціального розвитку країн, важливе місце посідає їх економічна безпека [320, 321, 322]. Так, саме економічна безпека виступає однією з найважливіших ознак якісного функціонування фінансово-економічних систем у кожній країні по всьому світу. Також рівень економічної безпеки характеризує здатність держави забезпечувати необхідні, достойні умови життєдіяльності суспільства; сталу достатність потрібних для розвитку національного господарства ресурсів; врегульоване, послідовне виконання національних державних інтересів. Однією з основних проблем економічної безпеки при цьому виділяють удосконалення існуючих не достатньо ефективних та результативних механізмів

функціонування, регулювання фінансово-економічної діяльності на державному рівні [323, 324, 325, 326, 327, 328].

Тому, на сьогоднішній день, в умовах зростаючої глобалізації світового господарства, формування ефективної, дієвої системи державного регулювання економічної безпеки національної економіки, як складової частини державної національної безпеки, є особливо актуальним напрямом, що потребує пріоритетної уваги. Отже, питання та проблемні аспекти, що виникають при державному регулюванні економічної безпеки національної економіки, ще не достатньо вивчені та розроблені, і тому потребують пошуку нових підходів та методик до забезпечення належного рівня економічної безпеки держави.

Так постає потреба у здійсненні формалізації системи заходів Державного регулювання економічної безпеки національної економіки, щодо знаходження компромісної точки у тріаді таких напрямів: зведення до мінімуму величини інтегрального індексу загрози національної економіки, мінімізації рівня використання банків з метою легалізації кримінальних доходів за рахунок максимізації рівня ефективності внутрішньобанківської системи фінансового моніторингу в розрізі певного банку та одночасної мінімізації узагальнюючої оцінки ризику використання банків для легалізації кримінальних доходів. Здійснювати таку формалізацію запропоновано шляхом такого інструментарію, як «теорія ігор». Тому, сформульовано постановку задачі для апарату «теорія ігор» для проведення Державного регулювання економічної безпеки національної економіки. На цьому етапі методики першим кроком постає ідентифікація існуючої конфліктної ситуації. Перший гравець (держава) переслідує мету мінімізації інтегрального індексу загрози національної економіки шляхом державного регулювання, що в свою чергу суперечить існуючій стратегії функціонування другої групи учасників (економічних агентів, які намагаються легалізувати кримінальні доходи), які відповідно свідомо чи не свідомо призводять до фактів порушень, і в кінцевому підсумку спричиняють збільшення рівня використання банків з метою легалізації кримінальних доходів. Також, потрібно відмітити, що відповідний взаємозв’язок інтегрального індексу

загрози національної економіки та рівня використання банків з метою легалізації кримінальних доходів пропонується формалізувати за рахунок узагальнюючої оцінки ризику використання банків для легалізації кримінальних доходів, що у дослідження представлений у якості результативного показника та яку держава намагається мінімізувати.

Далі другим кроком постановки задачі дослідження виступає створення платіжної матриці, що показує результати функціонування учасників у кількісному вираженні. Показниками такої матриці (SVA^*_{ji}) є певні математичні сподівання узагальнюючої оцінки ризику використанням банків для легалізації кримінальних доходів, що в свою чергу подібна до стратегії країни, та описується досягнутим розміром інтегрального індексу загрози національної економіки, як регресант впровадження стратегії економічних агентів, які намагаються легалізувати кримінальні доходи, формалізованої у вигляді рівня використання банків з метою легалізації кримінальних доходів (таблиця 3.19).

Таблиця 3.19 – Платіжна матриця гри «державного регулювання економічної безпеки національної економіки»

Рівень використання банківської системи з метою легалізації кримінальних доходів/ Інтегральний індекс загрози		Рік 1	…	Рік і	…	Рік n
		D_1	…	D_i	…	D_n
Банк 1	θ_1	SVA^*_{11}	…	SVA^*_{1i}	…	SVA^*_{1n}
…	…	…	…	…	…	…
Банк j	θ_j	SVA^*_{j1}	…	SVA^*_{ji}	…	SVA^*_{jn}
…	…	…	…	…	…	…
Банк m	θ_m	SVA^*_{m1}	…	SVA^*_{mi}	…	SVA^*_{mn}

Примітка: D_i – інтегральний індекс загрози національної економіки за і-тий рік; θ_j – рівень використання банківської системи для легалізації злочинних доходів; SVA^*_{ji} - узагальнююча оцінка ризику використанням j-го банку для легалізації кримінальних доходів за і-тий рік.

В якості фактичних даних практичної побудови платіжної матриці гри «державного регулювання економічної безпеки національної економіки» пропонується обрати вибірку банків України, кожен з яких характеризується показником рівня використання з метою легалізації кримінальних доходів. Вони

дозволять сформувати рядки платіжної матриці. В межах стовбців платіжної матриці обрано динаміку показника інтегральний індекс загрози національної економіки з 2008 по 2019 рр. Сформувати внутрішній діапазон платіжної матриці зазначеної конфліктної ситуації між державою та економічними агентами, які намагаються легалізувати кримінальні доходи, пропонується шляхом використання узагальнюючої оцінки ризику використання в розрізі обраного переліку банків для легалізації кримінальних доходів станом на 2019 рік. Для обчислення даного ризику за 2008 – 2018 роки пропонується використати дані 2019 року, скориговані на співвідношення інтегрального індексу загрози поточного та 2019 року в розрізі кожного із вибраних для аналізу банків. Фрагмент результатів проведених розрахунків приведемо у вигляді таблиці 3.20.

Таблиця 3.20 – Фрагмент фактичних даних платіжної матриці гри «державного регулювання економічної безпеки національної економіки»

Рівень використання банківської системи з метою легалізації кримінальних доходів/ Інтегральний індекс загрози		2008	2009	2010	…	2017	2018	2019
		0,8148	0,2566	0,5144	…	0,5538	0,4557	0,6195
Bank 8	68,75	0,6939	0,2185	0,4381	…	0,4717	0,3881	0,5276
Bank 13	100,00	0,8148	0,2566	0,5144	…	0,5538	0,4557	0,6019
Bank 16	4,37	0,7142	0,2249	0,4509	…	0,4855	0,3995	0,6382
Bank 20	88,69	0,6736	0,2122	0,4253	…	0,4579	0,3768	0,6489
…	…	…	…	…	…	…	…	…
Bank 39	100,00	0,8822	0,2778	0,5570	…	0,5997	0,4934	0,6909
Bank 41	100,00	0,6222	0,1960	0,3929	…	0,4230	0,3480	0,6929
Bank 36	100,00	0,6204	0,1954	0,3917	…	0,4217	0,3470	0,6900
Bank 54	100,00	0,6230	0,1962	0,3933	…	0,4235	0,3484	0,7051

Останнім кроком постановки задачі у «теорії ігор» під час проведення державного регулювання економічної безпеки національної економіки є існування визначених правил у грі, що спричиняють наслідки використання кожного серед учасників своїх власних «чистих стратегій». Так, залежність узагальнюючої оцінки ризику використання банків для легалізації злочинних доходів від рівня загрози національної економіки та рівня використання банків

для легалізації доходів, отриманих злочинним шляхом, формалізуємо за допомогою інструментарію регресійного аналізу пакету MS Excel у вигляді побудови лінійного багатофакторного регресійного рівняння.

Залежність узагальнюючої оцінки ризику використання банків для легалізації кримінальних доходів від рівня загрози національної економіки та рівня використання банків для легалізації доходів, отриманих злочинним шляхом, формалізуємо з використанням приведеного нижче рівняння множинної регресії (формула 3.27):

$$\mathrm{SVA}^{*}_{ji} = -0{,}0150 + 0{,}0001 \cdot \theta_j + 0.9089 \cdot D_i \qquad (3.27)$$

де $\mathrm{D_i}$ – інтегральний індекс загрози національної економіки за і-тий рік;

θ_j – рівень використання j-го банку з метою легалізації кримінальних доходів;

SVA^{*}_{ji} - узагальнююча оцінка ризику використанням j-го банку для легалізації кримінальних доходів за і-тий рік.

Подальше вирішення задачі удосконалення системи державного регулювання економічної безпеки національної економіки вимагає проведення формалізації стратегій поведінки як з бору держави щодо заходів державного регулювання, так і з боку економічних агентів щодо використання банків з метою легалізації кримінальних доходів. Так, в таблиці 3.21 наведемо перелік відповідних стратегій для обох гравців розглянутої конфліктної ситуації.

Виходячи з доцільності виділення саме трьох стратегій поведінки економічних агентів в межах рівня використання банків з метою легалізації кримінальних доходів, відповідну шкалу інтервалів представимо у вигляді таблиці 3.22.

Таблиця 3.21 – Стратегії держави та економічних агентів щодо запобігання використання банків з метою легалізації кримінальних доходів

Стратегія	Рівень використання банків з метою легалізації кримінальних доходів	Держава
Стратегія A	Активного використання фінансових посередників з метою легалізації кримінальних доходів	Стратегія активної протидії легалізації кримінальних доходів
Стратегія B	Помірного використання фінансових посередників з метою легалізації кримінальних доходів	Стратегія помірної протидії легалізації кримінальних доходів
Стратегія C	Мінімального використання фінансових посередників з метою легалізації кримінальних доходів	Стратегія мінімальної протидії легалізації кримінальних доходів

Таблиця 3.22 – Шкала інтервалів значень рівня використання банків для легалізації кримінальних доходів

Показник	$(\bar{\theta} - 2\sigma k;\ \bar{\theta} + 2\sigma(k+1))$		
Якісна інтерпретація	Стратегія активного використання фінансових посередників з метою легалізації кримінальних доходів	Стратегія помірного використання фінансових посередників з метою легалізації кримінальних доходів	Стратегія мінімального використання фінансових посередників з метою легалізації кримінальних доходів
Шкала значень	[0; 30)	[30; 70)	[70; 100]

Переходячи до визначення кількісної відповідності значень рівня використання банків для легалізації кримінальних доходів якісній характеристиці, представленій в таблиці 3.22 за відповідною шкалою інтервалів, виникає необхідність перевірки вхідних даних нормальному закону розподілу в розрізі як рівня використання банків для легалізації кримінальних доходів, так і інтегрального індексу загрози національної економіки. Для реалізації даного кроку використаємо інструментарій програмного пакету Statistica: Statistics, Distribution Fitting, що дозволяє побудувати гістограму розподілу значень досліджуваного показника та за допомогою критерію Chi-Square перевірити відповідність нормальному закону розподілу з подальшою формалізацією шкали інтервалів значень.

Так в розрізі рівня використання банків для легалізації кримінальних доходів гістограма розподілу значень набуває вигляду рисунку 3.49 і дозволяє стверджувати про підтвердження гіпотези щодо відповідності нормальному закону розподілу рівнів даного ряду.

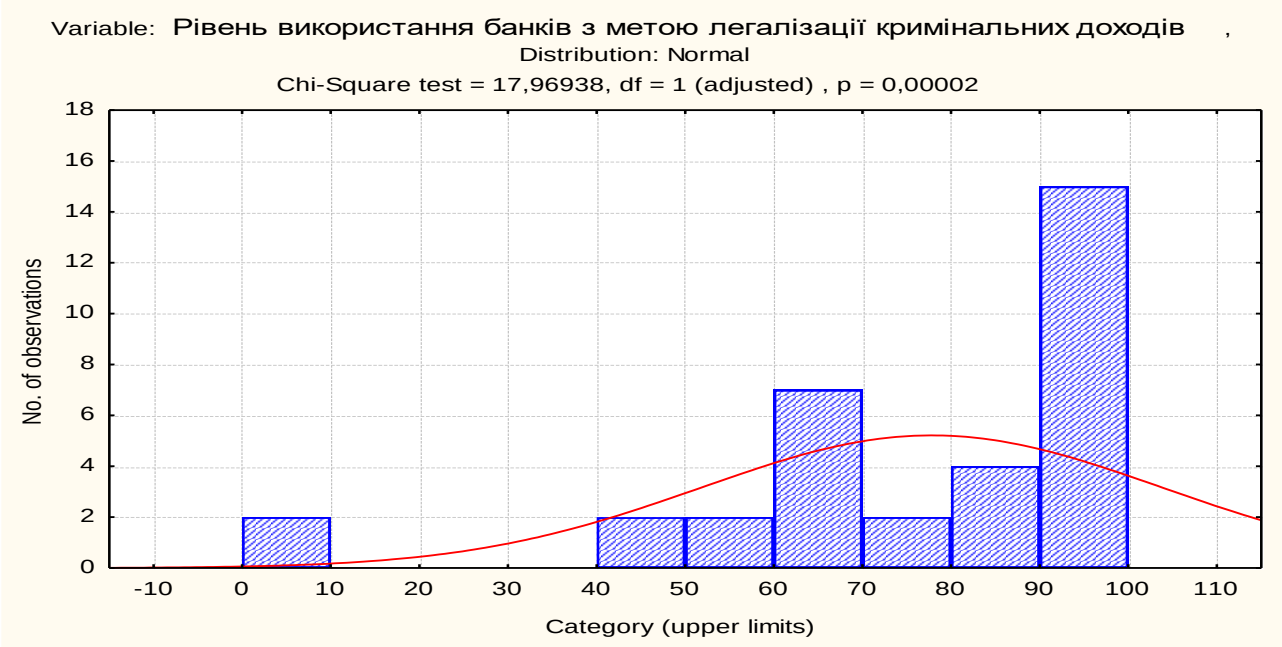


Рисунок 3.49 – Гістограма розподілу значень рівня використання банків для легалізації кримінальних доходів

Аналогічно описаному вище підходу проведено шкалювання інтервалів значень інтегрального індексу загрози національної економіки в розрізі стратегій поведінки держави (таблиця 3.23).

Таблиця 3.23 – Шкала інтервалів значень інтегрального індексу загрози національної економіки

Показник	$(\bar{\theta} - 2\sigma k;\ \bar{\theta} + 2\sigma(k+1))$		
Якісна інтерпретація	Стратегія активної протидії легалізації кримінальних доходів	Стратегія помірної протидії легалізації кримінальних доходів	Стратегія мінімальної протидії легалізації кримінальних доходів
Шкала значень	[0; 0,43)	[0,43; 0,67)	[0,67; 100]

Виконавши процедуру формалізації процесу державного регулювання економічної безпеки національної економіки, розглянемо методику вирішення поставленої задачі. У межах методики «теорії ігор» для обрання раціональної ефективної стратегії поведінки держави, яка намагається мінімізувати інтегральний індекс загрози національної економіки, та економічними агентами, які намагаються збільшити рівень використання банківської системи з метою легалізації кримінальних доходів вирішено застосувати критерій: мінімаксу та максиміну відповідно. Цей критерій надає можливість встановити мінімально, а також максимально можливий певний середній рівень ризику використання банків для легалізації кримінальних доходів. Такі умови з математичної сторони можна відобразити у подібним способом (формула 3.28):

$$\alpha = \max_i \left(\min_j a_{ij} \right), \qquad \beta = \min_j \left(\max_i a_{ij} \right), \tag{3.28}$$

де $\alpha\,(\beta)$ – мінімально (максимально) можливий рівень ризику використання банків для легалізації кримінальних доходів, досягнутий за результатами регулюючих дій держави, яка намагається мінімізувати інтегральний індекс загрози національної економіки, та відповідних дій економічних агентів, які намагаються збільшити рівень використання банків з метою легалізації кримінальних доходів.

У ситуації, за якої $\alpha = \beta$ є змога встановити розмір максимального допустимого узагальнюючого рівня ризику використання банків для легалізації кримінальних доходів, а саме встановити її точкову величину. В цій ситуації набуття визначеного рівня ризику можливе за рахунок застосування кожним із учасників їх власних чистих стратегій. У протилежному випадку можна встановити розмір інтервальної оцінки максимального ризику використання банків для легалізації кримінальних доходів, і як результат використання

економічними агентами, які намагаються збільшити рівень використання банків з метою легалізації кримінальних доходів (формула 3.29) та державою, яка намагається мінімізувати інтегральний індекс загрози національної економіки (формула 3.30).

$$S_A^* = (p_1^*, p_2^*, ..., p_m^*), \tag{3.29}$$

де S_A^* – оптимальний змішаний тип стратегії «учасника А»;

p_i^* –певна імовірність використання *i-ї* чистої стратегії учасника А.

$$S_B^* = (q_1^*, q_2^*, ..., q_n^*), \tag{3.30}$$

де S_B^* – оптимальний змішаний тип стратегія «учасника Б»;

q_i^* – імовірність використання *i-ї* чистої стратегії учасника Б.

І як результат того, що держава застосовує мінімаксний тип стратегії, а економічні агенти використовують протилежний максимінний тип стратегії, розрахунок ціни гри (максимальний середній рівень ризику використання банків для легалізації кримінальних доходів)здійснюється з використанням теореми Неймана у вигляді формули 3.31:

$$v = \sum_{j=1}^{n}\sum_{i=1}^{m} a_{ij} p_i^* q_j^*, , \tag{3.31}$$

де v – мінімальна величина максимально можливого рівня ризику використання банків для легалізації кримінальних доходів.

Переходячи до практичного впровадження максимінної та мінімаксної стратегій гри «державного регулювання економічної безпеки національної економіки» як конфліктної ситуації між державою, яка намагається мінімізувати інтегральний індекс загрози національної економіки, та економічними агентами, які намагаються збільшити рівень використання банківської системи з метою легалізації кримінальних доходів, побудуємо таблицю 3.24, де візуально

зобразимо описаний вище механізм пошуку оптимальних стратегій дій гравців, та таблицю 3.25, де представимо фрагмент практичного впровадження гри.

Таблиця 3.24 – Візуалізація механізму впровадження максимінної та мінімаксної стратегій гри

Рівень використання банківської системи з метою легалізації кримінальних доходів/ Інтегральний індекс загрози		Рік 1	…	Рік і	…	Рік n	Нижня межа ризику використання банку для ЛКД	
		D_1	…	D_i	…	D_n	min	maxmin
Банк 1	θ_1	SVA^*_{11}	…	SVA^*_{1i}	…	SVA^*_{1n}	$\min_i \mathrm{SVA}^*_1$	$\max_j \min_i \mathrm{SVA}^*_{ji}$
…	…	…	…	…	…	…	…	
Банк j	θ_j	SVA^*_{j1}	…	SVA^*_{ji}	…	SVA^*_{jn}	$\min_i \mathrm{SVA}^*_{ji}$	
…	…	…	…	…	…	…	…	
Банк m	θ_m	SVA^*_{m1}	…	SVA^*_{mi}	…	SVA^*_{mn}	$\min_i \mathrm{SVA}^*_m$	
Верхня межа ризику використання банку для ЛКД	Max	$\max_j \mathrm{SVA}^*_{j1}$	…	$\max_j \mathrm{SVA}^*_j$	…	$\max_j \mathrm{SVA}^*_{jn}$		
	minmax	$\min_i \max_j \mathrm{SVA}^*_{ji}$						

Таблиця 3.25 – Фрагмент практичного впровадження максимінної та мінімаксної стратегій гри

Рівень використання Банківської системи з метою легалізації кримінальних доходів/ Інтегральний Індек сзагрози		2008	2009	2010	…	2018	2019	min	maxmin
		0,8148	0,2566	0,5144	…	0,4557	0,6195		
Bank 8	68,75	0,6939	0,2185	0,4381	…	0,3881	0,5276	0,2185	0,3058
Bank 13	100,00	0,8148	0,2566	0,5144	…	0,4557	0,6019	0,2566	
Bank 16	4,37	0,7142	0,2249	0,4509	…	0,3995	0,6382	0,2249	
Bank 20	88,69	0,6736	0,2122	0,4253	…	0,3768	0,6489	0,2122	
Bank 50	100,00	0,6624	0,2086	0,4182	…	0,3705	0,7000	0,2086	
Bank 1	100,00	0,6141	0,1934	0,3878	…	0,3435	0,4428	0,1934	
Bank 4	69,09	0,9708	0,3058	0,6130	…	0,5430	0,4880	0,3058	
…	…	…	…	…	…	…	…	…	
	Max	0,9708	0,3058	0,6130	…	0,5430	0,7266		
	Minmax	0,3058			.				

Таким чином, економічні агенти намагаються збільшити рівень використання банківської системи з метою легалізації кримінальних доходів. Тому в розрізі рядків таблиці 3.25 ми спочатку визначаємо мінімально можливий рівень ризику використання банків для легалізації кримінальних доходів, який держава в свою чергу намагається знизити за рахунок регулюючих заходів, що передбачає необхідність пошуку максимального з мінімально можливих рівнів ризику. Це передбачає необхідність для економічних агентів застосування чистої стратегії, кількісною мірою якої виступає рівень використання банків з метою легалізації кримінальних доходів на рівні 69,09%, що відповідає стратегії помірного використання фінансових посередників з метою легалізації кримінальних доходів.

В свою чергу, держава намагається мінімізувати інтегральний індекс загрози національної економіки, застосовуючи мінімаксну стратегію. Тобто спочатку обчислюється максимально можливий рівень ризику використання банків для легалізації коштів, отриманих злочинним шляхом як результат дій економічних агентів, які цьому сприяють. Далі визначаємо мінімально можливе значення, що відповідає намірам держави за рахунок регулювання зменшити узагальнюючу оцінку даного ризику, обираючи таку стратегію поведінки, яка дозволяє мінімізувати інтегральний індекс загрози національної економіки. Отже, для держави пропонується використовувати оптимальну чисту стратегію, яка відповідає інтегральному індексу загрози національної економіки на рівні 0,2566 частки одиниці, що відповідає стратегії активної протидії легалізації кримінальних доходів. При цьому узагальнююча оцінка ризику використання банків для легалізації кримінальних доходів становитиме 0,3058 частки одиниці.

Враховуючи вищевикладене, сформовано висновок, що для удосконалення Державного регулювання економічної безпеки національної економіки, запропоновано застосовувати інструментарій «теорія ігор». Практичне застосування такої методики дозволить вирішити ряд існуючих проблемних питань у напрямі сучасного, новітнього розвитку країни. Це допоможе створити дієві інструменти для стабільного розвитку національної

економіки, забезпечить стійку макроекономічну позицію, дозволить зменшити економічну, технологічну та виробничу залежність держави, знизити рівень інфляції, скоротити ресурсну заборгованість країни, збільшити імпорт, зменшити експорт, сприятиме розвитку міжнародних ділових відносин, залучення іноземних інвестицій, допоможе знизити рівень корупції та впливу її негативних наслідків на економіку, зменшити розрив у фінансовому рівні забезпечення серед населення країни, забезпечить збалансованість бюджету, скорочення дефіцит бюджету, сприятиме збільшенню податкових надходжень до бюджету, дозволить забезпечити конкурентоспроможність країни, допоможе забезпечити стійкість до дестабілізуючих факторів.

Пункт 3.4.2 даного звіту було виконано із використанням матеріалів публікацій виконавців [186, 329, 330].

ВИСНОВКИ

Представлені у першому розділі наукові результати створюють передумови формування ефективної системи кібербезпеки банків, спрямованої на боротьбу із банківськими шахрайствами. Серед основних результатів, що мають наукову новизну і практичну значущість, слід зазначити такі:

- проведений аналіз кіберзагроз дозволив визначити найбільш проблемні діялнки банківської діяльності, які піддаються найбільшого впливу з боку шахраїв. В результат виявлено, що проблемними є операції, які здійснюються за допомогою Інтернет-банкінгу та мобільного банкінгу, а найбільш розповсюдженими методами шахрайства є соціальна інженерія, в результаті чого населення України, які є клієнтами банків, все частіше становиться об’єктом шахрайства;
- проведений первинний аналіз даних щодо загальних сум транзакцій; типів пристроїв, з яких здійснювалася транзакція; місцеположення пристрою, з якого проведено транзакцію; країни, яка була вказана користувачем мобільного або інтернет-банкінгу при реєстрації; суми, що знаходиться на балансі клієнта після проведення транзакції; суми, що знаходилась на балансі клієнта до проведення транзакції; типу транзакції, яку було проведено користувачем мобільного або інтернет-банкінгу. Результати аналізу дозволили виділити ті вузькі місця в системі кіберзахисту, які піддаються шахрайствам;
- проведений кластерний аналіз дозволив виділити найбільш важливі змінні та сгрупувати операції за сумою транзакції та балансом, місцем знаходженням, новим значенням балансу після проведення транзакції. Результати кластерного аналізу дозволили нам виявити основні групи банківських операцій, що підпадають під ознаки кібершахрайств, що дозволяє організувати моніторинг саме за цими групами, та сформувати основні гіпотези, які сприяли розробці моделей інтелектуального аналізу;

- розроблено концептуальну модель, побудовану на основних гіпотезах виникнення ознак кібершахрайств, що дозволило обрати фактори, які ідентифікують операцію, як шахрайську. Це, в свою чергу, сприяло розробці математичних моделей визначення ймовірності виникнення ознак кібершахрайських операцій із використанням Data Mining, які дозволять виявляти в транзакціях ознаки кібернетичних загроз, тим самим попереджаючи користувачів мобільного та інтернет-банкінгу від можливих збитків, завданих злочинними діями;
- розроблено інформаційні моделі виявлення ознак шахрайства з боку зовнішніх та внутрішніх шахраїв з урахуванням системного підходу та на основі стандарту BPMN 2.0, які базуються на запропонованих моделях Data Mining. Дані моделі слугуватимуть підґрунтям для розробки автоматизованого модулю банківського моніторингу та його інтеграції в автоматизовану банківську систему;
- розроблено математичні портрети потенційних жертв та шахраїв, що дозволяють ідентифікувати ситуації ймовірного виникнення ознак кібершахрайств. Врахування таких ознак, як вік, стать, соціальне становище, способи здійснення операцій (Інтернет, мобільний телефон, тощо), історію клієнта, місце здійснення операції, та інше, дозволяють банківським підрозділам кіберзахисту швидко реагувати на зміни та попереджувати шахрайства на ранніх етапах;
- розроблено науково-методичний підхід до визначення ймовірних збитків банків від їх залучення до шахрайських операцій із застосуванням витратного підходу, витратних матриць, формуванням дерева рішень можливих альтернатив, який сприятиме зменшенню ризиків шахрайських операцій банківської діяльності, підвищенню системи внутрішньобанківського моніторингу сприятиме;
- запропонований механізм моделювання кількісної оцінки рівня операційного ризику банку в сфері інформаційної безпеки дозволить банківським установам значно знизити ризики інформаційного характеру та

ефективно управляти операційними ризиками в напрямку інформаційних активів;

- розроблено модель впливу макроекономічних факторів на формування схильності до шахрайства в банківській сфері, яка включає три сфери – економічну (мінімальна заробітна плата населення, індекс економічної свободи, ВВП на душу населення), політичну (рівень сприйняття корупції, індекс цивільної свободи, рівень злочинності в країні та індекс недієздатності держави), соціальну (індекс цивільно свободи, індекс процвітання, індекс миру, населення, яке проживає в країні, індекс щастя та індекс людського розвитку). В результаті побудовано трикутник з урахуванням даних сфер, за допомогою якого на основі аналізу центру мас визначається схильність до шахрайства з банківськими продуктами. Запропонована методика дозволяє прогнозувати та попереджати шахрайські операції на макрорівні, шляхом розробки превентивних заходів контролю, як частини системи кібербезпеки;
- розроблено гравітаційну модель оцінки привабливості країни для легалізації кримінальних доходів, що дозволить зменшити ризики для держави з боку легалізації кримінальних доходів та фінансування тероризму, які здійснюються за допомогою банківського сектору. Її застосування дозволить сформувати інформаційну базу для прийняття управлінських рішень щодо підвищення рівня кіберзахисту, оскільки це надає можливості концентрувати увагу саме на тих країнах, з якими ризик легалізації є підвищеним. Впровадження даної методики сприятиме розробці нових інструментів моніторингу, аналізу, оцінки та прогнозування фінансових операцій, здійснення яких можливе за межами країни;
- розроблено прототип автоматизованого модулю процесу виявлення шахрайських операцій з банківськими картками, які здійснюються через Інтернет в процесі он-лайн платежів. В результаті модуль дозволяє відслідковувати операції, які потенційно можуть бути шахрайськими з урахуванням кількості карток клієнта, його місцезнаходженням та месцем здійснення операції, місцезнаходженням та адресою доставки, тощо.

Запропонований модуль дозволяє попереджати клієнтів про факт здійснення шахрайства та попереджувати його.

Представлені у другому розділі 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.

Представлені у третьому розділі наукові результати створюють передумови розробки внутрішньобанківської системи кібербезпеки та організаційно-інституційних засад забезпечення стійкості фінансового кіберпростору на загальнодержавному рівні. Серед основних результатів, що мають наукову новизну і практичну значущість, слід зазначити такі:

- проведено канонічний аналіз взаємозв'язку кібербезпеки та соціо-економіко-політичного розвитку країни: для дослідження обрано дані національного індексу кібербезпеки та фактори соціо-економіко-політичного

розвитку для 159 країн світу; побудовано карту країн світу із зазначенням національного індексу кібербезпеки; визначено канонічні корені, факторну структуру, дисперсію та надмірність, канонічні ваги для факторів, регресійні рівняння. Результати аналізу підтвердили справедливість гіпотези, що фактори розвитку обумовлюють рівень інформаційної безпеки та навпаки, рівень безпеки може впливати на розвиток країни. Практичне значення отриманих результатів полягає у виробленні ряду стратегічних заходів: посилення інститутів безпеки, впровадження нових методів та заходів безпеки, що, в свою чергу, позитивно впливатиме на політичну стабільність в країні, соціальну захищеність населення від кібершахрайств, зниження збитків економіки держави та суб'єктів господарювання від незаконного використання ресурсів;

- проведено оцінку рівня інформаційної безпеки країни з урахуванням їх розвитку, що відбуватиметься з використанням самоорганізованих карт Кохонена: обрано дві групи показників – індекси інформаційної безпеки та розвитку для 159 країн світу; для виявлення показників із тісним статистичним зв'язком проведено кореляційний аналіз, за результатами якого було відібрано 12 показників розвитку; для приведення даних у співставні величини було проведено нелінійну нормалізацію; за допомогою аналітичної платформи Deductor Academic дані було перевірено на якість, наявність викидів, дублікатів та протиріч. На основі побудованих карт Кохонена отримано 7 кластерів країн: 0-й та 1-ий включає країни з найвищими показниками розвитку та безпеки, 2-й – країни з показниками вище середнього, 3-й – із середнім рівнем розвитку та безпеки, 4-й – рівнем нижче середнього, 5-й – низьким рівнем, 6-й – дуже низьким. Практичне застосування отриманих результатів дозволить виділити групи країн, які слабко розвиваються у напрямку підвищення ефективності системи інформаційної безпеки, а також ті сфери, які потребують додаткової уваги з боку відповідних державних органів, які займаються питаннями безпеки країни;
- проведене рейтингування 160 країн світу за рівнем кібербезпеки та ефективності системи інформаційної безпеки країни за допомогою використання

багатоатрибутних методів прийняття рішень (методи TOPSIS, VIKOR та MAAM). В результаті встановлено, що рейтинг за методом MAAM має близько 25% подібності із значеннями реального рейтингу. Найбільш ефективним для рейтингування країн виявився метод TOPSIS, який нівелює недоліки методу реальної оцінки та дозволяє визначати найкращу та найгіршу альтернативу, що сприяє здійсненню аналізу окремо й для показників. Застосування запропонованого підходу дозволяє вирішити ряд проблем, пов'язаних із розмірністю даних, визначенням вагів показників, врахуванням різнонаправленості значень показників та їх кардинальних відмінностей. Практичні результати показали, що країни Естонія та Чеська Республіка мають найвищі рейтинги та значення їх показників найбільше наближається до ідеальних, тобто доцільно звернути увагу на їх практику щодо формування стратегії кібербезпеки, особливо в частині тих показників, які для кожної окремої країни значно відхиляються від ідеальних та мають критичні значення. Країною із самим низьким рейтингом, що було підтверджено розрахунками за всіма методами, є Південний Судан. Оскільки вона має проблеми політичного, військового, соціально-економічного характеру, то це підтверджує відсутність пріоритету забезпечення її кіберзахисту;

- розроблено фронтірну модель оцінювання та оптимізації ефективності роботи внутрішньобанківської ALM-системи за допомогою програмного забезпечення Banxia Frontier Analyst 4 на основі технології Data Envelopment Analysis (DEA). Практичне запровадження такої моделі надасть можливість провести аналіз ефективності системи кібербезпеки банку, побудувати візуалізацію важливих даних, визначити слабкі та сильні сторони системи, глибше їх вивчити, ефективніше розподілити наявні ресурси для забезпечення кіберзахисту, що допоможе у боротьбі з банківським кібершахраями;
- побудовано економіко-математичну модель вибору стратегій державного регулювання економічної безпеки національної економіки як основи для подальшого формування внутрішньобанківських інструкцій щодо

організації AML-системи та системи кіберзахисту на основі застосування інструментарію теорії ігор (максимінний та мінімаксний критерії за допомогою теореми Неймана). Модель здійснює формалізацію системи заходів Державного регулювання економічної безпеки національної економіки, щодо знаходження компромісної точки у тріаді таких напрямів: зведення до мінімуму величини інтегрального індексу загрози національної економіки, мінімізації рівня використання банків з метою легалізації кримінальних доходів за рахунок максимізації рівня ефективності внутрішньобанківської системи фінансового моніторингу в розрізі певного банку та одночасної мінімізації узагальнюючої оцінки ризику використання банків для легалізації кримінальних доходів. Практичне застосування такої методики допоможе створити дієві інструменти для стабільного розвитку національної економіки, забезпечить стійку макроекономічну позицію, допоможе знизити рівень корупції, зменшити розрив у фінансовому рівні забезпечення серед населення країни, сприятиме збільшенню податкових надходженьдо бюджету, допоможе забезпечити стійкість до дестабілізуючих факторів;

- проведено оцінку інтегрального індексу загрози національної економіки як одного із векторів стратегії забезпечення стійкості фінансового кіберпростору на загальнодержавному рівні на основі застосування функції Кернела. Для здійснення оцінки індексу загрози національної економіки побудовано структурно-логічну математичну модель, що включає послідовність етапів дослідження: створено інформаційну базу вхідних предикторів за досліджуваний період часу; приведено показники вхідної інформаційної бази дослідження до співставного вигляду шляхом проведення нелінійної нормалізації; відібрано релевантні показники оцінювання індексу загрози національної економіки на базі комбінації методів Парето та діаграми розсіювання; проведено оцінювання інтегрального індексу загрози національної економіки за допомогою функції Кернела та мультиплікативної форми згортки. Здійснено візуалізацію як загальної тенденції поведінки інтегрального індексу загрози в часі, так і варіації в межах від мінімально та максимально можливих

рівнів. Практичне застосування запропонованої методології дозволить своєчасно та оперативно забезпечувати підтримку необхідних організаційних, інституційних, нормативно-правових умов, що передбачають спроможність системи національної економіки до протистояння зовнішніх та внутрішніх загроз та навантажень, подальшої якісної адаптації до проблем та дестабілізуючих факторів, швидкому відновленню після впливу негативних чинників.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Данилов В. Кибербезопасность в банковской сфере. ICF Legal Servic : веб-сайт. 2017. URL: https://icf.ua/blog/view/kiberbezopasnost-v-bankovskoy-sfere. (дата звернення 18.12.2020)

2. Проект Стратегії забезпечення кібернетичної безпеки України. URL: http://www.niss.gov.ua/public/File/2013_ nauk_an_rozrobku/kiberstrateg.pdf. (дата звернення 18.12.2020)

3. The Top Five Security Threats to Your Banking Institution. URL: http://www.level3.com/-/media/files/infographics/en_infg_financialserv_topnetworksecuritythreats_regionalbanks.pdf. (дата звернення 18.12.2020)

4. DoS-атака. Вікіпедія : веб-сайт. URL: https://ru.wikipedia.org/wiki/DoS-атака.

5. Qijun Gu, Peng Liu Denial of Service Attacks. URL: https://s2.ist.psu.edu/paper/DDoS-Chap-Gu-June-07.pdf. (дата звернення 18.12.2020)

6. K. Munivara Prasad, A. Rama Mohan Reddy, K. Venugopal Rao. DoS and DDoS Attacks: Defense, Detection and Traceback Mechanisms – A Survey. Global Journal of Computer Science and Technology: E Network, Web & Security. 2014. № 14 (7). URL: https://globaljournals.org/GJCST_Volume14/3-DoS-and-DDoS-Attacks-Defense-Detection.pdf. (дата звернення 18.12.2020)

7. Загидиев А.М. Киберугрозы в банковской сфере. Научное сообщество студентов XXI столетия. Єкономические науки: сб. ст. по мат. XXXI междунар. студ. науч.-практ. конф. № 4 (31).

8. Trend Report «Financial Cyber Threats Q1 2017» conducted with Kaspersky Labs and Telefónica. URL: http://www.level3.com//media/files/infographics/en_infg_financialserv_topnetworksecuritythreats_regionalbanks.pdf. (дата звернення 18.12.2020)

9. IT threat evolution Q3 2017. Statistics. Securelist : веб-сайт. URL: https://securelist.com/it-threat-evolution-q3-2017-statistics/83131/. (дата звернення 18.12.2020)

10. Головна мобільна кіберзагроза. Харківська обласна охорона : веб-сайт. URL: http://www.ohrana-ua.com/articles/837-golovna-moblna-kberzagroza.html. (дата звернення 18.12.2020)

11. Кібербезпека в боротьбі з банківськими шахрайствами: захист споживачів фінансових послуг та зростання фінансово-економічної безпеки України : звіт про НДР (проміжний) / кер. О. В. Кузьменко. Суми : СумДУ, 2018. 199 с.

12. The official site of the company “SAS” (2016), “SAS Enterprice Miner. Solution Overview”. URL: https://www.sas.com/content/dam/SAS/ru_ru/doc/factsheet/sas-enterprise-miner-04-04-2016.pdf. (дата звернення 18.12.2020)

13. Чернышова Г. Ю. Интеллектуальный анализ данных: учебное пособие для студентов. Саратов : Саратовский государственный социально-экономический университет, 2012. 92 с.

14. Барсегян А. А., Куприянов М. С., Степаненко В. В., Холод И. И. Методы и модели анализа данных: OLAP и Data Mining. Санкт-Петербург : БХВ-Петербург, 2004. 336 с.

15. Бахрушин В. Є. Методи аналізу даних : навч. посіб. Запоріжжя : КПУ, 2011. 268 с.

16. Кластерний аналіз. Вікіпедія : веб-сайт. URL: http://uk.wikipedia.org/wiki/Кластерний_аналіз. (дата звернення 18.12.2020)

17. Яровенко Г. М., Сковронська А. І., Бояджян М. М. Моделювання виявлення ознак кіберзагроз в банках із використанням інтелектуального аналізу. *Ефективна економіка*. 2018. № 7. URL: http://www.economy.nayka.com.ua/pdf/7_2018/39.pdf. (дата звернення 18.12.2020)

18. Сучасні інструменти боротьби з кібершахрайствами у банках : монографія / О. В. Кузьменко, Г.М. Яровенко, С. В. Лєонов та ін. / за заг. ред. О.

В. Кузьменко, Г. М. Яровенко. Суми : Сумський державний університет, 2018. 143 с.

19. Ryan C. Hybrid Risk: The truth behind first party fraud. The official site of the company "Experian". 2015. URL: http://www.experian.com/blogs/insights/2015/10/hybrid-risk-the-truth-behind-first-party-fraud/. (дата звернення 18.12.2020)

20. Third Party Fraud. Open Risk Manual : website. 2017. URL: https://www.openriskmanual.org/wiki/Third_Party_Fraud. (дата звернення 18.12.2020)

21. #FraudStats. Experian: website. 2018. URL: https://www.experian.co.uk/identity-and-fraud/fraud-statistics/. (дата звернення 18.12.2020)

22. What is Mortgage Fraud? MortgageLoan.com : website. 2015. URL: https://www.mortgageloan.com/. (дата звернення 18.12.2020)

23. Яровенко Г. М., Ковач В. О. Моделювання портретів потенційних шахрая та жертви банківських шахрайств. *Ефективна економіка*. 2018. № 10. URL: http://www.economy.nayka.com.ua/pdf/10_2018/63.pdf. (дата звернення 18.12.2020)

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

25. AllFusion® Process Modeler Data Flow Diagramming. Design Guide r7.2. CA : website. 2006. URL: https://supportcontent.ca.com/cadocs/0/e002761e.pdf. (дата звернення 18.12.2020)

26. Business Process Model and Notation (BPMN) Version 2.0. Object Management Group : website. 2011. URL: http://www.omg.org/spec/BPMN/2.0. (дата звернення 18.12.2020)

27. Рекомендації щодо зниження ризику шахрайських операцій НБУ 04.07.2018 № 57-0009/36366. URL: http://zakon.rada.gov.ua/laws/show/v3636500-18. (дата звернення 18.12.2020)

28. Левченко В. П., Бойко А. О., Доценко Т. В. Оцінювання збитків банків від їх залучення до процесу легалізації кримінальних доходів. *Науковий журнал "Причорноморські економічні студії"*. Одеса, 2018. № 35 (2). С. 22-27.

29. Boiko A., Dotcenko T. Modeling the probable losses of banks from their involvment in the process of legalization (laundering) of inflammable funds. *Advanced Information Systems and Technologies*: proceedings of the VI international conference, Sumy, May 16-18 2018 / edited by S. I. Protsenko, V.V. Shendryk. Sumy : SSU, 2018. P.133-136.

30. Дмитров О. С. Моделювання оцінки операційного ризику комерційного банку : монографія / О. С. Дмитров, К. Г. Гончарова, О. В. Меренкова (Кузьменко) та ін. / за заг. ред. О. С. Дмитрова. Суми : ДВНЗ “УАБС НБУ”, 2010. 264 с.

31. Кібальник Л. О., Напора І. Ю. Концептуальний підхід до формування інформаційної безпеки банківських установ в системі економічної безпеки. *Ефективна економіка*. 2016. № 12. URL: http://www.economy.nayka.com.ua/?op=1&z=5303. (дата звернення 18.12.2020)

32. ГСТУ СУІБ 1.0/ISO/IEC 27001:2010. Інформаційні технології - методи захисту – система управління інформаційною безпекою. Офіційний переклад, ст.3.

33. Щодо впровадження системи управління інформаційною безпекою та методики оцінки ризиків відповідно до стандартів Національного банку України : метод. рек. від 03.03.2011 № 24-112/365. URL: http://document.ua/shodo-vprovadzhennja-sistemi-upravlinnja-informaciinoyu-bezp-doc49593.html. (дата звернення 18.12.2020)

34. Про організацію заходів із забезпечення інформаційної безпеки в банківській системі України : положення, затверджене Постановою Правління НБУ від 28 вересня 2017 року № 95. URL: https://bank.gov.ua/document/download?docId=56426049. (дата звернення 18.12.2020)

35. Щодо організації та функціонування систем ризик-менеджменту в банках України : метод. рек., схвалені Постановою Правління НБУ від 02 серпня 2004 № 361. URL: http://zakon.nau.ua/doc/?uid=1045.5945.1&nobreak=1. (дата звернення 18.12.2020)

36. Иванов С. В. Преимущества генетических алгоритмов и их применение в медицине. *Актуальные проблемы гуманитарных и естественных наук*. 2014. № 10. С. 44-47.

37. Нейман Дж., Моргенштерн О. *Теория игр и экономическое поведение*. Москва : Наука, 1970. 708 с.

38. Кривошапова С. В., Литвин Е. А. Оценка и способы борьбы с мошенничеством с банковскими картами. *Международный журнал прикладных и фундаментальных исследований*. 2015. № 4. С. 116–120.

39. Буреева Н.Н. Многомерный статистический анализ с использованием ППП “STATISTICA” : учебно-метод. материалы. Нижний Новгород, 2007. 112 с.

40. Барсегян А. А., Куприянов М. С., Степаненко В. В. Методы и модели анализа данных: OLAP и Data Mining. Санкт-Петербург : БХВ. 2004. 336 с.

41. Згуровський М. З., Панкратова Н. Д. Основи системного аналізу. Київ : BHV, 2007. 544 с.

42. Кузьменко О. В., Колотіліна О. В. Моделювання оцінювання рівня економічного, соціального та політичного розвитку України, Італії та Франції в контексті оптимізації їх взаємодії. *Сталий розвиток економіки*. 2018. № 2 (39). С. 111-120.

43. Kuzmenko O. V. Practical aspects of modeling the stable political and economic situation in the country on the basis of multi-criteria optimization methods. *Journal of Strategic and International Studies*. 2014. № 4 (9). P. 17-24.

44. Berzin P., Shyshkina O., Kuzmenko O., Yarovenko H. Innovations in the risk management of the business activity of economic agents. *Marketing and Management of Innovations*. 2018. № 4. P. 221-233.

45. Яровенко Г.М., Бояджян М.М. Концептуальна модель виявлення ознак кібершахрайств в банках. *Сучасні міжнародні економічні відносини: становлення та шляхи перспективного розвитку* : зб. тез наук. робіт учасн. всеукр. наук.-практ. конф., м. Одеса, 9-10 лют. 2018 р. Одеса : ЦЕДР, 2018. С. 98-100.

46. Бояджян М. М., Яровенко Г. М. Оцінка впливу макроекономічних факторів на формування схильності до шахрайства в банківській сфері. *Проблеми та перспективи розвитку фінансово-кредитної системи України* : зб. матеріалів ІІІ Всеукр. наук.-практ. on-line конф., м. Суми, 22-23 лист. 2018 р. Суми : ННІ БТ «УАБС» СумДУ, 2018. С. 294-297.

47. Бояджян М. М. Оцінка впливу макроекономічних факторів на формування схильності до шахрайства в банківській сфері : робота на здобуття кваліфікаційного ступеня магістр : 051 – економіка / СумДУ. Суми, 2018. 92 с.

48. Lyeonov S., Kuzmenko O., Yarovenko H., Dotsenko T. The Innovative Approach to Increasing Cybersecurity of Transactions Through Counteraction to Money Laundering. Marketing and Management of Innovations. 2019. № 3. P. 308-326.

49. Business Process Model and Notation (BPMN) version 2.0. Object Management Group : website. 2011. URL: http://www.omg.org/spec/BPMN/2.0. (дата звернення 18.12.2020)

50. PHP Manual URL: https://secure.php.net/manual/en/intro-whatcando.php. (дата звернення 18.12.2020)

51. Яровенко Г. М., Клімов С. В. Система виявлення шахрайських операцій з банківськими картками. *Проблеми та перспективи розвитку фінансово-кредитної системи України* : зб. матеріалів ІІІ Всеукр. наук.-практ. on-line конф., м. Суми, 22-23 лист. 2018 р. Суми : ННІ БТ «УАБС» СумДУ, 2018. С. 303-307.

52. Клімов, С.В. Розробка прототипу автоматизованого модулю процесу виявлення шахрайських операцій з банківськими картками : робота на здобуття кваліфікаційного ступеня магістра : 051 – економіка / СумДУ. Суми, 2018. 82 с.

53. Boer M., Vazquez J. Cyber Security & Financial Stability: How cyber-attacks could materially impact the global financial system. 2017. 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 18.12.2020)

54. 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 18.12.2020)

55. 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 18.12.2020)

56. 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 18.12.2020)

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

58. Кірєєв О. І. Внутрішній аудит у банку : навч. посіб. Київ : Центр навчальної літератури, 2006. 220 с.

59. Костырко Л. А. Банковский аудит : учеб. пособ.. Луганск, 1998. 220 с.

60. Маркевич М. А. Організація і методика внутрішнього аудиту в банку : дис. ... канд. екон. наук : 08.00.09. Київ, 2011. 301 с.

61. Письменна М. С. Внутрішній аудит в банківській системі : дис. ... канд. екон. наук : 08.00.09 Одеса, 2011. 265 с.

62. Аудит у банках : навч. посіб. / за заг. ред. О. М. Сарахман. Київ : УБС НБУ, 2007. 334 с.

63. Внутрішній аудит у банку : навч. посіб. / О. М. Сарахман та ін. Київ: УБС НБУ, 2015. 239 с.

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

65. Банк С. В. Аудит в коммерческих банках: учеб. пособ.. Москва : Экономистъ, 2007. 156 с.

66. Аудит банков: учеб. пособ. / Г. Н. Белоглазова, Л. П. Кроливецкая, Е. А. Лебедев и др. / под ред. Г. Н. Белоглазовой, Л. П. Кроливецкой. 2-е изд., перераб. и доп. Москва : Финансы и статистика, 2005. 413 с.

67. Соколинская Н. Э. Банковский аудит. Москва : Перспектива, 1994. 118 с.

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

69. 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.* 2007. P. 34-40.

70. 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 18.12.2020)

71. 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 18.12.2020)

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

73. 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 18.12.2020)

74. 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 18.12.2020)

75. 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. P. 1-12. URL: https://ibimapublishing.com/articles/JIACS/2011/726196/726196.pdf. (дата звернення 18.12.2020)

76. 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 18.12.2020)

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

78. 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.

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

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

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

82. 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.

83. Кібальник Л. О., Напора І. Ю. Впровадження політики інформаційної безпеки банківських установ. *Причорноморські економічні студії*. 2016. № 12(2). С. 119-122. URL: http://nbuv.gov.ua/UJRN/bses_2016_12(2)__23. (дата звернення 18.12.2020)

84. Король О. Г. Аналіз загроз і механізмів забезпечення безпеки інформації в системі електронних платежів комерційного банку України. *Системи обробки інформації*. 2015. № 9. С. 88-95. URL: http://nbuv.gov.ua/UJRN/soi_2015_9_21. (дата звернення 18.12.2020)

85. Щодо організації та функціонування систем ризик-менеджменту в банках України: методичні рекомендації, схвалені Постановою Правління НБУ від 02 серп. 2004 р. № 361. URL: http://zakon.nau.ua/doc/?uid=1045.5945.1&nobreak=1. (дата звернення 18.12.2020)

86. 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.

87. 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 18.12.2020)

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

89. Хох В. Д., Мелешко Є. В., Смірнов О. А. Дослідження методів аудиту систем управління інформаційною безпекою. *Системи управління, навігації та зв'язку*. 2017. № 1. С. 38-42.

90. 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.

91. Scarfone K., Souppaya A., Cody A., Orebaugh M. 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.

92. Кібербезпека в боротьбі з банківськими шахрайствами: захист споживачів фінансових послуг та зростання фінансово-економічної безпеки України : звіт про НДР (проміжний) / кер. О. В. Кузьменко. Суми : СумДУ, 2019. 116 с.

93. 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.

94. 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.

95. Криклій О. А., Павленко Л. Д. Вплив кібербезпеки на стабільність фінансового сектору. *Сталий розвиток соціально-економічних систем* : матеріали III Всеукр. наук.-практ. конф., м. Київ, 14 трав. 2019 р. Київ : ТОВ «ВІПО», 2019. С. 129-132

96. Криклій О. А. Сутність та особливості кібершахрайств у фінансовій сфері як об'єктів статистичного дослідження. *Нові джерела та методи поширення даних у статистиці* : матеріали XVII Міжнар. наук.-практ. конф., Київ : «Інформаційно-аналітичне агентство», 2019. С. 166-170.

97. Report to the nations on occupational fraud and abuse. Association of Certified Fraud Examiners (ACFE). 2018. URL: https://s3-us-west-2.amazonaws.com/acfepublic/2018-report-to-the-nations.pdf. (дата звернення 18.12.2020)

98. Спритність рук: топ-схеми шахрайства в банках. *Financial club : веб-сайт*. URL: https://finclub.net/ua/priama-mova/sprytnist-ruk-topskhemy-shakhraistva-v-bankakh. (дата звернення 18.12.2020)

99. KPMG. Global banking fraud survey. URL: https://assets.kpmg/content/dam/kpmg/xx/pdf/2019/05/global-banking-fraud-survey.pdf. (дата звернення 18.12.2020)

100. Мельник С. С. Сутність фінансового шахрайства в комерційному банку. *Науковий вісник Ужгородського національного університету. Серія «Міжнародні економічні відносини та світове господарство»*. 2016. № 6 (2). С. 91-95.

101. Рац О. М. Дослідження особливостей організації фрод-моніторингу в системі управління економічною безпекою банку. *Комунальне господарство міст*. 2016. № 127. С. 33-37.

102. 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.

103. Стандарт ISO/IEC 27001:2013. URL: https://intercert.com.ua/articles/posts/292-standart-iso-iec-27001-2013. (дата звернення 18.12.2020)

104. Monique Magalhaes. Cybersecurity assessments and audits: everything you need to know. URL: http://techgenix.com/cybersecurity-assessments-and-audits/. (дата звернення 18.12.2020)

105. 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.

106. Міжнародні стандарти професійної практики внутрішнього аудиту. URL: https://na.theiia.org/translations/PublicDocuments/IPPF-Standards-2017-Ukrainian.pdf. (дата звернення 18.12.2020)

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

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

109. 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 18.12.2020)

110. 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 18.12.2020)

111. Гутцайт Е. М. Аудит: концепция, проблемы, эффективность, стандарты. Москва : ЭЛИТ 2000, ЮНИТИ ДАНА. 2002. 416 с.

112. Jarrod West, Maumita Bhattacharya, Rafigul Islam Intelligent financial fraud detection practices: an investigation. *Proceedings of the international conference on security and privacy in communication networks*. 2014. № 153. P. 186-203. DOI: 10.1007/978-3-319-23802-9_16

113. Rinky D. Patel, Dheeraj Kumar Singh. Credit card fraud detection & prevention of fraud using genetic algorithm. *International journal of soft computing and engineering (IJSCE)*. 2013. № 2 (6). P. 292-294.

114. MohdAvesh Zubair Khan, JabirDaud Pathan, Ali Haider Ekbal Ahmed. Credit card fraud detection system using hidden Markov model and k-clustering. *International journal of advanced research in computer and communication engineering.* 2014. №3 (2). P. 5458-5461.

115. Balamurugan M., Mathiazhagan P. Credit card transaction fraud detection system using fuzzy logic and k-means algorithm. *International Journal of Innovative Research in Technology*. 2015. № 2 (3). P. 171-176.

116. Гриценко К. Г. Дослідження особливостей незалежного аудиту для попередження шахрайства банківського персоналу. *Інфраструктура ринку*.

2019. № 37. URL: http://www.market-infr.od.ua/uk/37-2019. (дата звернення 18.12.2020)

117. Гриценко К. Г. Аналіз методів виявлення шахрайств у банках, що здійснюються персоналом банку. *Інфраструктура ринку*. 2019. № 34. С. 333-337. URL: http://www.market-infr.od.ua/uk/34-2019. (дата звернення 18.12.2020)

118. Небава М. І., Міронова Ю. В. Економічна безпека підприємства : навч. посіб. Вінниця : ВНТУ, 2017. 73 с. URL: https://web.posibnyky.vntu.edu.ua/fmib/33nebava_ekonomichna_bezpeka_pidpriyemstva/ekon_bezp_Nebava.pdf. (дата звернення 18.12.2020)

119. Корелин В. В., Габуниа Н. Г. Инструменты обеспечения экономической безопасности промышленного предприятия. *Известия Санкт-Петербургского государственного экономического университета CyberLeninka.* Санкт-Петербург : ФГБОУ ВО СПбГЭУ. 2016. №4 (100). С.114-116.

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

121. Мандзіновська Х. О. Економічна безпека держави: сутність, складові елементи та проблеми забезпечення: наукові записки. 2016. № 2 (53). С.159-166.

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

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

124. Кавун С. В., Пилипенко А. А., Репко Д. О. Економічна та інформаційна безпека підприємств у системі консолідації інформації : навч. посіб. Харків : ХНЕУ, 2013. 264 с.

125. Прокопішина О. В. Управління економічною безпекою зовнішньоекономічної діяльності підприємства: автореф. дис. … канд. екон. наук : 08.00.04 / Харківський національний економічний ун-т . Харків, 2009. 20 с

126. Василишин Т. С. Фінансова безпека: сутність і місце в системі економічної безпеки держави. *Соціально-економічний розвиток і безпека України: стан та перспективи :* матеріали міжвуз. наук.-практ. конф. здобувачів вищої освіти і молодих вчених, м. Львів, 19 квіт. 2018 р. / за заг. ред. Я.Я. Пушака. Львів: Ліга-Прес, 2018. С.53-55.

127. Новак О. С., Дідківська Н. І. Роль фінансового моніторингу у забезпеченні фінансової безпеки держави. *Ефективна економіка.* 2016. № 12. URL: http://www.economy.nayka.com.ua/?op=1&z=5511. (дата звернення 18.12.2020)

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

129. Куришко О.О. Національна система фінансового моніторингу в Україні : дис. ... канд. екон. наук : спец 08. 00. 08 - гроші, фінанси і кредит / О.О. Куришко; ДВНЗ "Укр. акад. банк. справи Нац. банку України". Суми, 2013. 262 с.

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

131. Зеленецький В. С., Кротюк В. Л., Файєр Д. А. Боротьба з легалізацією (відмиванням) доходів, одержаних злочинним шляхом, та фінансуванням тероризму (економікоправовий аналіз) : наук.-практ. посіб. Харків : Кросроуд, 2007. 668 с.

132. Протидія легалізації злочинних доходів і фінансуванню тероризму / С. Г. Гуржій, С. М. Клюшке, В. М. Кірсанов та ін. Київ : Такі справи, 2008. 560 с.

133. Schneider F. The (Hidden) Financial Flows of Terrorist and Organized Crime Organizations: A Literature Review and Some Preliminary Empirical Results.

IZA Institute of Labor Economics. 2010. №4860. URL: http://ftp.iza.org/dp4860.pdf. (дата звернення 18.12.2020)

134. Небава М. І. Інституціоналізація тіньової економічної діяльності як загроза економічній безпеці України. *Тіньова економіка: генезис, джерела розвитку, перспективи подолання та цивілізаційної інтеграції* : матеріали І Міжнар. наук.-практ. конфер., м. Вінниця, 23-24трав. 2013 р. Вінниця: НВЦ «Генеза», 2013. С. 139-143.

135. 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.

136. OECD science, technology, and industry scoreboard: Towards a knowledge-based economy. Organisation for Economic Cooperation and Development : website. 2001. URL: http://www.oecd.org/. (дата звернення 18.12.2020)

137. Babenko V., Syniavska O. Analysis of the current state of development of electronic commerce market in Ukraine. *Technology Audit and Production Reserves.* 2018. № 5. P. 40-45.

138. Mia A., Rahman M., Uddin M. E-Banking: Evolution, Status and Prospects. *Cost & Management*. 2007. № 1(35). P. 36-48.

139. The Statistical Portal. 2019. URL: https://www.statista.com/. (дата звернення 18.12.2020)

140. Lastdrager E. Achieving a consensual definition of phishing based on a systematic review of the literature. *Crime Science*. 2014. № 3 (9).

141. Jakobsson M., Myers S. Phishing and countermeasures: understanding the increasing problem of electronic identity theft. *John Wiley & Sons, Inc.*. 2007. 736 p.

142. Shi J., Saleem S. Phishing: Final Report. 2012. URL: https://www2.cs.arizona.edu/~collberg/Teaching/466-566/2014/Resources/presentations/2012/topic5-final/report.pdf. (дата звернення 18.12.2020)

143. Swanink R. Persistent effects of manin-the-middle attacks. Bachelor Thesis, Radboud University. 2016.

144. Damodaram R. Study on phishing attacks and antiphishing tools. International Research Journal of Engineering and Technology (IRJET). 2016. № 3(1). P. 700-705.

145. Alsayed A., Bilgrami A. E-banking security: Internet hacking, phishing attacks, analysis and prevention of fraudulent activities. *International Journal of Emerging Technology and Advanced Engineering.* 2017. № 7(1). P. 109-115.

146. Delgado O., Fuster-Sabater A., Sierra J. Analysis of new threats to online banking authentication schemes. *Universidad de Salamanca.* 2008. P. 337-344 URL: https://core.ac.uk/download/pdf/36021441.pdf. (дата звернення 18.12.2020)

147. Oliinyk V., Wiebe I., Syniavska O., Yatsenko V. Optimization model of Bass. *JAES*. 2018. № 8(62). P. 2168–2183.

148. Gupta R. Dynamics of a Holling-Tanner Model. *AJER*. 2017. № 6(4). P. 132-140.

149. Syniavska O., Dekhtyar N., Deyneka O., Zhukova T., Syniavska O. Security of e-banking systems: modelling the process of counteracting e-banking fraud. *CEUR Workshop Proceedings*. 2019. № 2422. P. 100-110. URL: http://ceur-ws.org/Vol-2422/paper08.pdf. (дата звернення 18.12.2020)

150. A-Z of internal banking fraud. URL: https://netguardians.ch/internal-banking-fraud/. (дата звернення 18.12.2020)

151. 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*. 2010. № 2 (3). P. 95-140.

152. 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 18.12.2020)

153. Пономаренко В.С., Малярець Л.М. Багатовимірний аналіз соціально-економічних систем : навч. посіб. Харків : ХНЕУ, 2009. 384 с.

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

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

156. 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. (дата звернення 18.12.2020)

157. Гриценко К.Г. Нечітко-множинний метод оцінювання рівня ризику шахрайства банківського персоналу. *Приазовський економічний вісник*. 2019. № 3(14). С. 451-456. URL: http://pev.kpu.zp.ua/vypusk-14. (дата звернення 18.12.2020)

158. Гриценко К.Г. Нечітко-множинна ієрархічна модель оцінювання рівня ризику шахрайства банківського персоналу. *Проблеми та перспективи розвитку фінансово-кредитної системи України* : зб. матеріалів IV Всеукр. наук.-практ. on-line конф., м. Суми, 21-22 лист. 2019 р. Суми : ННІ БТ «УАБС» СумДУ, 2019. С. 151-155.

159. Lyeonov S., Kuzmenko O., Yarovenko H., Dotsenko T. The Innovative Approach to Increasing Cybersecurity of Transactions Through Counteraction to Money Laundering. *Marketing and Management of Innovations.* 2019. № 3. P. 308-326. DOI: 10.21272/mmi.2019.3-24.

160. World Bank Open Data. URL: https://data.worldbank.org. (дата звернення 18.12.2020)

161. Organisation for Economic Co-operation and Development. URL: https://data.oecd.org/?_ga=2.69359696.157983792.1546455347-1152323357.1544691649. (дата звернення 18.12.2020)

162. Transparency International. URL: https://www.transparency.org/news/feature/corruption_perceptions_index_2017?gclid=EAIaIQobChMIusejy-PP3wIVVIuyCh0NdwBEEAAYASAAEgIyc_D_BwE. (дата звернення 18.12.2020)

163. Institute for economics & peace. URL: http://visionofhumanity.org/app/uploads/2017/11/Global-Terrorism-Index-2017.pdf. (дата звернення 18.12.2020)

164. Happy Planet Index. URL: http://happyplanetindex.org. (дата звернення 18.12.2020)

165. Pham D.T., Packianather M.S., Afify A.A. Artificial Neural Networks. *Computational Intelligence*. 2007. DOI: 10.1007/0-387-37452-3_3.

166. Michael J. D. Powell, Michael J. D. Powell. Restart procedures for the conjugate gradient method. *Mathematical Programming*. 1977. № 12. P. 241-254. DOI: 10.1007/bf01593790.

167. Broomhead David H., Lowe David. Multivariable Functional Interpolation and Adaptive Networks. *Complex Systems*. 1988. № 2. P. 321-355.

168. Метод Бройдена–Флетчера–Гольдфарба–Шанно. URL: https://math.semestr.ru/optim/broyden.php. (дата звернення 18.12.2020)

169. Кузьменко О. В. , Яровенко Г. М., Бойко А. О., Миненко С. В. Інформаційна система фінансового моніторингу: особливості розробки та реалізації в сучасних умовах протидії легалізації кримінальних доходів : монографія / за заг. ред. О. В. Кузьменко. Суми : Ярославна, 2019. С. 7-70.

170. Kuzmenko O., Boiko A., Yarovenko H., Dotsenko T. Data mining-based assesselement of the risk of using financial intermediaries for money laundering. *Ефективна економіка*. 2019. № 10. P. 1-13.

171. 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. (Edinburgh, October 25, 2019). UK : European Scientific Platform. P.29-31.

172. 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» (Ottawa, December 16-18, 2019). Canada : Methuen Publishing House, 2019. P. 73-75.

173. The State Financial Monitoring Service. URL: http://www.sdfm.gov.ua/index.php?lang=en. (дата звернення 18.12.2020)

174. About the business process model and notation specification version 2.0. Object Management Group Business Process Model and Notation : website. 2011. URL: https://www.omg.org/spec/BPMN/2.0/. (дата звернення 18.12.2020)

175. Bizagi Studio – the most business-friendly and flexible process automation software. Bizagi : website. URL: https://www.bizagi.com/en/products/bpm-suite/studio. (дата звернення 18.12.2020)

176. BPM Microsystems company. URL: https://bpmmicro.com/support/software/downloads/. (дата звернення 18.12.2020)

177. Leonov S., Yarovenko H., Boiko A., Dotsenko T. Information system for monitoring banking transactions related to money laundering. *CEUR Workshop Proceedings.* 2019. № 2422. P. 297-307.

178. 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).* 2019. № 65. DOI: 10.1051/shsconf/20196504013.

179. 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* : зб. тез доп. міжнар. наук.-практ. конф. (м. Полтава, 20 квіт. 2019 р.). Полтава : ЦФЕНД, 2019. С. 55-57.

180. Rikk R. National Cyber Security Index 2018. *E-governance Academy* : веб-сайт. URL: https://ega.ee/wp-content/uploads/2018/05/ncsi_digital_smaller.pdf. (дата звернення 18.12.2020)

181. National Cyber Security Index. *NCSI* : веб-сайт. URL: https://ncsi.ega.ee/ncsi-index/. (дата звернення 18.12.2020)

182. Халафян А. А. STATISTICA 6. Статистический анализ данных : учебн. пособ. Москва : ООО «Бином-Пресс», 2007. 512 с.

183. World Development Indicators. *The World Bank* : веб-сайт. URL: https://databank.worldbank.org/source/world-development-indicators/Type/TABLE/preview/on. (дата звернення 18.12.2020)

184. Яровенко Г.М. Канонічний аналіз взаємозв'язку інформаційної безпеки та соціо-економіко-політичного розвитку країни. *Науковий вісник УжНУ. Серія: Міжнародні економічні відносини та світове господарство*. 2020. № 31. С. 160-167. DOI: 10.32782/2413-9971/2020-31-26.

185. Yarovenko H. Research of relationship between information security and country development factors. *Theoretical and empirical scientific research: concept and trends: Collection of scientific papers «ΛΌГОΣ» with Proceedings of the International Scientific and Practical Conference* (Vol. 1), July 24, 2020. Oxford, United Kingdom: Oxford Sciences Ltd. & European Scientific Platform. с. 37-38.

186. Теорія та практика забезпечення розвитку кіберпростору країни : Монографія / О. В. Кузьменко, Г. М. Яровенко, О. А. Криклій, К. Г. Гриценко та ін.; за заг. ред. О. В. Кузьменко, Г. М. Яровенко. Суми : ФОП Ширяєв, 2020. 200 с.

187. National Cyber Security Index. *NCSI* : веб-сайт. URL: https://ncsi.ega.ee/ncsi-index/. (дата звернення 18.12.2020)

188. World Development Indicators. *The World Bank* : веб-сайт. URL: https://databank.worldbank.org/source/world-development-indicators/Type/TABLE/preview/on. (дата звернення 18.12.2020)

189. Kohonen, T. Self-Organized Formation of Topologically Correct Feature Maps. *Biological Cybernetics.* 1982. № 43(1). P. 59-69.

190. Яровенко Г.М. Використання карт Кохонена для аналізу рівня інформаційної безпеки країн з урахуванням їх розвитку. *Економічний простір*. 2020. № 157. С. 118-124. DOI: 10.32782/2224-6282/157-21.

191. Akram S. M., Al-Kenani A. N., Alcantud J.C.R. Group Decision-Making Based on the VIKOR Method with Trapezoidal Bipolar Fuzzy Information. *Symmetry*. 2019. № 11. P. 1-21. DOI: 10.3390/sym11101313.

192. Ghaleb A. M., Kaid H., Alsamhan A., Mian S. H., Hidri, L. Assessment and Comparison of Various MCDM Approaches in the Selection of Manufacturing Process. *Advances in Materials Science and Engineering.* 2020. P. 1-16. DOI: 10.1155/2020/4039253.

193. Mardani A., Zavadskas E.K., Govindan K., Amat Senin A., Jusoh A.VIKOR technique: A systematic review of the state of the art literature on methodologies and applications. *Sustainability.* 2016. №8(1). P. 1-38. DOI: 10.3390/su8010037.

194. Suniantara I. K. P., Putra I. G. E. W. Comparison of VIKOR and TOPSIS Methods in Multiresponse Taguchi Optimization. *Journal of Education Research and Evaluation*. 2019. № 2(3). P. 106-113. URL: https://ejournal.undiksha.ac.id/index.php/JERE. (дата звернення 18.12.2020)

195. Chatterjeea P., Chakraborty S. A comparative analysis of VIKOR method and its variants. *Decision Science Letters.* 2016. № 5. P. 469–486. DOI: 10.5267/j.dsl.2016.5.004.

196. e-Governance Academy Foundation. National Cyber Security Index. URL: https://ncsi.ega.ee/ncsi-index/. (дата звернення 18.12.2020)

197. Hwang C.L., Yoon K. Multiple Attribute Decision Making: Methods and Applications. 1981. New York: Springer-Verlag. DOI: 10.1007/978-3-642-48318-9.

198. Opricovic S. T. G.-H. The Compromise solution by MCDM methods: A comparative analysis of VIKOR and TOPSIS. *European Journal of Operational Research*. 2004. № 156(2). P. 445–455.

199. Miller K.E. A Situational Multi-Attribute Attitude Model. *Advances in Consumer Research*. 1975. № 2. P. 455-464.

200. Yarovenko H., Kuzmenko O., Stumpo M. Strategy for Determining Country Ranking by Level of Cybersecurity. *Financial Markets, Institutions and Risks*. 2020. 4(3). P. 124-137. DOI: 10.21272/fmir.4(3).124-137.2020.

201. Ковальчук А. Запобігання та протидія відмиванню тіньових фінансів: подолання викликів та загроз. *Публічне право*. 2015. № 4. С. 122-128.

202. Івченко І. Ю. Моделювання економічних ризиків і ризикових ситуацій : навч. посіб. Київ : ЦУЛ, 2007. 344 с.

203. Смагло О. В. Удосконалення системи оцінювання ризиків легалізації злочинних доходів при здійсненні зовнішньоекономічної діяльності. *Проблеми теорії та методології бухгалтерського обліку, контролю і аналізу*. 2015. № 2 (32). С. 356-368.

204. Бунчук М. М. Проблеми страхування ризиків тероризму в процесі аналізу антитерористичної політики України. *Державне управління: теорія та практика*. 2016. № 1. URL: http://e-patp.academy.gov.ua/2016_1/4.pdf. (дата звернення 18.12.2020)

205. Глібчук В.М. Моделювання і оптимізація інвестиційних ризиків на підприємствах в умовах невизначеності. *Інститут менеджменту та економки «Галицька академія»*. 2010. № 1. С. 263-269.

206. Глущевський В.В. Методологічні основи концепції управління ризиками підприємницької діяльності. *Фінанси України*. 2009. № 10. С. 57-72.

207. Донець Л. І. Економічні ризики та методи їх вимірювання : навч. посіб. Київ : Центр навчальної літератури, 2006. 312 с.

208. Економічний ризик: методи оцінки та управління : навч. посіб. / за ред. Т. А. Васильєва, Я. М. Кривич. Суми : ДВНЗ "УАБС НБУ", 2015. 207 с.

209. Патюта І. М. Державне регулювання системи факторів оцінки та мінімізації ризиків легалізації коштів, одержаних злочинним шляхом в процесі фінансового моніторингу комерційних банків України. *Культура народов Причерноморья.* 2012. № 220. С. 77-81.

210. Худокормова М. І. Методика оцінювання ризику клієнта при використанні ним послуг банку для легалізації кримінальних доходів. *Актуальні проблеми економіки*. 2012. № 6(132). С. 283-289.

211. Журавель В. А. Розслідування легалізації (відмивання) доходів, одержаних злочинним шляхом. Настільна книга слідчого : наук.- практ. видання

для слідчих і дізнавачів / за ред. М. І. Панов, В. І. Шепітько, В. О. Коновалова. 2-ге вид., переробл. і допов. Київ : Вид. дім "Ін Юре", 2008. С. 322–335.

212. Ніколаюк С. І., Семчук А. Г. Проблеми оперативного забезпечення протидії легалізації коштів, здобутих злочинним шляхом. *Науковий вісник*. Київ : НАВСУ. 2003. № 4. С. 153–161.

213. Погорецький М. А. Особливості розслідування легалізації (відмивання) грошових коштів, отриманих злочинним шляхом, з використанням кредитно-банківської системи. Розслідування окремих видів злочинів : навч. посіб. / О. В, Бищовець, М. А. Погорецький, Д. Б. Сергєєва та ін. / за ред. М. А. Погорецького та Д. В. Сергєєвої. Київ : Алерта, 2015. С. 279–300.

214. Сухонос В.В. Легалізація злочинних доходів у банківській сфері та боротьба з нею. *Правовий вісник Української академії банківської справи*. 2014. № 1 (6). С. 149-153.

215. Phill Seib, Dana M. Janbek. Global Terrorism and New Media: The post-Al Qaeda generation. *London and New York*. 2011. 138 p.

216. Антипенко В. Ф. Міжнародна кримінологія: досвід дослідження тероризму : монографія. Одеса : Фенікс, 2011. 320 с.

217. Богуцький П. Тероризм як антиправова соціальна практика. *Право України*. 2015. № 9. С. 90-96.

218. Іващенко О. А. Економічні ефекти терористичних атак: наслідки для міжнародного бізнесу. *Наукові розробки, передові технології, інновації* : зб. наук. праць та тез наук. доп. за матеріалами III Міжнар. наук.-практ. конф. Київ : НДІСР. 2016. С. 210-213. URL: http://194.44.12.92:8080/jspui/bitstream/123456789/1721/1. (дата звернення 18.12.2020)

219. Підюков П. П., Устименко Т. П., Осипенко Р. І. Відповідальність за фінансування тероризму має передбачати невідворотнє відшкодування суб'єктом злочину завданих державі і його жертвам збитків. *Наше право*. 2015. № 3. С. 90-95. URL: http://www.irbis-nbuv.gov.ua/cgi bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21RE

F=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=Nashp_2015_3_16. (дата звернення 18.12.2020)

220. Тероризм: теоретико-прикладні аспекти : навч. посіб. / за заг. ред. В. К. Грищука. Львів : ЛьвДУВС, 2011. 328 с.

221. Бисага К. В. Правові та інституційні заходи протидії відмиванню доходів і фінансуванню тероризму у Словацькій республіці. *Інвестиції: практика та досвід*. 2016. № 3. URL: http://www.investplan.com.ua/pdf/3_2016/22.pdf. (дата звернення 18.12.2020)

222. Боротьба з відмиванням коштів: правовий, організаційний і практичний аспект / С.Г. Гуржій, О.Л. Копиленко, Я.В. Янушевич та ін. Київ : Парламентське вид., 2005. 216 с.

223. Ковальчук А., Криштоф А. Детінізація економіки як нормативно-правовий імператив. *Підприємництво, господарство, право*. 2016. №1. С.51-55. URL: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=Pgip_2016_1_9. (дата звернення 18.12.2020)

224. Правове регулювання відносин на фінансовому ринку: стан та напрями вдосконалення : монографія / за ред. В.Д. Чернадчук. Суми : ВВП "Мрія" ТОВ, 2015. 340 с.

225. Chen Y., Cook W.D., Li N., Zhu J. Additive Efficiency Decomposition in Two-stage DEA. *European Journal of Operational Research*. 2009. № 196. P. 1170-1176.

226. Hosseinzadeh Lotfi F., Toloie Eshlaghy A., Shafiee M., Salehl H., Nikoomaram H., Seyedhoseini S. M. A new two-stage data envelopment analysis (DEA) model for evaluating the branch performance of banks, *African Journal of Business Management*. 2012. № 6(24). P. 7230-7241.

227. An introduction to Frontier Analyst. Banxia Software : website. URL: https://translate.google.com.ua/translate?hl=ru&sl=en&u=http://banxia.com/pdf/fa/FAWorkbook1.pdf&prev=search. (дата звернення 18.12.2020)

228. Frontier Analyst. URL : http://technology.msb.edu/old/training/statistics/frontieranalyst. (дата звернення 18.12.2020)

229. Kuzmenko O., Dotsenko T. The shadow of National Economy: financial monitoring effectiveness of money laundering. Inclusive Growth: basics, indicators and development priorities: monograph / edited by T. Vasilyeva, S. Lyeonov. Publishing House: Centre of Sociological Research. 2020. P. 103-135.

230. Кузьменко О.В., Доценко Т.В. Моделювання ефективності фінансового моніторингу банків в розрізі оцінювання ризиків легалізації коштів, одержаних злочинним шляхом, фінансування тероризму та розповсюдження зброї масового знищення. *Інвестиції: практика та досвід.* 2017. №15. С.32-41.

231. Кузьменко О.В., Доценко Т.В. Фронтірний аналіз ефективності фінансового моніторингу банків в розрізі оцінювання ризиків легалізації коштів, одержаних злочинним шляхом. *Пріоритетні напрями досліджень в науковій та освітній діяльності: матеріали II Міжнародної науково-практичної конференції (м. Львів, 13-14 липня 2020 року).* Львів: Львівський науковий форум, 2020. С.8-10.

232. Кузьменко О.В., Бойко А.О., Доценко Т.В. Система фінансового моніторингу як запорука досягнення високого рівня економічної безпеки національної економіки. *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. 1. С.144-147.

233. Корнівська *В.О.* Цифровий банкінг: ризики фінансової дигіталізації. *Проблеми економіки*. 2017. № 3. С. 254-261.

234. Деякі питання об’єктів критичної інформаційної інфраструктури. Постанова Кабінету Міністрів України від 09.10.2020 № 942. URL: https://zakon.rada.gov.ua/laws/show/943-2020-%D0%BF. (дата звернення 18.12.2020)

235. The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study. Accenture : website. URL: https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf. (дата звернення 18.12.2020)

236. National Cyber Security in Practice. E-governance academy : website. URL: https://ega.ee/wp-content/uploads/2020/05/Kuberturvalisuse_kasiraamat_ENG.pdf. (дата звернення 18.12.2020)

237. The Financial Matrix: Bitglass' 2019 Financial Breach Report. Bitglass : website. URL: https://www.bitglass.com/blog/the-financial-matrix-bitglass-2019-financial-breach-report. (дата звернення 18.12.2020)

238. Operational Risk Horizon. ORX : website. URL: https://managingrisktogether.orx.org/sites/default/files/public/downloads/2020/09/orx operationalriskhorizonsummaryreport2020.pdf. (дата звернення 18.12.2020)

239. The Global Risks Report 2020. World Economic Forum : website. URL: http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf. (дата звернення 18.12.2020)

240. Держспецзв'язку створює експертну раду з кібербезпеки. URL: https://nv.ua/ukr/biz/tech/v-ukrajini-z-yavivsya-ekspertna-rada-z-kiberbezpeki-novini-ukrajini-50116214.html. (дата звернення 18.12.2020)

241. Dupont B. The cyber-resilience of financial institutions: significance and applicability. *Journal of Cybersecurity*. 2019. № 5(1). DOI: 10.1093/cybsec/tyz013

242. Домарєв В.В., Домарєв Д.В. Управління інформаційною безпекою в банківських установах (теорія і практика впровадження стандартів серії ISO 27k). Донецьк: Велстар, 2012. 146 с.

243. Framework for Improving Critical Infrastructure Cybersecurity. National Institute of Standards and Technology : website. URL: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf. (дата звернення 18.12.2020)

244. An endurance course: surviving and thriving through 10 major risks over the next decade: Tenth annual EY/IIF global bank risk management survey. URL: https://www.iif.com/Portals/0/Files/content/Regulatory/11062019_iif_ey_global_risk_survey_2019.pdf. (дата звернення 18.12.2020)

245. EPG. Analytics-based approach to cyber security. URL: http://docplayer.net/2410200-An-analytics-based-approach-to-cybersecurity.html (дата звернення 18.12.2020).

246. Бир С. Мозг фирмы. Москва: Радио и связь, 1993. 416 с.

247. Криклій О.А. Теорія та практика забезпечення кіберстійкості банків. *Ефективна економіка*. 2020. № 10. DOI: 10.32702/2307-2105-2020.10.50

248. SAS. Trends in combating cyber crime. Tips and technology for defending your network. URL: https://www.risktech-forum.com/research/sas-trends-in-combating-cybercrime-tips-and-techniques-for-defending-your-n. (дата звернення 18.12.2020)

249. Толюпа С.В., Іванова О.М., Демченко І.О. Підходи до проектування та оцінки ефективності системи захисту інформації в автоматизованих системах обробки та передачі даних. *Сучасний захист інформації*. 2013. № 1. С. 25-30.

250. Маслова Н.А. Методы оценки эффективности систем защиты информационных систем. *Штучний інтелект*. 2008. № 4. С. 253-264.

251. Гарасимчук О.І., Костів Ю.М. Оцінка ефективності систем захисту інформації. *Вісник КНУ імені Михайла Остроградського*. 2011. № 1 (1). С. 16-20.

252. Богданов В.В. Застосування критерію ризику для оцінки захищеності автоматизованої системи. *Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення* : зб. матеріалів V-ої наук.-тех. конф. (м. Київ, 20-21 жовт. 2010 р.). Київ : ВІТІ НТУУ “КПІ”. 2010. С. 70-72.

253. Барташевська Ю. М. Оцінка ефективності витрат компанії на інформаційну безпеку. *Науковий вісник Міжнародного гуманітарного університету*. *Серія «Економіка і менеджмент»*. 2017. № 28. С. 87-90.

254. Новожилова М.В., Овечко К.А. Оценка систем защиты информации в компьютерных информационных системах по критерию «эффективность-стоимость». *Системи обробки інформації*. 2004. № 1. С. 148-151.

255. Маковецький О.М., Мальцева І.Р., Паламарчук Н.А., Черниш Ю.О., Шемендюк О.В. Підходи до удосконалення методики оцінки ефективності комплексної системи захисту інформації. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2016. № 2 (26). С. 54-58.

256. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты. Киев : ТИД ДиаСофт, 2002. 688 с.

257. Куцаєв В.В., Радченко М.М., Козубцова Л.М., Терещенко Т.П. Методика оцінки кібернетичної захищеності інформаційно-телекомунікаційного вузла зв'язку. *Збірник наукових праць ВІТІ НТУУ "КПІ"*. 2018. № 2. С. 67-76.

258. Бешелев С.Д., Гурвич Ф.Г. Экспертные оценки. Москва : Наука, 1973. 263 с.

259. Ротштейн А.П. Интеллектуальние технологии идентификации: нечеткие множества, генетический алгоритм, нейронные сети. Винница : УНИВЕРСУМ, 1999. 320 с.

260. NIST SP 800-53 National Institute of Standards and Technology. Special Publication Security and Privacy Controls for Federal information Systems and Organizations. URL: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/draft. (дата звернення 18.12.2020)

261. DoD 8530.01. Department of Defense. Indicators. Defend the nation from attack. Secure national security and military systems. URL: http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/853001p.pdf. (дата звернення 18.12.2020)

262. Толюпа С.В., Борисов І.В. Методика оцінки комплексної системи захисту інформації на об'єкті інформаційної діяльності. *Сучасний захист інформації*. 2013. № 2. С. 43-48.

263. Тихонов Д.В. Модели оценки эффективности систем информационной безопасности : дисс. … канд. экон. наук : 08.00.05. Санкт-Петербург, 2009. 126 с.

264. Самохвалов Ю., Браиловский Н. Оценка информационной безопасности организации по критерию уверенности. *Захист інформації*. 2019. № 1. С. 13-24.

265. Михайлова Л. Анализ существующих методов оценки эффективности мер по защите информации. *Науковий вісник Одеського національного економічного університету*. 2015. № 5. С. 90-101.

266. Гриценко К.Г. Шляхи забезпечення стійкості фінансового кіберпростору. *Інфраструктура ринку*. 2020. Випуск 49. URL: http://www.market-infr.od.ua/uk/49-2020. (дата звернення 18.12.2020)

267. Гриценко К.Г. Шляхи підвищення ефективності забезпечення кібербезпеки банку. *Інфраструктура ринку*. 2020. Випуск 45. С. 274-279. URL: http://www.market-infr.od.ua/uk/45-2020. (дата звернення 18.12.2020)

268. Гриценко К.Г. Аналіз методів оцінки ефективності внутрішньобанківської системи кібербезпеки. *Інфраструктура ринку.* 2020. Випуск 41. С. 320-325. URL: http://www.market-infr.od.ua/uk/41-2020. (дата звернення 18.12.2020)

269. Гриценко К.Г. Актуальні напрями підвищення ефективності забезпечення кібербезпеки банку. *Проблеми та перспективи розвитку фінансово-кредитної системи України: збірник матеріалів V Всеукраїнської науково-практичної on-line конференції (19-20 листопада 2020 року)*. Суми : ННІ БТ «УАБС» СумДУ, 2020. С. 213-217.

270. The Global Risks Report 2020. World Economic Forum : website. 2020. URL:http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf. (дата звернення 18.12.2020)

271. Agrafiotis I. , Nurse J. R. C. , Goldsmith M. , Creese S. , Upton D. A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding

how they propagate. *Journal of Cybersecurity.* 2018. № 4(1). DOI: 10.1093/cybsec/. (дата звернення 18.12.2020)

272. Bouveret A. Cyber risk for the financial sector: A framework for quantitative assessment. *IMF Working Paper*. 2018. №18/143. P. 1-28. URL: https://www.imf.org/en/Publications/WP/Issues/2018/06/22/Cyber-Risk-for-the-Financial-Sector-A-Framework-for-Quantitative-Assessment-45924. (дата звернення 18.12.2020)

273. Шугунов Т., Жуков А., Хочуева Ф. Проблемы обеспечения киберустойчивости банковской системы Российской Федерации: правовой и методологический аспекты. Пробелы в российском законодательстве. 2019. № 6. С. 250-253.

274. Петренко С. Киберустойчивость индустрии 4.0. *The 2018 symposium on cybersecurity of the digital economy (CDE'18)* : II междунар. науч.-техн. конф. 2018. С. 370-381.

275. Дубина М., Середюк І., Білоус Н. Роль кіберстрахування в системі ризик-менеджменту банківських установ. П*роблеми і перспективи економіки та управління.* 2020. № 1 (21). С.183-196.

276. Gray A., Mee P. Large-scale cyber attacks on the Financial System. Oliver Wyman. URL: https://www.oliverwyman.com/content/dam/oliver-wyman/v2/publications/2018/march/Large-Scale-Cyber-Attacks-DTCC-2018.pdf. (дата звернення 18.12.2020)

277. Gracie A. Managing cyber risk – the global banking perspective. *British Bankers' Association Cyber Conference.* 2014. P. 1-5.

278. Богославський М. Ю. Дослідження ступеню протидії банківським кібератакам на світовому та вітчизняному рівнях. *Агросвіт*. 2018. № 2. С. 88-92.

279. Гладких Д. М. Банківська безпека держави в умовах розвитку інформаційної економіки (трансформації банківських операцій) : монографія. Київ : НУОУ, 2019. 393 с.

280. Cyber resilience oversight expectations for financial market infrastructures. European Central Bank : website. 2018. URL:

https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf. (дата звернення 18.12.2020)

281. Guidance on cyber resilience for financial market infrastructures, CPMI-IOSCO. Committee on Payments and Market Infrastructures Board of the International Organization of Securities Commissions : website. 2016. URL: https://www.bis.org/cpmi/publ/d146.pdf. (дата звернення 18.12.2020)

282. Bodeau D., Graubart R. Cyber Resiliency Design Principles. Mitre technical report : website. 2017. 98 p. URL: https://www.mitre.org/sites/default/files/publications/PR%2017-0103%20Cyber%20Resiliency%20Design%20Principles%20MTR17001.pdf. (дата звернення 18.12.2020)

283. Cyber resilience: Health check. Australian Securities and Investments Commission : website. 2015. URL: https://download.asic.gov.au/media/3062900/rep429-published-19-march-2015-1.pdf. (дата звернення 18.12.2020)

284. Cyber Lexicon. Financial Stability Board : website. 2018. URL: https://www.fsb.org/wp-content/uploads/P121118-1.pdf. (дата звернення 18.12.2020)

285. Collins R., O'Connor-Close C., Zhang A. Cyber incident cost estimates and the importance of building resilience. *The Reserve Bank of New Zealand*. 2020. № 84(2). URL: https://www.rbnz.govt.nz/research-and-publications/reserve-bank-bulletin/2020/rbb2020-84-. (дата звернення 18.12.2020)

286. Комітет «Кіберстійкості бізнесу». URL: https://corporatesecurity.org.ua/uk-UA/Novyny/Vidbulos-zasidannya-komitetu-Kiberstijkosti-biznesu.aspx?ID=272. (дата звернення 18.12.2020)

287. NIST Special Publication, Systems Security Engineering: Cyber Resiliency Considerations for the Engineering of Trustworthy Secure Systems. *NIST* : website. URL: https://www.tenable.com/whitepapers/adhering-to-the-nist-framework-with-tenable-ot?utm_campaign=00019887&utm_promoter=tenable-enterprise-comp-

00019887&utm_source=google&utm_medium=cpc&utmgeo=emea &gclid =CjwKCAjww5r8BRB6EiwArcckC3rzHgkmtvFh4oj-fRYHlBtX0ZAB-0z0uZK4NGFvER8qlpE-iJFkzRoCaIQQAvD_. (дата звернення 18.12.2020)

288. Колосок И. Н., Гурина Л. А. Оценка рисков кибербезопасности информационно-коммуникационной инфраструктуры интеллектуальной энергетической системы. *Информационные и математические технологии в науке и управлении*. 2019. № 2(14). URL: https://cyberleninka.ru/article/n/otsenka-riskov-kiberbezopasnosti-informatsionno-kommunikatsionnoy-infrastruktury-intellektualnoy-energeticheskoy-sistemy. (дата звернення 18.12.2020)

289. Cyber-resilience: Range of practices. Basel Committee on Banking Supervision : website. 2018. URL: https://www.bis.org/bcbs/publ/d454.pdf. (дата звернення 18.12.2020)

290. Financial Sector's Cybersecurity: A Regulatory Digest. The World Bank Group : website. 2017. URL: http://pubdocs.worldbank.org/en/524901513362019919/FinSAC-CybersecDigestOct-2017-Dec2017.pdf. (дата звернення 18.12.2020)

291. Almansi A. A. Financial sector's cybersecurity: regulations and supervision. *FCI Insight Washington, D.C. World Bank Group.* 2018. 38 P.

292. World Bank adopts ECB's cyber resilience oversight expectations. European Central Bank : website. 2020. URL: https://www.ecb.europa.eu/paym/intro/news/html/ecb.mipnews200106.en.html. (дата звернення 18.12.2020)

293. TIBER-EU FRAMEWORK How to implement the European framework for Threat Intelligence-based Ethical Red Teaming. European Central Bank : website. 2018. URL: https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf. (дата звернення 18.12.2020)

294. Fundamental Elements of Cybersecurity for the Financial Sector. 2016. URL:

https://www.mof.go.jp/english/international_policy/convention/g7/g7_161011_1.pdf. (дата звернення 18.12.2020)

295. Криклій О.А. Актуальні питання підвищення кіберстійкості банків. *Глобальні тенденції в економіці, фінансах та управлінні* : тези доп. міжнар. наук.-практ. конф. (м. Одеса, 2 жовт. 2020 р.). Одеса : Східноєвропейський центр наукових досліджень, 2020. С. 61-63.

296. Michael A. Rigdon, Franz R. Epting, Robert A. Neimeyer, Seth R. Krieger. The threat index: A research report, Death Education. 1979. № 3. P. 245-270.

297. Paul J. Robinson, Keith Wood. The Threat Index: An Additive Approach. *Omega*. 1985. № 15(2). P. 139-144.

298. Seth Hardy, Masashi Crete-Nishihata, Katharine Kleemola, Adam Senft, Byron Sonne, and Greg Wiseman, Phillipa Gill, Ronald J. Deibert. Targeted Threat Index: Characterizing and Quantifying Politically-Motivated Targeted Malware. *USENIX Security Symposium*. 2014. № 23. P. 527-541.

299. Oakleaf J. R., Kennedy C. M., Baruch-Mordo S., West P. C., Gerber J. S., Jarvis L., Kiesecker J. Development Threat Index. Palisades. *Socioeconomic Data and Applications Center (SEDAC).* 2019. №1 DOI: 10.7927/61jv-th84.

300. Мартинюк В. П. Оцінка стану національної економіки на основі інтегрального показника економічної безпеки держави. *Економіка, менеджмент, підприємництво*. 2013. № 25 (1). С. 179-188.

301. Berglund A., Guidolin M., Pedio M. Monetary policy after the crisis: A threattohedge funds'alphas? *Journal of Asset Management.* 2020. № 21(3). P. 219-238.

302. Bukhtiarova A., Semenog A., Razinkova M., Nebaba N., Haber J.A. Assessment of financial monitoring efficiency in the banking system of Ukraine. *Banks and Bank Systems.* 2020. № 15(1). P. 98-106.

303. Hkilchenko N.V., Atamanova E.A., Slavikovskaya Y.O. Diagnostics of environmental and social threatstothe territory's development. *Economy of Region.* 2020. № 16(1). P. 43-58.

304. Бесчастний А. В. Економічна безпека України у контексті світової економічної кризи. *Економіка і держава*. 2009. №15. С. 67-69.

305. Гбур З.В. Актуальні гібридні загрози економічній безпеці України. *Інвестиції:практика та досвід*. 2018. № 7. С. 97-99.

306. Макарчук І.М. Оцінка сучасного стану та актуальні загрози економічній безпеці в Україні. *Економічний аналіз*. 2015. № 21(1). С. 83-89.

307. Варналій З. С., Буркальцева Д. Д., Наєнко О. С. Економічна безпека України: проблеми та пріоритети зміцнення : монографія. Київ, 2011. 299 с.

308. Акімова Л.М. Сутнісна характеристика основних загроз в економічній безпеці держави. *Державне управління: удосконалення та розвиток*. 2016. № 10.

309. Комеліна О.В., Онищенко С. В., Матковський А. В. Економічна безпека держави: оцінювання та стратегічні орієнтири забезпечення : монографія. Полтава : ПолтНТУ, 2013. 202 с.

310. Мамалуй О. О. Про пріоритетні напрями забезпечення економічної безпеки держави. *Вісник Національної юридичної академії України імені Ярослава Мудрого.* Харків : Вид-во НЮА України ім. Я. Мудрого, 2011. №4. С. 18-28.

311. Петрушевська, В. В. Економічна безпека держави: зміст і класифікація загроз. *Ефективність державного управління*. 2012. № 32. С. 441-448.

312. Третяк В.В. Економічна безпека : сутність та умови формування. *Економіка і держава*. 2010. №1. С. 6-8.

313. Henderson D. J., Parmeter C. F. Applied Nonparametric Econometrics. *Cambridge University Press*. 2015. DOI: 10.1017/CBO9780511845765.

314. Luong Ha Nguyen, Ianis Gaudot, Shervin Khazaeli, James-A. Goulet A Kernel-Based Method for Modeling Non-harmonic Periodic Phenomena in Bayesian Dynamic Linear Models. *Frontiers in Built Environment.* 2019. № 5. DOI: 10.3389/fbuil.2019.00008.

315. Duvenaud D. Automatic Model Construction With Gaussian Processes. *University of Cambridge*. 2014. DOI: 10.17863/CAM.14087.

316. Яровенко Г.М., Доценко Т.В., Кушнерьов О.С. Моделювання інтегрального індексу загрози національної економіки на основі функції Кернела. *Теоретико-практичні аспекти аналізу економіки, обліку, фінансів і права: збірник тез доповідей Міжнародної науково-практичній конференції (Полтава, 18 червня 2020 р.)*. Полтава: ЦФЕНД, 2020, ч.1. С. 60-62.

317. 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.

318. Кузьменко О.В., Бойко А.О., Яровенко Г.М., Доценко Т.В. Сценарії реформування національної системи фінансового моніторингу. *Економіка і держава*. 2020. №1. С. 9-15.

319. Яровенко Г.М., Доценко Т.В., Кушнерьов О.С. Формування інтегрального індексу загрози національної економіки. *Вісник СумДУ. Серія Економіка*. 2020. №2. С.16-28.

320. Геєць В. М., Кизим М. О., Клебанова Т. С., Черняк Т. С. Моделювання економічної безпеки: держава, регіон, підприємство : монографія Харків : ВД "ИНЖЭК", 2006. 240 с.

321. Каламбет С. В., Кириленко Б. О. Економічна безпека як багаторівнева система. *Економіка і суспільство*. 2016. № 5. С. 344-349.

322. Пономаренко В. С., Кавун С. В. Концептуальні основи економічної безпеки : монографія. Харків : Видавництво ХНЕУ, 2008. 256 с.

323. Акімова Л. М. Теоретичні основи державного управління розвитком національної безпеки. *Державне управління: удосконалення та розвиток*. 2015. № 5.

324. Майстро С.В. Напрями удосконалення механізму державного управління фінансово-економічною безпекою України в сучасних умовах. *Актуальні проблеми державного управління*. 2015. №1(46). С. 210–218.

325. Матвійчук І.О. Інституціоналізація управління економічною безпекою держави. *Вісник Академії митної служби України. Серія: Економіка*. 2012. № 2. С. 131-141.

326. Плакіда А. О. Реалізація державної політики у сфері економічної безпеки національної економіки : автореф. дис. … канд. наук з держ. упр. : 25.00.02 – механізми державного управління. Запоріжжя, 2008. 20 с.

327. Сороківська О. А. Інноваційні напрями підвищення економічної безпеки підприємств малого бізнесу в умовах конфліктних ситуацій : дис. … докт. екон. наук : 08.00.04 / Тернопільський національний технічний університет імені Івана Пулюя. Тернопіль, 2016. 488 с.

328. Ткачова Н. М. Механізм державного регулювання економічної безпеки регіону : автореф. дис. … докт. наук з держ. упр. : спец. 25.00.02 – механізми державного управління. Запоріжжя, 2009. 40 с.

329. КузьменкоО.В., ДоценкоТ.В. Удосконалення системи державного регулювання економічної безпеки національної економіки. *"БІЗНЕС-ІНФОРМ"*. 2020. №7 (510). С.36-43.

330. КузьменкоО.В, ДоценкоТ.В. Ігромоделювання стратегій державного регулювання економічної безпеки національної економіки. *Економіка в контексті глобальних змін суспільства: матеріали Міжнародної науково-практичної конференції (м. Дніпро, 18 липня 2020 р.)*. Дніпро: НО «Перспектива», 2020. С.135-138.

ДОДАТКИ

Додаток А

Інформаційне забезпечення системи

Лістинг А.1 – Створення бази даних, ключових таблиць та зв’язків між ними

```
CREATE DATABASE ip2;
CREATE TABLE `cards` (
  `cardID` varchar(16) COLLATE utf8_bin NOT NULL,
  `clientID` int(11) NOT NULL
) ENGINE=InnoDB DEFAULT CHARSET=utf8 COLLATE=utf8_bin;
CREATE TABLE `clients` (
  `clientID` int(11) NOT NULL,
  `fname` varchar(100) COLLATE utf8_bin NOT NULL,
  `sname` varchar(100) COLLATE utf8_bin NOT NULL,
  `patronymic` varchar(100) COLLATE utf8_bin NOT NULL,
  `telephone` varchar(12) COLLATE utf8_bin NOT NULL
) ENGINE=InnoDB DEFAULT CHARSET=utf8 COLLATE=utf8_bin;
CREATE TABLE `frauds` (
  `fraudID` int(11) NOT NULL,
  `transactionID` int(11) NOT NULL,
  `code` int(11) NOT NULL,
  `reason` varchar(128) COLLATE utf8_bin NOT NULL
) ENGINE=InnoDB DEFAULT CHARSET=utf8 COLLATE=utf8_bin;
CREATE TABLE `location` (
  `ip_from` int(10) UNSIGNED DEFAULT NULL,
  `ip_to` int(10) UNSIGNED DEFAULT NULL,
  `country_code` char(2) COLLATE utf8_bin DEFAULT NULL,
  `country_name` varchar(64) COLLATE utf8_bin DEFAULT NULL,
  `region_name` varchar(128) COLLATE utf8_bin DEFAULT NULL,
  `city_name` varchar(128) COLLATE utf8_bin DEFAULT NULL,
  `latitude` double DEFAULT NULL,
  `longitude` double DEFAULT NULL,
  `zip_code` varchar(30) COLLATE utf8_bin DEFAULT NULL
) ENGINE=MyISAM DEFAULT CHARSET=utf8 COLLATE=utf8_bin;
CREATE TABLE `location_ua` (
  `ip_from` int(10) UNSIGNED DEFAULT NULL,
  `ip_to` int(10) UNSIGNED DEFAULT NULL,
  `region_name` varchar(128) COLLATE utf8_bin DEFAULT NULL,
  `city_name` varchar(128) COLLATE utf8_bin DEFAULT NULL,
  `latitude` double DEFAULT NULL,
  `longitude` double DEFAULT NULL
) ENGINE=MyISAM DEFAULT CHARSET=utf8 COLLATE=utf8_bin;
CREATE TABLE `transactions` (
  `transactionID` int(11) NOT NULL,
  `cardID` varchar(16) COLLATE utf8_bin NOT NULL,
  `time` datetime NOT NULL DEFAULT CURRENT_TIMESTAMP,
  `region` varchar(128) COLLATE utf8_bin NOT NULL,
  `ort` varchar(128) COLLATE utf8_bin NOT NULL,
  `ip` int(10) UNSIGNED NOT NULL,
  `fraud` tinyint(1) NOT NULL DEFAULT ‘0’
```

```
) ENGINE=InnoDB DEFAULT CHARSET=utf8 COLLATE=utf8_bin;
ALTER TABLE `cards`
  ADD PRIMARY KEY (`cardID`),
  ADD KEY `userID` (`clientID`);
ALTER TABLE `clients`
  ADD PRIMARY KEY (`clientID`);
ALTER TABLE `frauds`
  ADD PRIMARY KEY (`fraudID`),
  ADD KEY `transactionID` (`transactionID`);
ALTER TABLE `location`
  ADD KEY `idx_ip_from` (`ip_from`),
  ADD KEY `idx_ip_to` (`ip_to`),
  ADD KEY `idx_ip_from_to` (`ip_from`,`ip_to`);
ALTER TABLE `location_ua`
  ADD KEY `idx_ip_from` (`ip_from`),
  ADD KEY `idx_ip_to` (`ip_to`),
  ADD KEY `idx_ip_from_to` (`ip_from`,`ip_to`);
ALTER TABLE `transactions`
  ADD PRIMARY KEY (`transactionID`),
  ADD KEY `cardID` (`cardID`);
ALTER TABLE `clients`
  MODIFY `clientID` int(11) NOT NULL AUTO_INCREMENT,
AUTO_INCREMENT=3;
ALTER TABLE `frauds`
  MODIFY `fraudID` int(11) NOT NULL AUTO_INCREMENT,
AUTO_INCREMENT=7;
ALTER TABLE `transactions`
  MODIFY `transactionID` int(11) NOT NULL AUTO_INCREMENT,
AUTO_INCREMENT=11;
ALTER TABLE `cards`
  ADD CONSTRAINT `cards_cl ` FOREIGN KEY (`clientID`) REFERENCES
`clients` (`clientID`) ON DELETE CASCADE ON UPDATE CASCADE;
ALTER TABLE `frauds`
  ADD CONSTRAINT `frauds_ibfk_1` FOREIGN KEY (`transactionID`)
REFERENCES `transactions` (`transactionID`) ON DELETE CASCADE ON
UPDATE CASCADE;
ALTER TABLE `transactions`
  ADD CONSTRAINT `trans_card` FOREIGN KEY (`cardID`) REFERENCES
`cards` (`cardID`) ON DELETE CASCADE ON UPDATE CASCADE;
```

Лістинг А.2 – Підключення бази даних

```
<?php
define('DB_NAME', 'ip2');
define('DB_USER', 'root');
define('DB_PASSWORD', '123qsc');
define('DB_HOST', 'localhost');
define('DB_CHARSET', 'utf8');
$link = mysqli_connect(DB_HOST, DB_USER, DB_PASSWORD, DB_NAME) or
die('ошибка подключения БД');
mysqli_set_charset($link, "utf8");
?>
```

Додаток Б

Алгоритмічне забезпечення системи

Лістинг Б.1 – Програмний код фільтрування операції з банківською картою

```
$bregion = $_POST['region_name'];
$bcity = $_POST['city_name'];
$fraudrisk = 0; $fraud = [];
$cardID = str_replace(" ","",$_POST['cardID']);
$sql = "SELECT `ort` FROM transactions WHERE cardID = '" .$cardID
. "' AND fraud=0";
$arr = mysqli_query($link,$sql);
while ($result = mysqli_fetch_assoc($arr)) {
    $array[] = $result['ort'];
}
/* фильтр 1 местоположение по IP и адрес доставки*/
if(!empty($array)) {
    if ($region == $bregion) {
        if($city != $bcity) {
            if (!in_array($bcity, $array)) {
                $fraud[] = "новый город доставки";
                $fraudrisk++;
            }
        }
    } else {
        if (!in_array($bcity, $array)) {
                $fraud[] = "разные регионы";
                $fraudrisk++;
        }
    }
}
/* фильтр 2 время и расстояние между заказами*/
if(!empty($array)) {
    $sql = "SELECT `time`, `ort`, `ip`, `latitude`, `longitude`,
`city_name` FROM transactions, location WHERE cardID = '" .
$cardID . "' AND `ip` <= ip_to ORDER BY `time` DESC LIMIT 1";
    $arr = mysqli_query($link,$sql);
    $res = mysqli_fetch_assoc($arr);
    if($res['city_name'] != $city) { // город текущий и город
последней транзакции
        $time_dif = (strtotime("now")-
strtotime($res['time']))/3600; // разница в часах
        $sql = "SELECT `latitude`, `longitude` FROM location WHERE
city_name = '" . $city . "'";
        $result = mysqli_fetch_assoc(mysqli_query($link,$sql)); //
координаты текущего города
        $lat1 = $res['latitude'];
        $long1 = $res['longitude'];
        $lat2 = $result['latitude'];
        $long2 = $result['longitude'];
```

```
        $dist = calculateTheDistance($lat1, $long1, $lat2, $long2)
/ 1000; // расстояние в км
        if($time_dif < $dist/50) { // скорость 50 км/ч
            $fraudrisk=1;
            $fraud[] = "ошибка во времени";
        }
    }
}
/* фильтр 3 несколько карт по 1 IP*/
if(!empty($array)) {
    $sql = "SELECT DISTINCT cardID as `Cards` FROM `transactions`
WHERE `time` > DATE_SUB(NOW(), INTERVAL 1 DAY) AND `ip` = '" .
$ipnum . "'";
    $result = mysqli_query($link,$sql);
    $cards = [];
    foreach ($result as $res) {
        $cards[] = $res['Cards'];
    }
    $cards[] = $cardID;
    $cards = count(array_unique($cards));
    if ($cards > 2) {
        $fraudrisk=2;
        $fraud[] = "много карт по 1 IP";
    }
}
```

Лістинг Б.2 – Розрахунок відстані між містами

```
define('EARTH_RADIUS', 6372795);
function calculateTheDistance ($φA, $λA, $φB, $λB) {
    // перевести координаты в радианы
    $lat1 = $φA * M_PI / 180;
    $lat2 = $φB * M_PI / 180;
    $long1 = $λA * M_PI / 180;
    $long2 = $λB * M_PI / 180;
    // косинусы и синусы широт и разницы долгот
    $cl1 = cos($lat1);
    $cl2 = cos($lat2);
    $sl1 = sin($lat1);
    $sl2 = sin($lat2);
    $delta = $long2 - $long1;
    $cdelta = cos($delta);
    $sdelta = sin($delta);
    // вычисления длины большого круга
    $y = sqrt(pow($cl2 * $sdelta, 2) + pow($cl1 * $sl2 - $sl1 *
$cl2 * $cdelta, 2));
    $x = $sl1 * $sl2 + $cl1 * $cl2 * $cdelta;
    $ad = atan2($y, $x);
    $dist = $ad * EARTH_RADIUS;
    return $dist;
}
```

Лістинг Б.3 – Збереження результатів в базі даних

```
if ($fraudrisk > 0) {
```

```
    $sql = "SELECT tr.cardID, tr.ip FROM frauds f, transactions tr
WHERE f.transactionID = tr.transactionID AND tr.fraud = 0
            AND tr.time > DATE_SUB(NOW(), INTERVAL 3 HOUR)";
    $frauds = mysqli_query($link, $sql);
    while ($result = mysqli_fetch_assoc($frauds)) {
        $WL_cards[] = $result['cardID'];
        $WL_ip[] = $result['ip'];
    }
    if(in_array($cardID, $WL_cards) || in_array($ipnum, $WL_ip))
    {
        $sql = 'INSERT INTO `transactions`(`cardID`, `region`,
`ort`, `ip`, `fraud`) VALUES ("' . $cardID . '", "' . $bregion .
'", "' .
        $bcity . '", "' . $ipnum . '", "0")';
        echo $sql;
        mysqli_query($link, $sql);
    } else {
        $fraud = implode(" ",$fraud);
        $sql = 'INSERT INTO `transactions`(`cardID`, `region`,
`ort`, `ip`, `fraud`) VALUES ("' . $cardID . '", "' . $bregion .
'", "' .
        $bcity . '", "' . $ipnum . '", "1")';
        mysqli_query($link, $sql);
        $transactionID = mysqli_insert_id($link);
        $code = mt_rand(10000, 99999);
        $sql = "INSERT INTO `frauds`(`transactionID`, `code`,
`reason`) VALUES ('" . $transactionID . "', '" . $code . "', '"
.$fraud . "')";
        mysqli_query($link, $sql);
        include_once('send.php');
        mysqli_close($link);
        echo '<form method="post" accept-charset="UTF-
8"action="send_form.php" name="send_form">
                <input type="hidden" name="transaction" value="' .
$transactionID . '">
            </form>';
        echo '<script type="text/javascript">
        document.forms["send_form"].submit();
        </script>';
    }
}
```

Додаток В

Клієнтський веб-додаток

Лістинг В.1 – Створення вікна здійснення онлайн-платежу

```
<?php include_once('ip.php'); ?>
<!DOCTYPE html>
<html lang="en">
<head>
     <meta charset="utf-8">
    <meta name="viewport" content="width=device-width, initial-
scale=1, shrink-to-fit=no">
     <title>Anti-fraud system</title>
     <link rel="stylesheet"
href="https://stackpath.bootstrapcdn.com/bootstrap/4.1.3/css/boots
trap.min.css" integrity="sha384-
MCw98/SFnGE8fJT3GXwEOngsV7Zt27NXFoaoApmYm81iuXoPkFOJwJ8ERdknLPMO"
crossorigin="anonymous">
     <link rel="stylesheet" type="text/css" href="css/style.css">
</head>
<body>
     <div class="container">
          <h1>Страница осуществления онлайн-транзакции</h1>
               <form method="post" accept-charset="UTF-8"
name="myform" action="analys.php" id="form">
                    <div class="row">
                         <div class="form-group col-lg-4 col-md-6
col-sm-8 col-12">
                              <label class="form-row">
                                   <span class="folm_label">Номер
карты</span>
                                  <input type="text" class="form-
control form__input" name="cardID" pattern="[0-9]{4}\s[0-
9]{4}\s[0-9]{4}\s[0-9]{4}"  required placeholder="XXXX XXXX XXXX
XXXX">
                              </label>
                        </div>
                        <div class="form-group col-lg-3 col-md-4 col-
sm-6 col-8">
               <label class="form-row">
               <span class="folm_label">Срок действия</span>
                    <div class="grid grid-gutter">
                         <div class="item-gutter">
                              <span class="form__input form_input-
selectable">
                                   <select id="MM" name="MM"
class="form-select">
                                   <option value="01">01</option>
                                   <option value="02">02</option>
                                   <option value="03">03</option>
                                   <option value="04">04</option>
```

```
                                        <option value="05">05</option>
                                        <option value="06">06</option>
                                        <option value="07">07</option>
                                        <option value="08">08</option>
                                        <option value="09">09</option>
                                        <option value="10">10</option>
                                        <option value="11">11</option>
                                        <option value="12">12</option>
                                </select>
                                </span>
                        </div>
                        <div class="item-gutter">
                        <span class="form__input form_input-selectable">
                        <select id="YY" name="YY" class="form-select">
                                        <option value="18">18</option>
                                        <option value="19">19</option>
                                        <option value="20">20</option>
                                        <option value="21">21</option>
                                        <option value="22">22</option>
                                        <option value="23">23</option>
                                        <option value="24">24</option>
                                        <option value="25">25</option>
                        </select>
                        </span>
                        </div>
                </div>
                </label>
        </div>
        <div class="form-group col-md-2 col-sm-3 col-4">
                <label class="form-row">
                        <span class="folm_label">Код CVV2</span>
                       <input type="password" class="form-control
form__input" name="CVV2" maxlength="3" required placeholder="XXX">
                </label>
         </div>
                        </div>
                        <div class="row"><b>Адрес доставки</b></div>
                        <div class="row">
                        <div class="form-group col-lg-3 col-sm-6 col-12">
                             <label class="form-row">
                                  <span class="folm_label">Область</span>
                                      <span class="form__input form_input-
selectable">
                                       <select id="region_name"
name="region_name" class="form-select">
                                        <?php
                                        $sql = "SELECT DISTINCT
region_name FROM location_ua WHERE `region_name` <> '-'";
                                     $array = mysqli_query($link, $sql);
                                          while ($result =
mysqli_fetch_assoc($array)) {
        if($result['region_name']== $region){
```

```
                                        echo '<option value="' .
$result['region_name'] . '" selected>' . $result['region_name'] .
'</option>';
                                            } else {
               echo '<option value="' . $result['region_name'] .
'">' . $result['region_name'] . '</option>';
                                                }
                                            }
                                            ?>
                                        </select>
                                    </span>
                                </label>
                            </div>
                <div class="form-group col-lg-3 col-sm-6 col-12">
                    <label class="form-row">
                    <span class="folm_label">Город доставки</span>
                   <span class="form__input form_input-selectable" >
                    <select id="city_name" name="city_name" class="form-
select">
                        <?php $sql = "SELECT DISTINCT city_name FROM
location_ua WHERE `region_name` = '" . $region . "'";
                        $array = mysqli_query($link, $sql);
                        while ($result = mysqli_fetch_assoc($array)) {
     if($result['city_name']== $city){
                        echo '<option value="' . $result['city_name'] .
'" selected>' . $result['city_name'] . '</option>';
                                            } else {
                        echo '<option value="' . $result['city_name'] .
'">' . $result['city_name'] . '</option>';
                                        }
                                    }
                                        mysqli_close($link);?>
                                            </select>
                                        </span>
                                    </label>
                            </div>
                 <div class="form-group col-lg-3 col-sm-6 col-12">
                        <label class="form-row">
                        <span class="folm_label">Улица</span>
                       <input type="text" class="form-control
form__input" name="street" required >
                        </label>  </div>
                   <div class="form-group col-lg-1 col-sm-3 col-6">
                        <label class="form-row">
                             <span class="folm_label">Дом</span>
                            <input type="text" class="form-control
form__input" name="street" required >
                        </label>
                          </div>
                          <div class="form-group col-lg-1 col-6">
                                  <label class="form-row">
                             <span class="folm_label">Квартира</span>
```

```
                    <input type="text" class="form-control
form__input" name="street" >
                                </label>
                        </div>
                </div>
                <div class="center">
                <input type="submit" name="form" class="button"
value="Оплатить">
                </div>
            </form>
     </div>
<script type="text/javascript" src="js/jquery-
3.3.1.min.js"></script>
<script src="https://cdnjs.cloudflare.com/ajax/libs/popper.js/
1.14.3/umd/popper.min.js" integrity="sha384-
ZMP7rVo3mIykV+2+9J3UJ46jBk0WLaUAdn689aCwoqbBJiSnjAK/l8WvCWPIPm49"
crossorigin="anonymous"></script>
<script src="https://stackpath.bootstrapcdn.com/bootstrap/4.1.3
/js/bootstrap.min.js" integrity="sha384-
ChfqqxuZUCnJSK3+MXmPNIyE6ZbWh2IMqE241rYiqJxyMiZ6OW/JmZQ5stwEULTy"
crossorigin="anonymous"></script>
<script type="text/javascript">
      $(document).ready(function(){
        $("#region_name").change(function() {
            var region = {region:$("#region_name").val()};
            $.ajax({
                type:'POST',
                url:'ajax.php',
                data:region,
                success:function(data){
                    $('#city_name').html(data)
                }
            });
        });
        var field = $('#region_name').find('option');
    });
     var cc = myform.cardID;
     for (var i in ['input', 'change', 'blur', 'keyup']) {
     cc.addEventListener('input', formatCardCode, false);
     }
     function formatCardCode() {
         var cardCode = this.value.replace(/[^\d]/g,
'').substring(0,16);
         cardCode = cardCode != '' ?
cardCode.match(/.{1,4}/g).join(' ') : '';
         this.value = cardCode;
     }
</script>
</body>
</html>
```

Лістинг В.2 – Створення вікна підтвердження платежу

```
<?php
include_once('db.php');
if(!empty($_POST['code'])) {
     $sql = "SELECT code FROM `frauds` WHERE transactionID = " .
$_POST['transaction'] ;
    mysqli_query($link, $sql);
    $result = mysqli_fetch_assoc(mysqli_query($link,$sql));
    if($result['code'] == $_POST['code']) {
     $sql = "UPDATE transactions SET fraud=0 WHERE transactionID =
" . $_POST['transaction'];
     mysqli_query($link, $sql);
     header("Location: /");
    } else {
     $error = "Вы ввели неверный код попробуйте снова";
    }
}
mysqli_close($link);
?>
<!DOCTYPE html>
<html lang="en">
<head>
     <meta charset="utf-8">
    <meta name="viewport" content="width=device-width, initial-
scale=1, shrink-to-fit=no">
     <title>Anti-fraud system</title>
     <link rel="stylesheet"
href="https://stackpath.bootstrapcdn.com/bootstrap/4.1.3/css/boots
trap.min.css" integrity="sha384-
MCw98/SFnGE8fJT3GXwEOngsV7Zt27NXFoaoApmYm81iuXoPkFOJwJ8ERdknLPMO"
crossorigin="anonymous">
     <link rel="stylesheet" type="text/css" href="css/style.css">
</head>
<body>
     <div class="container">
          <h1>Подтверждение онлайн-транзакции</h1>
          <?php if (!empty($error)) {
               echo "<h2 class='error'>" . $error . "</h2>";
          } else {
               echo '<h2>на ваш телефон было отправлено СМС-
сообщение с кодом подтверждения<br> введите этот код в поле и
нажмите подтвердить</h2>';
          }
          ?>
          <form method="post" accept-charset="UTF-8" name="myform"
action="send_form.php" id="form">
               <div class="row">
          <div class="form-group col-lg-4 col-sm-3 col-12"></div>
               <div class="form-group col-lg-4 col-sm-6 col-12">
                         <label class="form-row">
```

```
                                <span class="folm_label">Код
подтверждения</span>
                               <input type="text" class="form-control
form__input" name="code" maxlength="5" required >
                               <input type="hidden"
name="transaction" value="<?= $_POST[‘transaction’]; ?>">
                           </label>
                  </div>
                  <div class="form-group col-lg-4 col-sm-3 col-12
center"></div>
             </div>
             <div class="center">
               <input type="submit" name="form" class="button"
value="Подтвердить">
          </div>
        </form>
    </div>
</body>
</html>
```

Лістинг В.3 – Створення вікна виведення шахрайських операцій

```
<?php include_once(‘db.php’);
$sql = "SELECT Tr.`transactionID`, Concat(Cl.sname, ‘ ’, Cl.fname)
as ‘Client’, Tr.`cardID`, Cl.telephone, Tr.`time`, Tr.`fraud`,
Fr.`reason`
FROM `frauds` Fr
INNER JOIN `transactions` Tr ON Tr.`transactionID` =
Fr.`transactionID`
INNER JOIN `cards` C ON C.cardID = Tr.cardID
INNER JOIN `clients` Cl ON Cl.clientID = C.clientID";
$array = mysqli_query($link,$sql);
 ?>
<!DOCTYPE html>
<html lang="en">
<head>
     <meta charset="utf-8">
    <meta name="viewport" content="width=device-width, initial-
scale=1, shrink-to-fit=no">
     <title>Anti-fraud system</title>
     <link rel="stylesheet"
href="https://stackpath.bootstrapcdn.com/bootstrap/4.1.3/css/boots
trap.min.css" integrity="sha384-
MCw98/SFnGE8fJT3GXwEOngsV7Zt27NXFoaoApmYm81iuXoPkFOJwJ8ERdknLPMO"
crossorigin="anonymous">
</head>
<body>
     <div class="container">
          <h2 style="text-align: center;">Результат работы
модуля</h2>
          <h2 style="text-align: center;">операции, которые
вызывают подозрения</h2>
          <table class="table table-striped">
```

```
                <thead>
                    <tr>
                      <th scope="col">#</th>
                      <th scope="col">Клиент</th>
                      <th scope="col">Карта</th>
                      <th scope="col">Дата и время</th>
                      <th scope="col">Причина отмены платежа</th>
                      <th scope="col">Операция мошенническая</th>
                      <th scope="col">Телефон</th>
                    </tr>

                <tr>
                     <td></td>
                     <td>
                       <input id="client" class="form-control">
                   </td>
                   <td>
                       <input id="card" class="form-control">
                   </td>
                   <td>
                     <input type="date" name="date" id="time"
class="form-control">
                   </td>
                   <td>
                     <select id="reason" class="form-control">
                          <option value="">---</option>
                          <option value="новый город доставки">новый
город доставки</option>
                          <option value="ошибка во времени">ошибка
во времени</option>
                          <option value="разные регионы">разные
регионы</option>
                          <option value="много карт по 1 IP">много
карт по 1 IP</option>
                     </select>
                   </td>
                   <td>
                     <select id="fraud" class="form-control">
                          <option value="">--</option>
                          <option value="Нет">Нет</option>
                          <option value="Да">Да</option>
                     </select>
                   </td>

                   <td>
                     <input id="telephone" class="form-control">
                   </td>
                </tr>
                </thead>
                <tbody id="target">
               <?php $i=0; while ($result =
mysqli_fetch_assoc($array)) { $i++;
```

```
                echo "<tr>
                 <td>" . $i . "</td>
                 <td>" . $result['Client'] . "</td>
                 <td>" . $result['cardID'] . "</td>
                 <td class='edit time " .$result['transactionID']
."'>" . substr($result['time'], 0, 10) . "</td>
                 <td>" . $result['reason'] . "</td>
                 <td class='edit fraud " .$result['transactionID']
."'>";
               echo ($result['fraud']==1) ? "Да" : "Нет";
               echo "</td>
                 <td class='edit telephone "
.$result['transactionID'] ."'>" . $result['telephone'] . "</td>
                </tr>";
                } ?>
                </tbody>
          </table>
     </div>
<script type="text/javascript" src="js/jquery-
3.3.1.min.js"></script>
<script
src="https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.14.3/umd/p
opper.min.js" integrity="sha384-
ZMP7rVo3mIykV+2+9J3UJ46jBk0WLaUAdn689aCwoqbBJiSnjAK/l8WvCWPIPm49"
crossorigin="anonymous"></script>
<script
src="https://stackpath.bootstrapcdn.com/bootstrap/4.1.3/js/bootstr
ap.min.js" integrity="sha384-
ChfqqxuZUCnJSK3+MXmPNIyE6ZbWh2IMqE241rYiqJxyMiZ6OW/JmZQ5stwEULTy"
crossorigin="anonymous"></script>
<script type="text/javascript"
src="js/filterTable.v1.0.src.js"></script>
<script type="text/javascript" src="js/bank.js"></script>
</body>
</html>
```

Лістинг В.4 – Програмний код фільтрації інформації у веб-додатку

```
var filterTable = function (HTMLTBodyRef, aFilters) {
    var rows = HTMLTBodyRef.getElementsByTagName("TR"),
        filters = {}, n,
        walkThrough = function (rows) {
            var tr, i, f;
            for (i = 0; i < rows.length; i += 1) {
                tr = rows.item(i);
                for(f in filters) {
                    if (filters.hasOwnProperty(f)) {
                        if (false ===
filters[f].validate(tr.children[f].innerText) ) {
                            tr.style.display = "none"; break;
                        } else {
                            tr.style.display = "";
                        }
```

```
                    }
                }
            }
        };
    for(n in aFilters) {
        if (aFilters.hasOwnProperty(n)) {
            if (aFilters[n] instanceof filterTable.Filter) {
                filters[n] = aFilters[n];
            } else {
                filters[n] = new filterTable.Filter(aFilters[n]);
            }
            filters[n]._setAction("onchange", function ()
{walkThrough(rows);});
        }
    }
}
filterTable.Filter = function (HTMLElementRef, callback, eventName) {
  /* Если ф-цию вызвали не как конструктор фиксим этот момент: */
  if (!(this instanceof arguments.callee)) {
    return new arguments.callee(HTMLElementRef, callback, eventName);
  }
    /* Выравниваем пришедший аргумент к массиву */
    this.filters = {}.toString.call(HTMLElementRef) == "[object
Array]" ? HTMLElementRef : [HTMLElementRef];

    /**
     * Шаблонный метод вызывается для каждой строки таблицы, для
соответствующей
     * ячейки. Номер ячейки задается в объекте-конфигурации
фильтров ф-ции
     * filterTable (См. параметр 2 ф-ции tableFilter )
     * @param String cellValue - строковое значение ячейки
     * @returns {boolean}
     */
    this.validate = function (cellValue) {
        for (var i = 0; i < this.filters.length; i += 1) {
            if ( false === this.__validate(cellValue,
this.filters[i], i) ) {
                return false;
            }
        }
    }
    this.__validate = function (cellValue, filter, i) {
        /* Если фильтр был создан явно и явно указана функция
валидации: */
        if (typeof callback !== "undefined") {
            return callback(cellValue, this.filters, i);
        }
        /* Если в фильтр напихали пробелов или другой непечатной
фигни - удаляем: */
        filter.value = filter.value.replace(/^\s+$/g, "");
```

```
        /* "Фильтр содержит значение и оно совпало со значением
ячейки" */
        return !filter.value || filter.value == cellValue;
    }
    this._setAction = function (anEventName, callback) {
        for (var i = 0; i < this.filters.length; i += 1) {
            this.filters[i][eventName||anEventName] = callback;
        }
    }
};
```

Лістинг В.5 – Маніпулювання даними про шахрайські платежі у реальному часі

```
$(document).ready(function(){
        $("#region_name").change(function(){
            var region = {region:$("#region_name").val()};
            $.ajax({
                type:'POST',
                url:'ajax.php',
                data:region,
                success:function(data){
                    $('#city_name').html(data)
                }
            });
        });
        var field = $('#region_name').find('option');
        filterTable( document.getElementById("target"), {
   1: new filterTable.Filter(document.getElementById("client"),
                function (value, filters, i) {
                   return value.indexOf(filters[i].value) === 0;
                },
                "onkeyup"
            ),
   2: new filterTable.Filter(document.getElementById("card"),
                function (value, filters, i) {
                   return value.indexOf(filters[i].value) === 0;
                },
                "onkeyup"
            ),
   3: document.getElementById("time"),
   4: document.getElementById("reason"),
   5: document.getElementById("fraud"),
   6: new filterTable.Filter(document.getElementById ("telephone"),
                function (value, filters, i) {
                   return value.indexOf(filters[i].value) === 0;
                },
                "onkeyup"
            )
        });
        $('td.edit').click(function(){
          $('.ajax').html($('.ajax input').val());
```

```
          $('.ajax').removeClass('ajax');
               $(this).addClass('ajax');
               $(this).html('<input      id="editbox"      size="'+
$(this).text().length+'" type="text" value="' + $(this).text() + '"
/>');
               $('#editbox').focus();
        });
        $('td.edit').keydown(function(event){
          arr = $(this).attr('class').split( " " );
          console.log(arr);
          if(event.which == 13) {
                    $.ajax({
                         type: "POST",
                         url:"ajax.php",
                         data:                    "value="+$('.ajax
input').val()+"&id="+arr[2]+"&field="+arr[1],
                         success: function(data){

                              $('.ajax').html($('.ajax
input').val());
                              $('.ajax').removeClass('ajax');
                         }
                    });
               }
          });
          $(document).on('blur', '#editbox', function(){
               $('.ajax').html($('.ajax input').val());
               $('.ajax').removeClass('ajax');
          });
    });
```

Додаток Г

Аналіз адекватності кластеризації банків України

Variable	Analysis of Variance (Spreadsheet1.sta)					
	Between SS	df	Within SS	df	F	signif. p
K1	0,00	1	1,49	63	0,1522	0,697762
K2	3325,41	1	10102,04	63	20,7385	0,000025
K3	34166,78	1	5711,44	63	376,8765	0,000000
K4	3376,52	1	9466,03	63	22,4720	0,000013
K5	0,00	1	3,38	63	0,0191	0,890547
K6	0,08	1	2,91	63	1,6591	0,202439

Рисунок Г.1 – Аналіз адекватності кластеризації банків України на 2 групи станом на 2019 рік

Variable	Analysis of Variance (Spreadsheet1.sta)					
	Between SS	df	Within SS	df	F	signif. p
K1	0,01	2	1,485	62	0,1945	0,823709
K2	3983,70	2	9443,749	62	13,0769	0,000018
K3	35556,80	2	4321,418	62	255,0692	0,000000
K4	10064,80	2	2777,749	62	112,3244	0,000000
K5	0,01	2	3,370	62	0,0899	0,914145
K6	0,08	2	2,907	62	0,8827	0,418815

Рисунок Г.2 – Аналіз адекватності кластеризації банків України на 3 групи станом на 2019 рік

Variable	Analysis of Variance (Spreadsheet1.sta)					
	Between SS	df	Within SS	df	F	signif. p
K1	0,02	3	1,475	61	0,2719	0,845417
K2	10128,08	3	3299,369	61	62,4173	0,000000
K3	36181,66	3	3696,559	61	199,0212	0,000000
K4	10600,52	3	2242,035	61	96,1376	0,000000
K5	0,04	3	3,338	61	0,2542	0,858048
K6	0,37	3	2,616	61	2,9023	0,041972

Рисунок Г.3 – Аналіз адекватності кластеризації банків України на 4 групи станом на 2019 рік

Variable	Analysis of Variance (Spreadsheet1.sta)					
	Between SS	df	Within SS	df	F	signif. p
K1	0,03	4	1,468	60	0,2703	0,895985
K2	11137,62	4	2289,826	60	72,9594	0,000000
K3	36908,04	4	2970,180	60	186,3929	0,000000
K4	11009,52	4	1833,031	60	90,0927	0,000000
K5	0,05	4	3,333	60	0,2114	0,931154
K6	0,38	4	2,605	60	2,2157	0,077929

Рисунок Г.4 – Аналіз адекватності кластеризації банків України на 5 груп станом на 2019 рік

Variable	Analysis of Variance (Spreadsheet1.sta)					
	Between SS	df	Within SS	df	F	signif. p
K1	0,02	5	1,474	59	0,1632	0,975036
K2	10393,36	5	3034,085	59	40,4213	0,000000
K3	38666,29	5	1211,926	59	376,4769	0,000000
K4	12254,93	5	587,620	59	246,0913	0,000000
K5	0,06	5	3,321	59	0,2075	0,958080
K6	0,48	5	2,511	59	2,2511	0,060910

Рисунок Г.5 – Аналіз адекватності кластеризації банків України на 6 груп станом на 2019 рік

Variable	Analysis of Variance (Spreadsheet1.sta)					
	Between SS	df	Within SS	df	F	signif. p
K1	0,03	6	1,460	58	0,2289	0,965655
K2	11971,13	6	1456,312	58	79,4616	0,000000
K3	37162,34	6	2715,872	58	132,2728	0,000000
K4	12097,90	6	744,653	58	157,0480	0,000000
K5	0,25	6	3,133	58	0,7628	0,602067
K6	0,50	6	2,492	58	1,9319	0,090813

Рисунок Г.6 – Аналіз адекватності кластеризації банків України на 7 груп станом на 2019 рік

Variable	Analysis of Variance (Spreadsheet1.sta)					
	Between SS	df	Within SS	df	F	signif. p
K1	0,17	10	1,327	54	0,6794	0,738540
K2	12093,99	10	1333,460	54	48,9760	0,000000
K3	39457,59	10	420,630	54	506,5526	0,000000
K4	12345,16	10	497,390	54	134,0275	0,000000
K5	0,90	10	2,477	54	1,9685	0,055410
K6	0,61	10	2,376	54	1,3964	0,207037

Рисунок Г.7 – Аналіз адекватності кластеризації банків України на 11 груп станом на 2019 рік

	Analysis of Variance (Spreadsheet1.sta)					
Variable	Between SS	df	Within SS	df	F	signif. p
K1	0,19	11	1,304	53	0,7044	0,728662
K2	12406,89	11	1020,556	53	58,5746	0,000000
K3	39409,62	11	468,598	53	405,2143	0,000000
K4	12392,62	11	449,933	53	132,7085	0,000000
K5	0,69	11	2,687	53	1,2423	0,283569
K6	0,63	11	2,361	53	1,2834	0,259636

Рисунок Г.8 – Аналіз адекватності кластеризації банків України на 12 груп станом на 2019 рік

	Analysis of Variance (Spreadsheet1.sta)					
Variable	Between SS	df	Within SS	df	F	signif. p
K1	0,30	12	1,196	52	1,0815	0,394525
K2	12406,97	12	1020,473	52	52,6850	0,000000
K3	39409,62	12	468,594	52	364,4411	0,000000
K4	12453,37	12	389,183	52	138,6614	0,000000
K5	0,91	12	2,472	52	1,5907	0,123484
K6	0,69	12	2,296	52	1,3091	0,241957

Рисунок Г.9 – Аналіз адекватності кластеризації банків України на 13 груп станом на 2019 рік

	Analysis of Variance (Spreadsheet1.sta)					
Variable	Between SS	df	Within SS	df	F	signif. p
K1	0,32	13	1,176	51	1,0611	0,412220
K2	12406,67	13	1020,772	51	47,6819	0,000000
K3	39446,11	13	432,110	51	358,1267	0,000000
K4	12485,52	13	357,029	51	137,1923	0,000000
K5	0,92	13	2,464	51	1,4574	0,166673
K6	0,69	13	2,301	51	1,1738	0,324756

Рисунок Г.10 – Аналіз адекватності кластеризації банків України на 14 груп станом на 2019 рік

Variable	Cluster Means (Spreadsheet1.sta) Cluster No. 1	Cluster No. 2	Cluster No. 3	Cluster No. 4	Cluster No. 5	Cluster No. 6	Cluster No. 7	Cluster No. 8	Cluster No. 9
K1	0,2013	0,06525	0,09113	0,379208	0,107526	0,05923	0,07033	0,235642	0,0260
K2	100,0000	0,40000	15,33333	9,333333	0,209302	26,33333	0,00000	4,500000	0,0000
K3	100,0000	13,00000	73,00000	0,000000	0,232558	11,33333	5,00000	2,500000	37,0000
K4	34,0000	2,60000	9,00000	0,000000	0,232558	3,00000	39,00000	9,000000	100,0000
K5	0,5588	0,86964	0,75185	0,535088	0,737773	0,61717	0,84600	0,465884	0,8243
K6	1,0000	0,40808	0,41765	0,293911	0,390369	0,33949	0,70080	0,283598	0,4176

Рисунок Г.11 – Середні значення вхідних показників оцінювання ризику легалізації кримінальних доходів за виділеними кластерами

Cluster Number	Euclidean Distances between Clusters (Spreadsheet1.sta) Distances below diagonal Squared distances above diagonal No. 1	No. 2	No. 3	No. 4	No. 5	No. 6	No. 7	No. 8	No. 9
No. 1	0,00000	3079,264	1420,472	3229,496	3508,729	2375,002	3175,031	3208,670	3054,240
No. 2	55,49112	0,000	643,996	42,631	28,111	112,591	231,534	28,038	1677,154
No. 3	37,68915	25,377	0,000	907,691	933,451	659,967	959,867	847,955	1635,353
No. 4	56,82865	6,529	30,128	0,000	13,913	71,093	272,245	18,439	1909,389
No. 5	59,23453	5,302	30,552	3,730	0,000	135,562	254,299	16,754	1884,241
No. 6	48,73400	10,611	25,690	8,432	11,643	0,000	338,290	98,463	1793,545
No. 7	56,34742	15,216	30,982	16,500	15,947	18,393	0,000	154,474	790,847
No. 8	56,64513	5,295	29,120	4,294	4,093	9,923	12,429	0,000	1581,948
No. 9	55,26518	40,953	40,440	43,697	43,408	42,350	28,122	39,774	0,000

Рисунок Г.12 – Евклідові відстані між виділеними кластерами

Variable	Descriptive Statistics for Cluster 1 (Spreadsheet1.sta) Cluster contains 1 cases Mean	Standard Deviation	Variance
K1	0,2013	0,00	0,00
K2	100,0000	0,00	0,00
K3	100,0000	0,00	0,00
K4	34,0000	0,00	0,00
K5	0,5588	0,00	0,00
K6	1,0000	0,00	0,00

Рисунок Г.13 – Описові статистики першого кластеру

	Descriptive Statistics for Cluster 2 (Spreadsheet1.sta) Cluster contains 5 cases		
Variable	Mean	Standard Deviation	Variance
K1	0,06525	0,065357	0,00427
K2	0,40000	0,547723	0,30000
K3	13,00000	9,000000	81,00000
K4	2,60000	2,880972	8,30000
K5	0,86964	0,082559	0,00682
K6	0,40808	0,247655	0,06133

Рисунок Г.14 – Описові статистики другого кластеру

	Descriptive Statistics for Cluster 3 (Spreadsheet1.sta) Cluster contains 6 cases		
Variable	Mean	Standard Deviation	Variance
K1	0,09113	0,02651	0,0007
K2	15,33333	14,52813	211,0667
K3	73,00000	19,18333	368,000
K4	9,00000	10,56409	111,600
K5	0,75185	0,14606	0,0213
K6	0,41765	0,18838	0,0355

Рисунок Г.15 – Описові статистики третього кластеру

	Descriptive Statistics for Cluster 4 (Spreadsheet1.sta) Cluster contains 3 cases		
Variable	Mean	Standard Deviation	Variance
K1	0,379208	0,542008	0,29377
K2	9,333333	4,041452	16,33333
K3	0,000000	0,000000	0,0000
K4	0,000000	0,000000	0,0000
K5	0,535088	0,473707	0,2244
K6	0,293911	0,253570	0,0643

Рисунок Г.16 – Описові статистики четвертого кластеру

	Descriptive Statistics for Cluster 5 (Spreadsheet1.sta) Cluster contains 43 cases		
Variable	Mean	Standard Deviation	Variance
K1	0,107526	0,107728	0,011605
K2	0,209302	0,599926	0,359911
K3	0,232558	0,648706	0,42082
K4	0,232558	0,781854	0,611296
K5	0,737773	0,211235	0,04462
K6	0,390369	0,200499	0,04020

Рисунок Г.17 – Описові статистики п’ятого кластеру

Variable	Descriptive Statistics for Cluster 6 (Spreadsheet1.sta) Cluster contains 3 cases		
	Mean	Standard Deviation	Variance
K1	0,05923	0,04736	0,0022
K2	26,33333	5,13160	26,3333
K3	11,33333	15,50269	240,3333
K4	3,00000	3,00000	9,0000
K5	0,61717	0,14776	0,0218
K6	0,33949	0,17410	0,0303

Рисунок Г.18 – Описові статистики шостого кластеру

Variable	Descriptive Statistics for Cluster 7 (Spreadsheet1.sta) Cluster contains 1 cases		
	Mean	Standard Deviation	Variance
K1	0,07033	0,00	0,00
K2	0,00000	0,00	0,00
K3	5,00000	0,00	0,00
K4	39,00000	0,00	0,00
K5	0,84600	0,00	0,00
K6	0,70080	0,00	0,00

Рисунок Г.19 – Описові статистики сьомого кластеру

Variable	Descriptive Statistics for Cluster 8 (Spreadsheet1.sta) Cluster contains 2 cases		
	Mean	Standard Deviation	Variance
K1	0,235642	0,333248	0,11105
K2	4,500000	6,363961	40,5000
K3	2,500000	3,535534	12,5000
K4	9,000000	0,000000	0,0000
K5	0,465884	0,658859	0,4340
K6	0,283598	0,401068	0,1608

Рисунок Г.20 – Описові статистики восьмого кластеру

Variable	Descriptive Statistics for Cluster 9 (Spreadsheet1.sta) Cluster contains 1 cases		
	Mean	Standard Deviation	Variance
K1	0,0260	0,00	0,00
K2	0,0000	0,00	0,00
K3	37,0000	0,00	0,00
K4	100,0000	0,00	0,00
K5	0,8243	0,00	0,00
K6	0,4176	0,00	0,00

Рисунок Г.21 – Описові статистики дев’ятого кластеру

Додаток Д

Визначення ефективності функціонування фінансового моніторингу банків

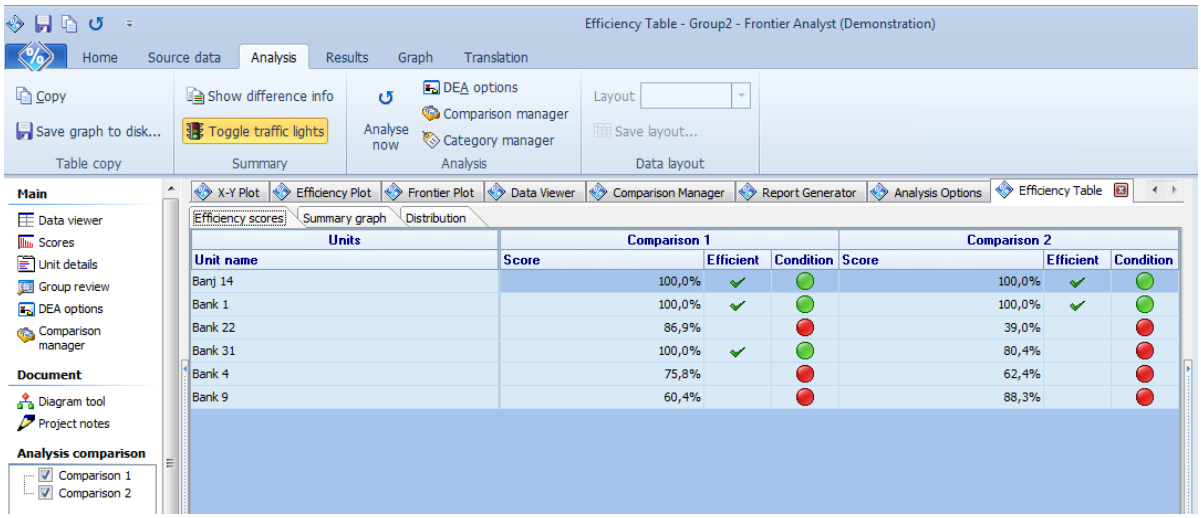


Рисунок Д.1 – Ефективність функціонування другої групи банків України станом на 2019 рік для BCC-моделі та для CCR-моделі

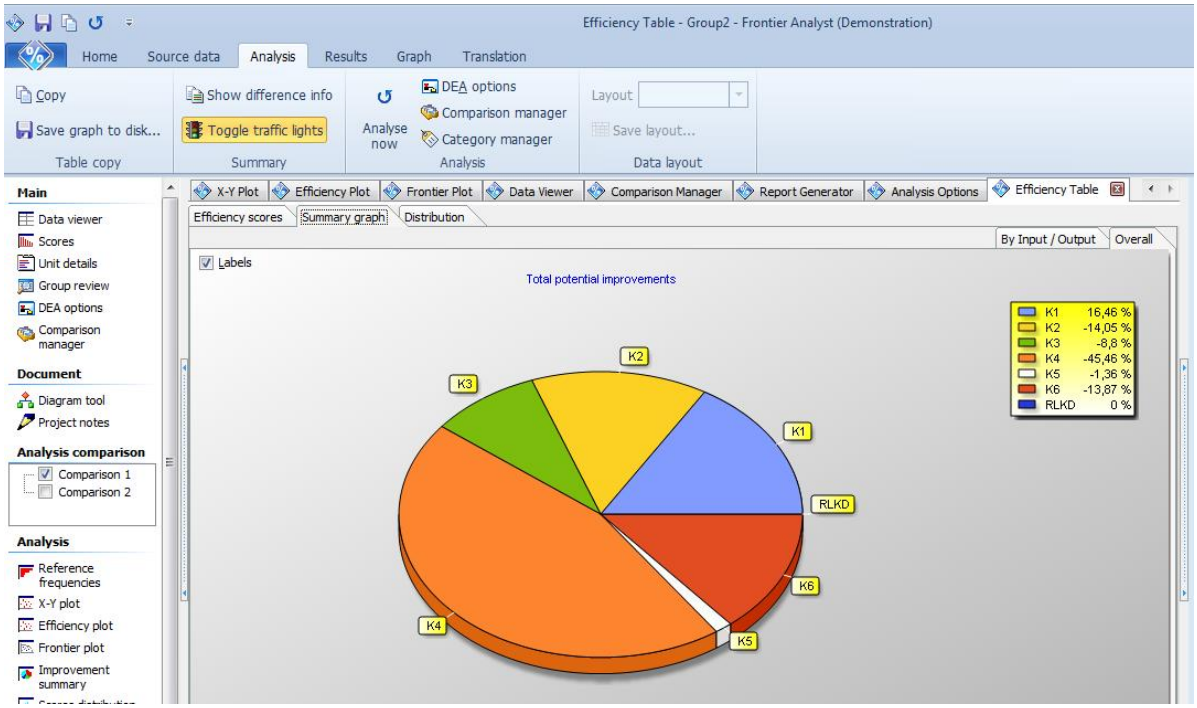


Рисунок Д.2 – Потенціал покращення ефективності функціонування фінансового моніторингу другої групи банків України станом на 2019 рік для BCC-моделі

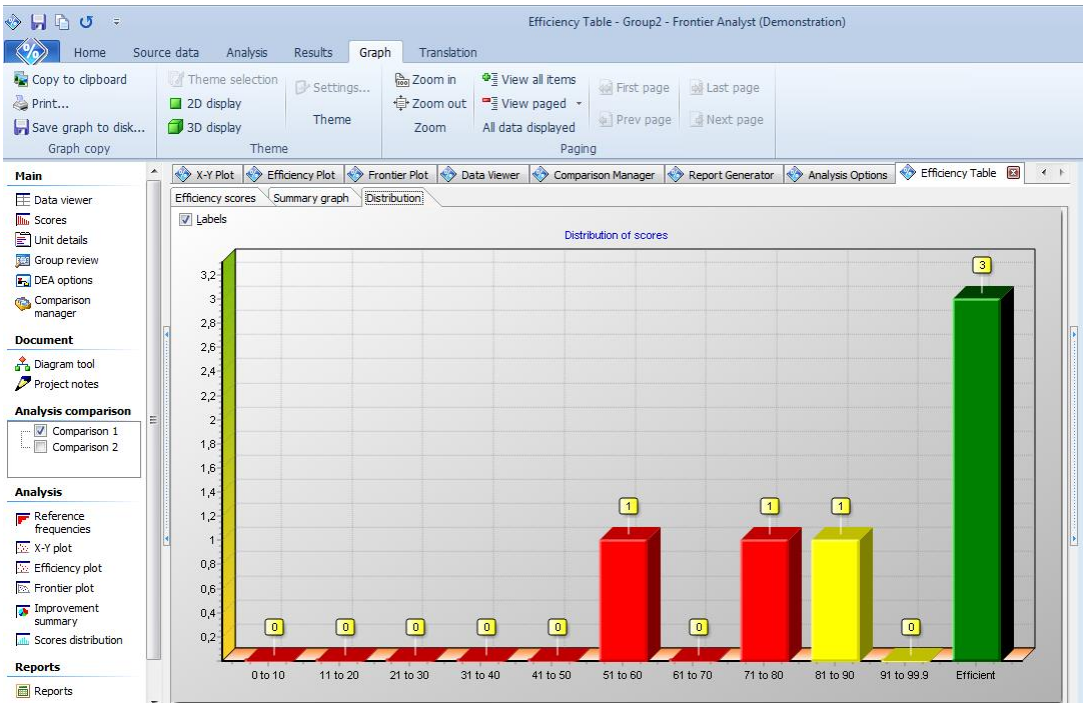


Рисунок Д.3 - Графік розподілу оцінок ефективності функціонування фінансового моніторингу другої групи банків України станом на 2019 рік для ВСС-моделі

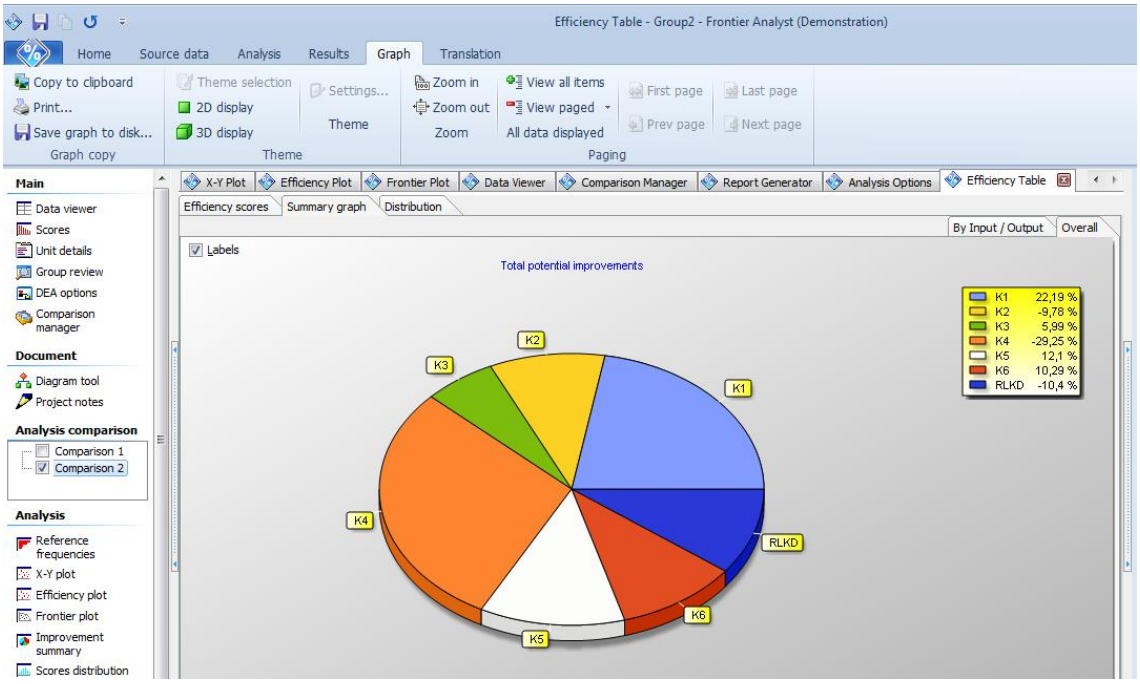


Рисунок Д.4 – Потенціал покращення ефективності функціонування фінансового моніторингу другої групи банків України станом на 2019 рік для ССR-моделі

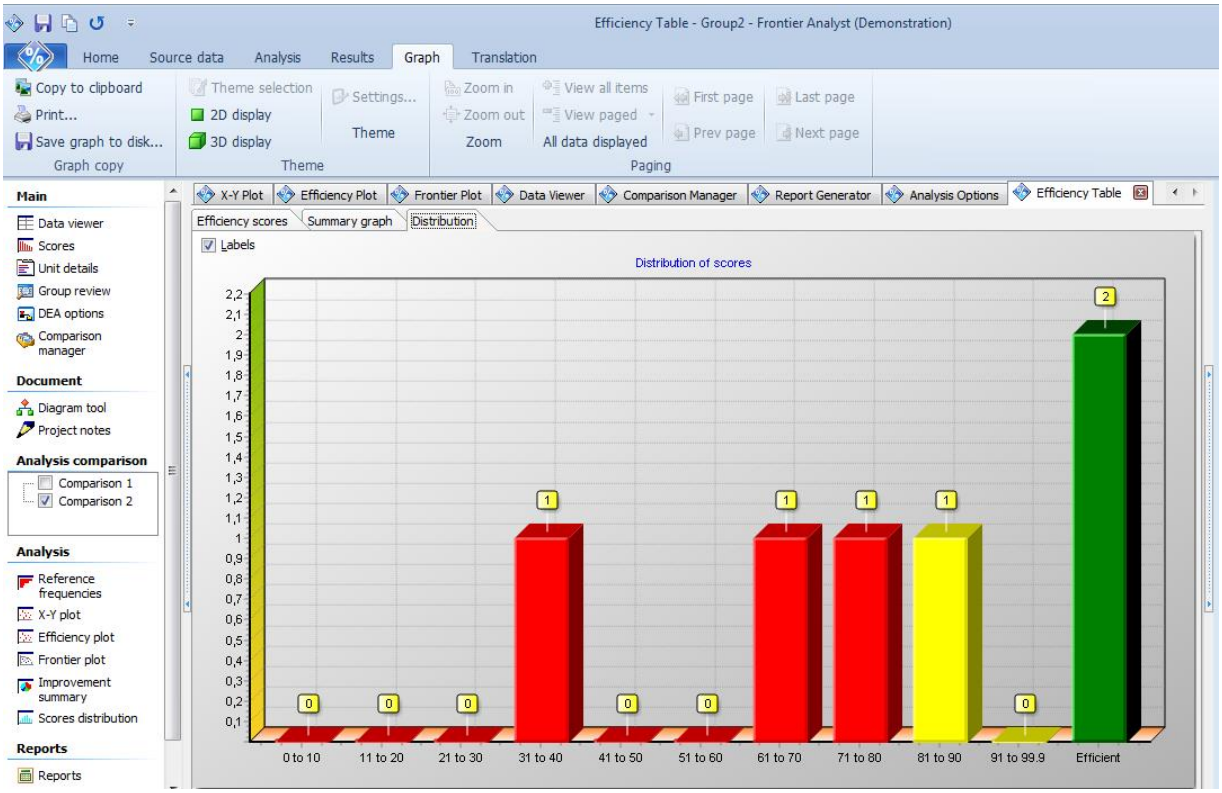


Рисунок Д.5 - Графік розподілу оцінок ефективності функціонування фінансового моніторингу другої групи банків України станом на 2019 рік для CCR-моделі

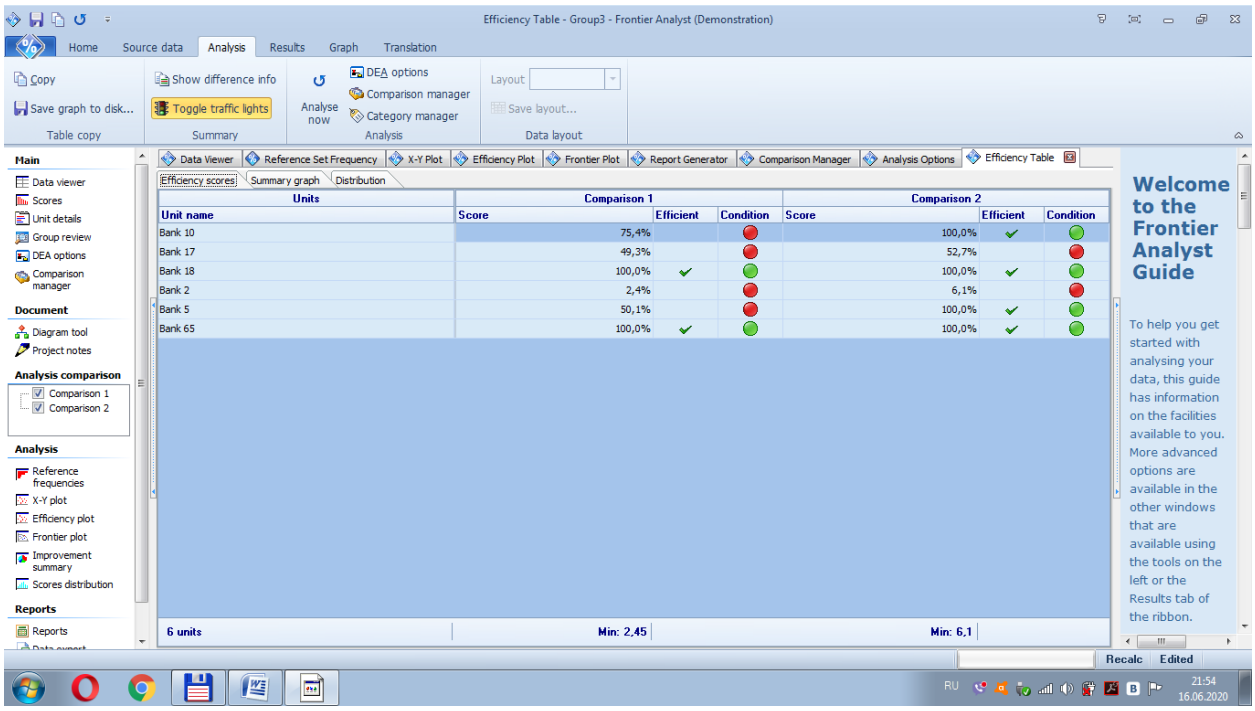


Рисунок Д.6 – Ефективність функціонування третьої групи банків України станом на 2019 рік для BCC-моделі та для CCR-моделі

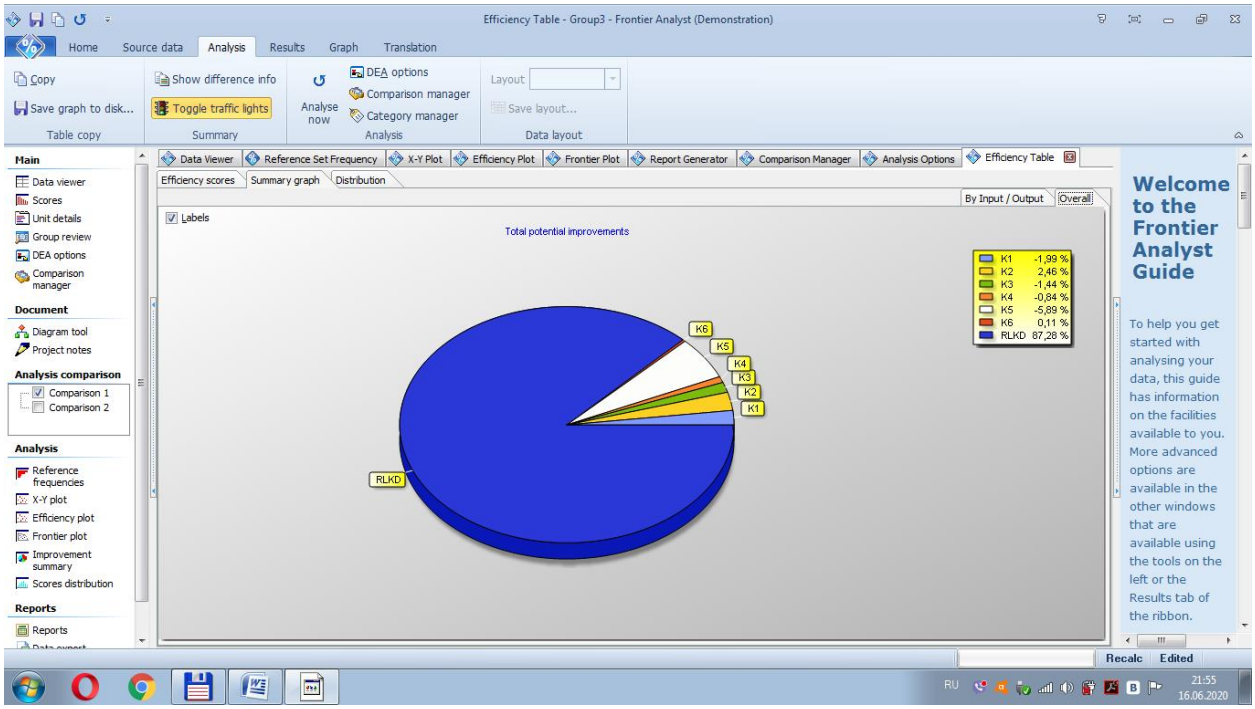


Рисунок Д.7 – Потенціал покращення ефективності функціонування фінансового моніторингу третьої групи банків України станом на 2019 рік для ВСС-моделі

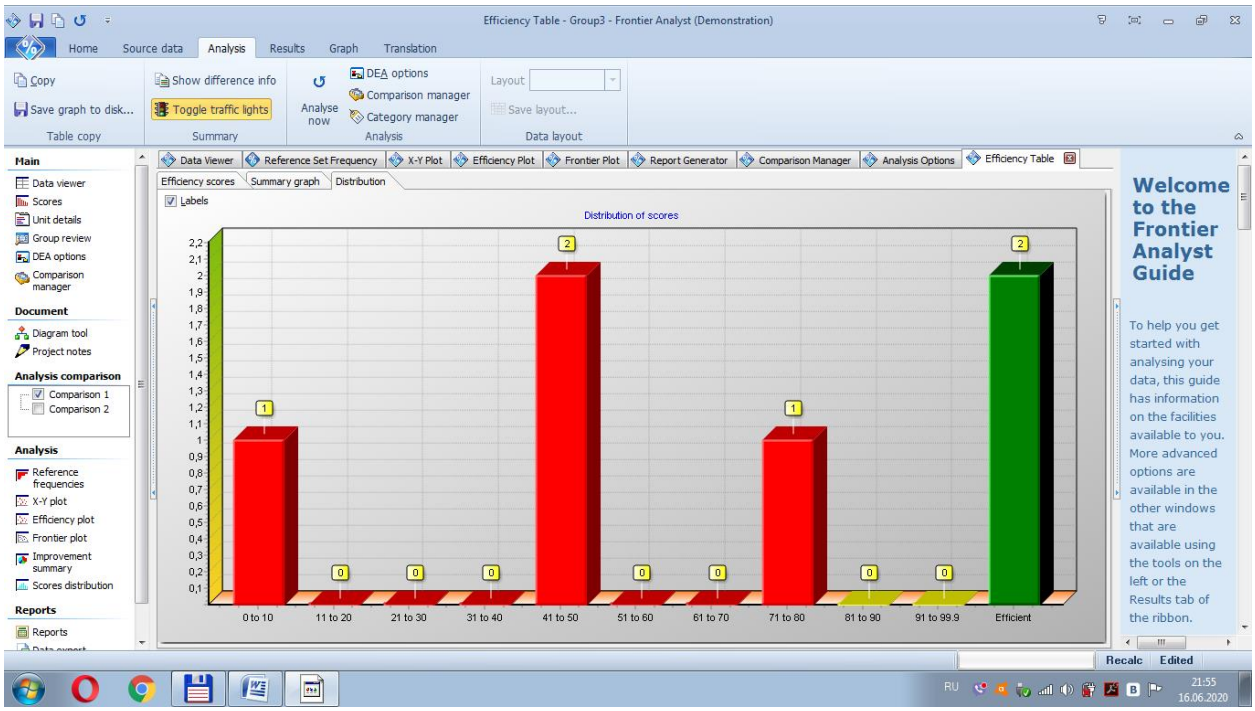


Рисунок Д.8 - Графік розподілу оцінок ефективності функціонування фінансового моніторингу третьої групи банків України станом на 2019 рік для ВСС-моделі

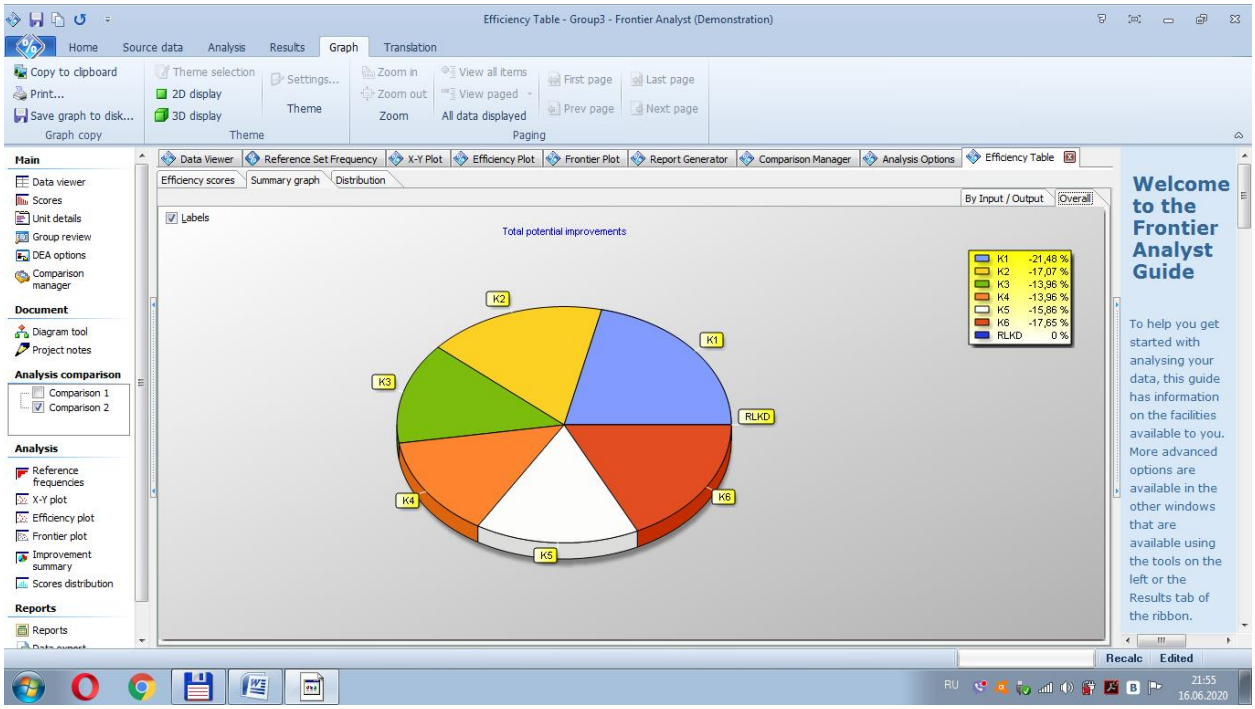


Рисунок Д.9 – Потенціал покращення ефективності функціонування фінансового моніторингу третьої групи банків України станом на 2019 рік для CCR-моделі

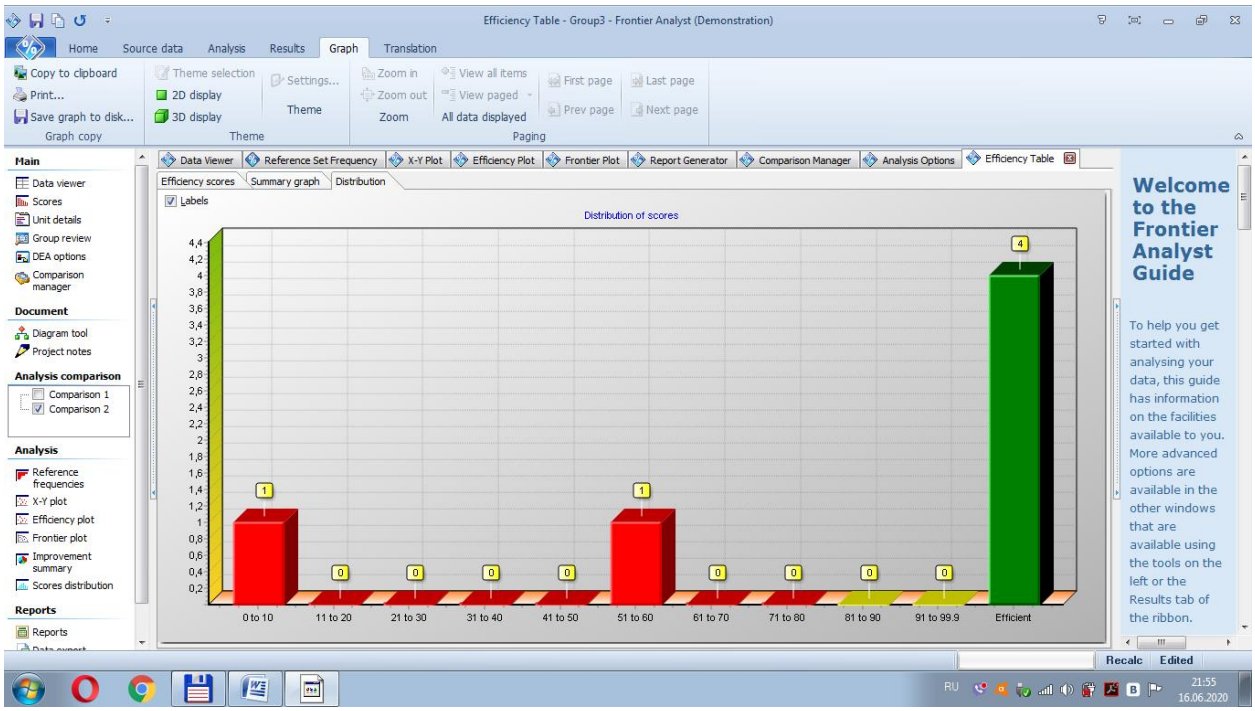


Рисунок Д.10 - Графік розподілу оцінок ефективності функціонування фінансового моніторингу третьої групи банків України станом на 2019 рік для CCR-моделі

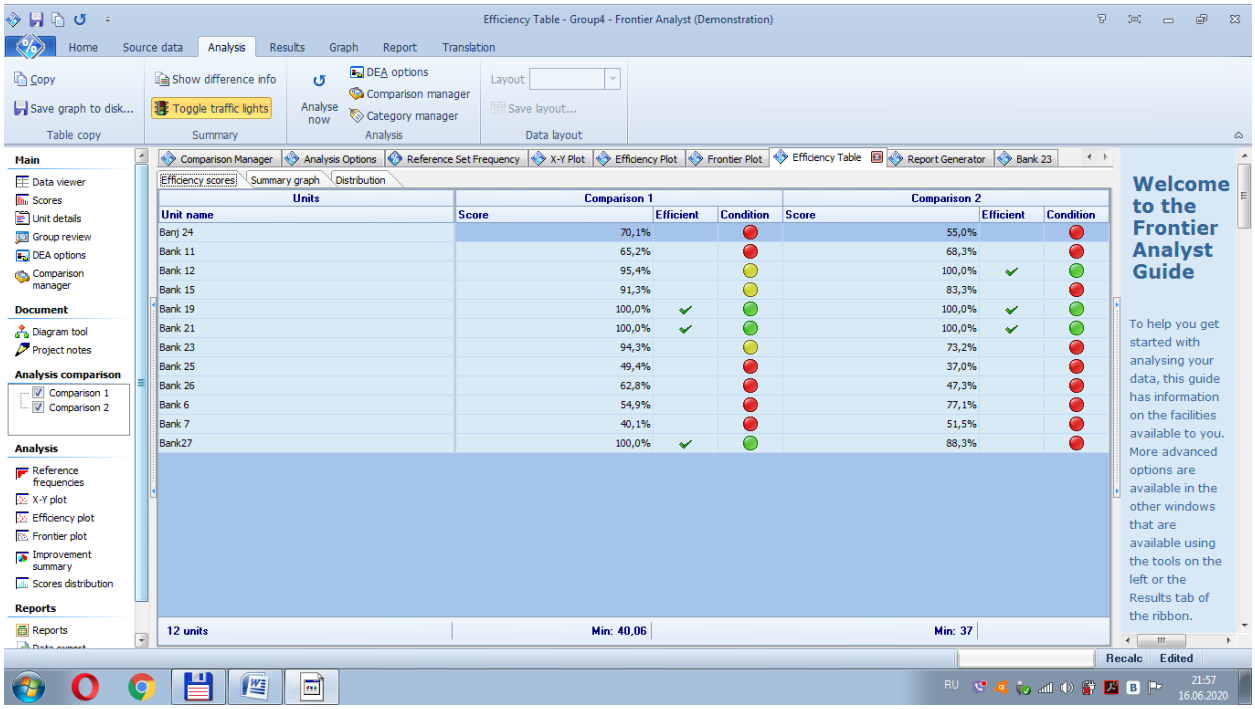


Рисунок Д.11 – Ефективність функціонування четвертої групи банків України станом на 2019 рік для ВСС-моделі та для CCR-моделі

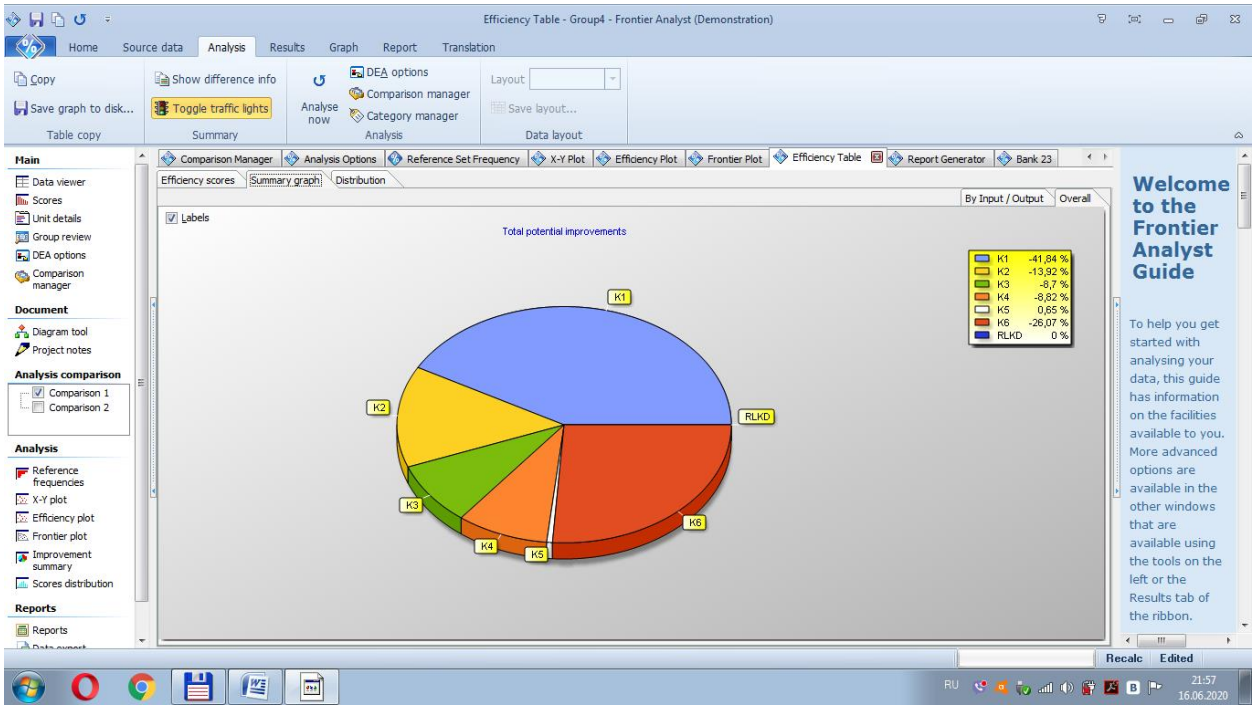


Рисунок Д.12 – Потенціал покращення ефективності функціонування фінансового моніторингу четвертої групи банків України станом на 2019 рік для ВСС-моделі

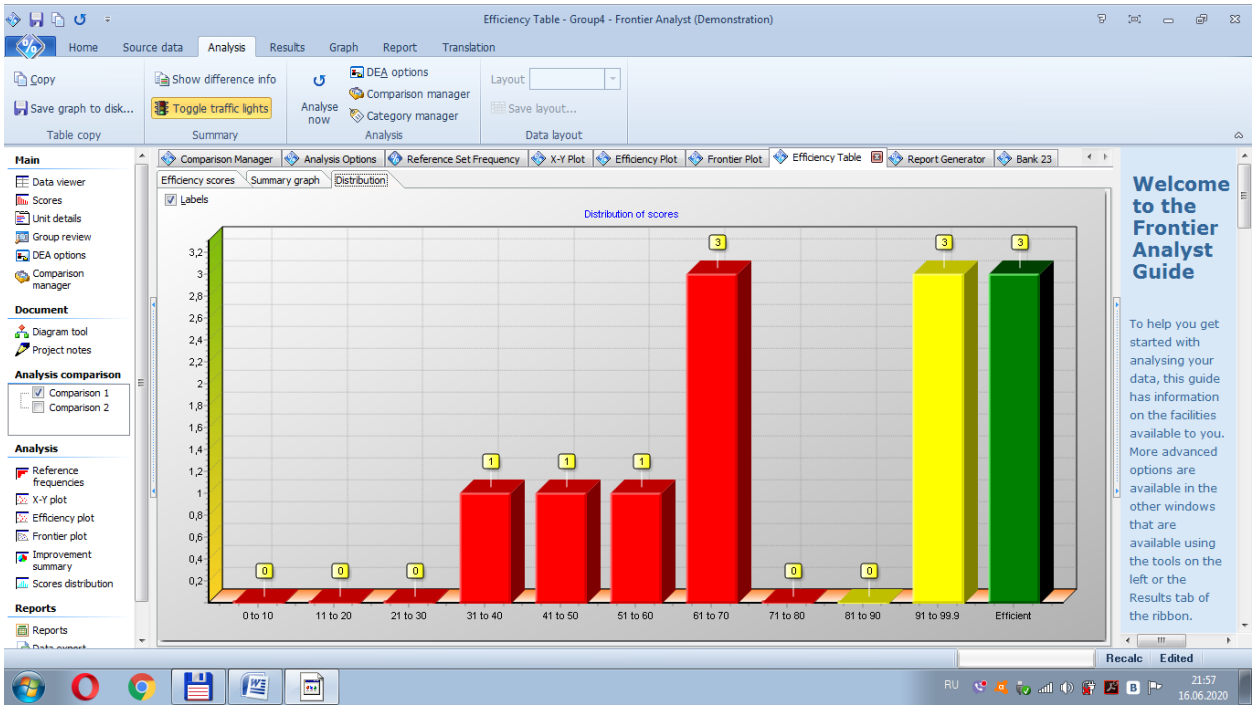


Рисунок Д.13 - Графік розподілу оцінок ефективності функціонування фінансового моніторингу четвертої групи банків України станом на 2019 рік для ВСС-моделі

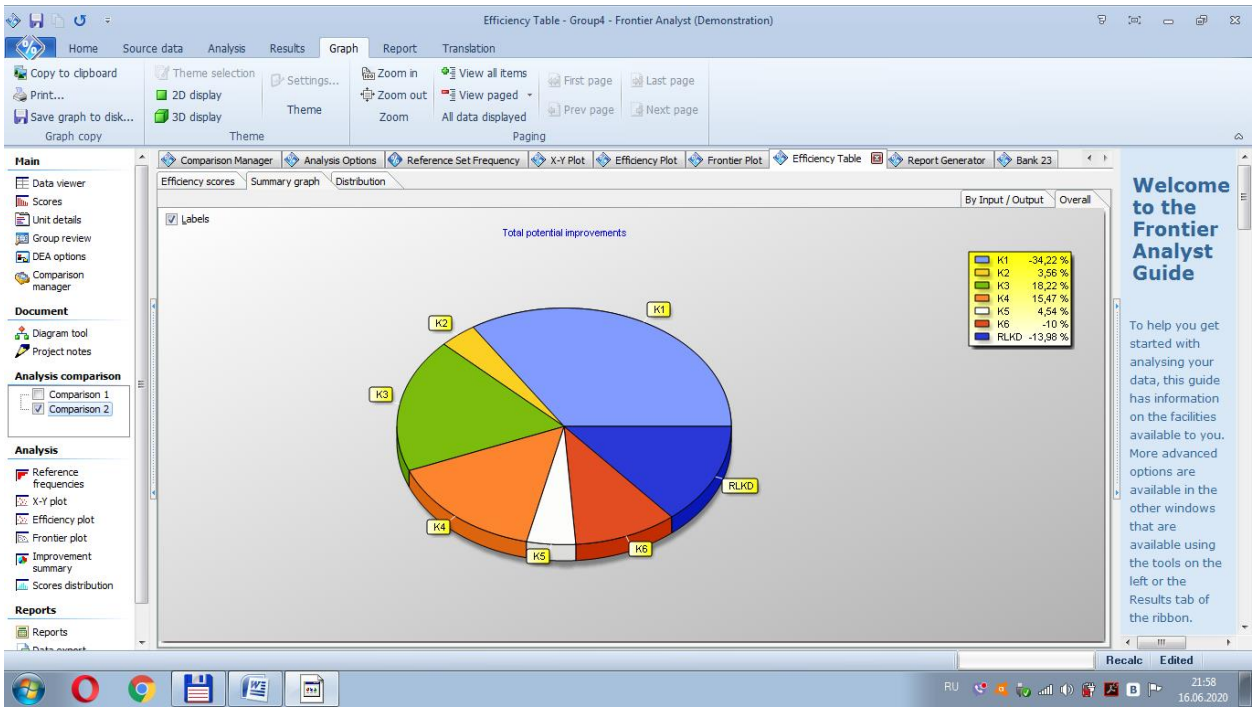


Рисунок Д.14 – Потенціал покращення ефективності функціонування фінансового моніторингу четвертої групи банків України станом на 2019 рік для CCR-моделі

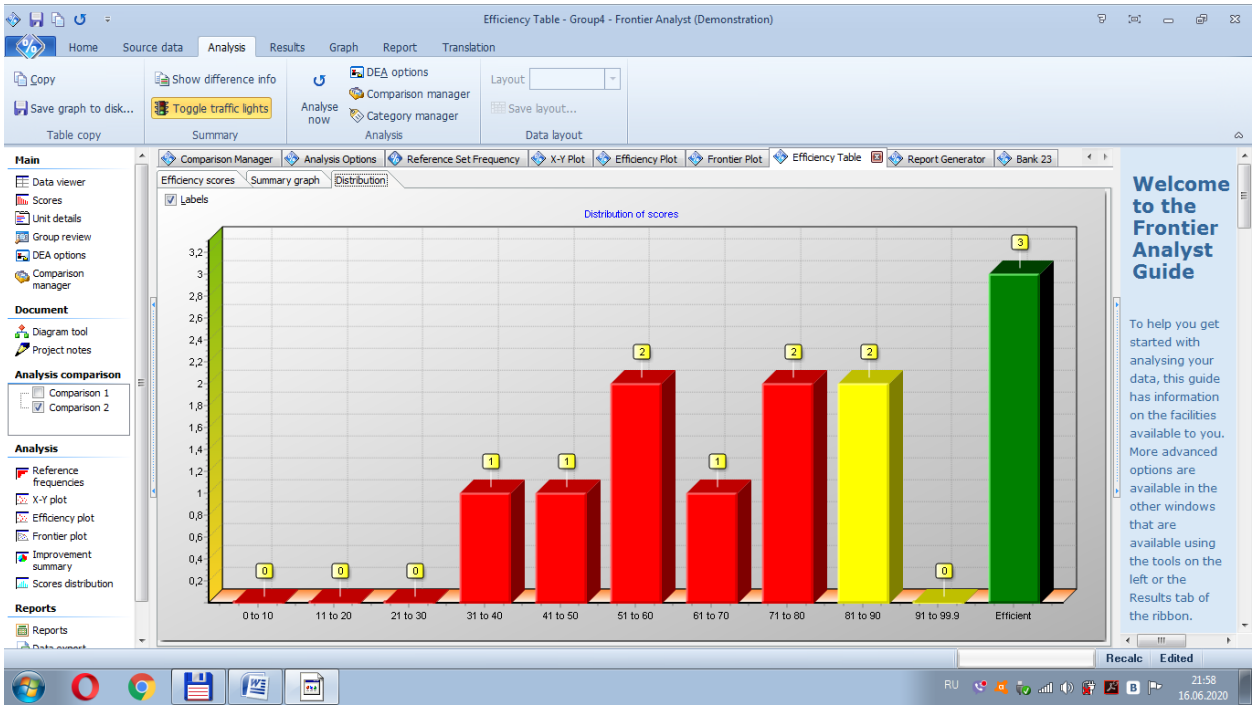


Рисунок Д.15 - Графік розподілу оцінок ефективності функціонування фінансового моніторингу четвертої групи банків України станом на 2019 рік для CCR-моделі

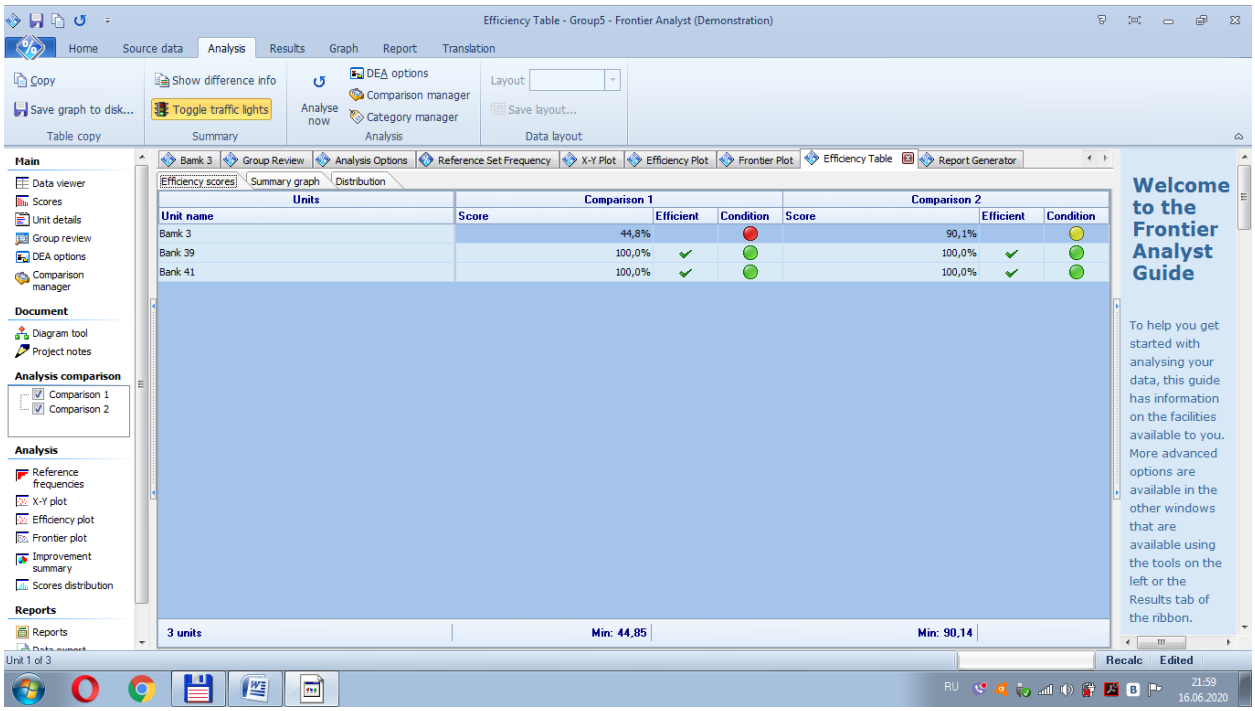


Рисунок Д.16 – Ефективність функціонування п’ятої групи банків України станом на 2019 рік для BCC-моделі та для CCR-моделі

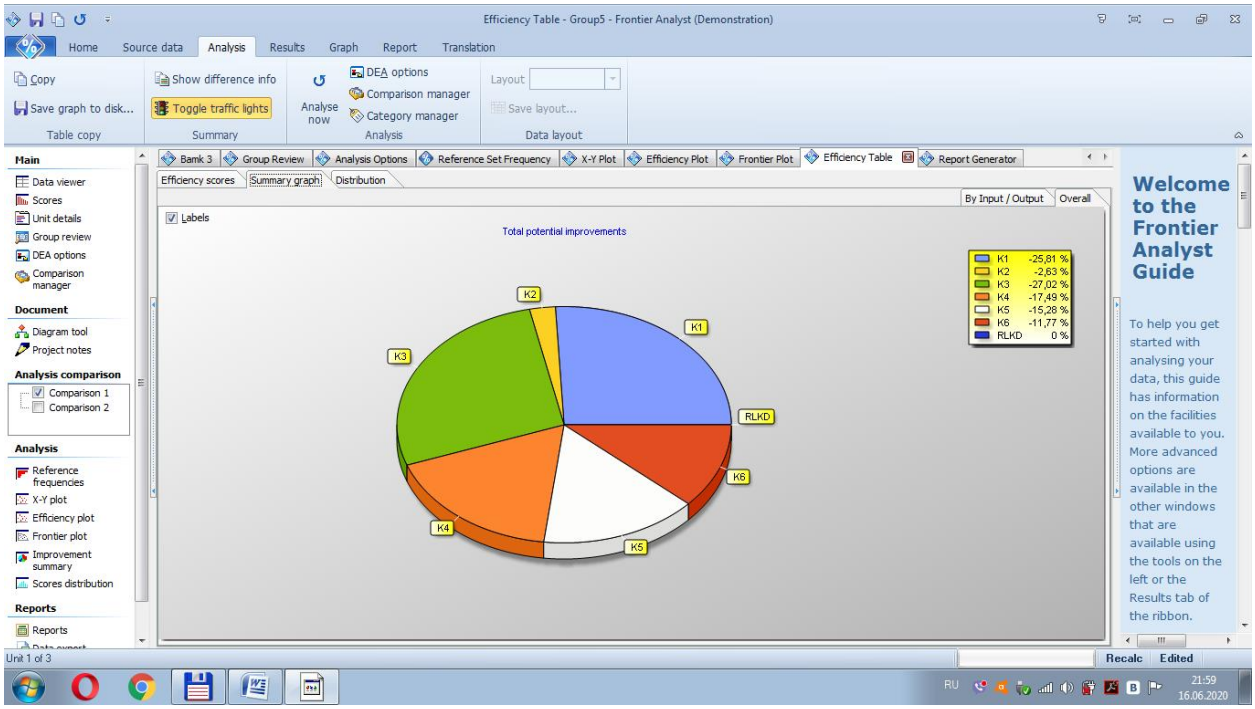


Рисунок Д.17 – Потенціал покращення ефективності функціонування фінансового моніторингу п’ятої групи банків України станом на 2019 рік для ВСС-моделі

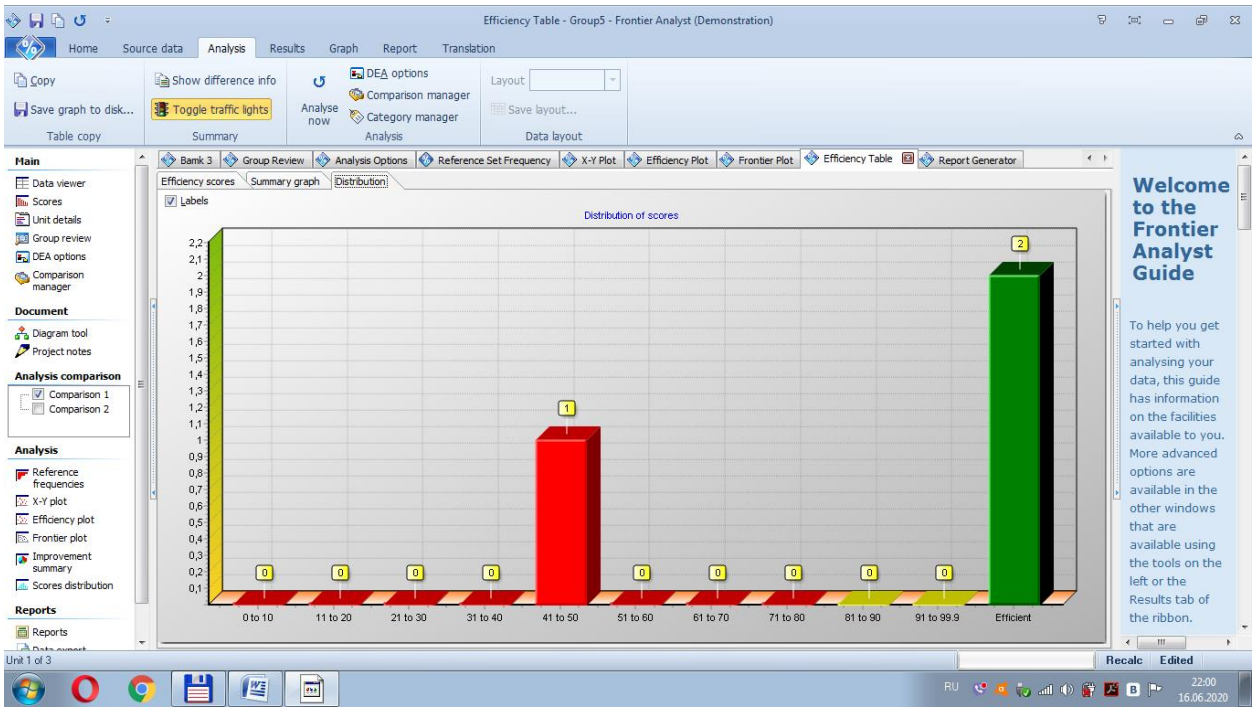


Рисунок Д.18 - Графік розподілу оцінок ефективності функціонування фінансового моніторингу п’ятої групи банків України станом на 2019 рік для ВСС-моделі

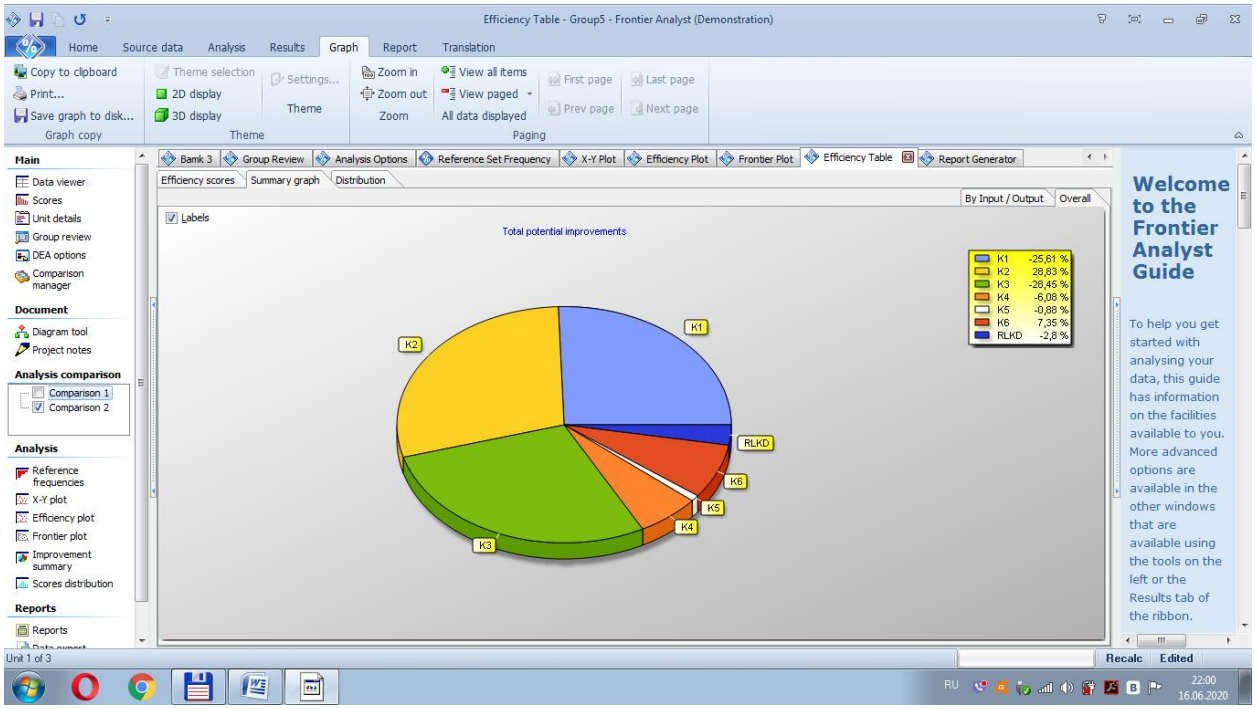


Рисунок Д.19 – Потенціал покращення ефективності функціонування фінансового моніторингу п’ятої групи банків України станом на 2019 рік для CCR-моделі

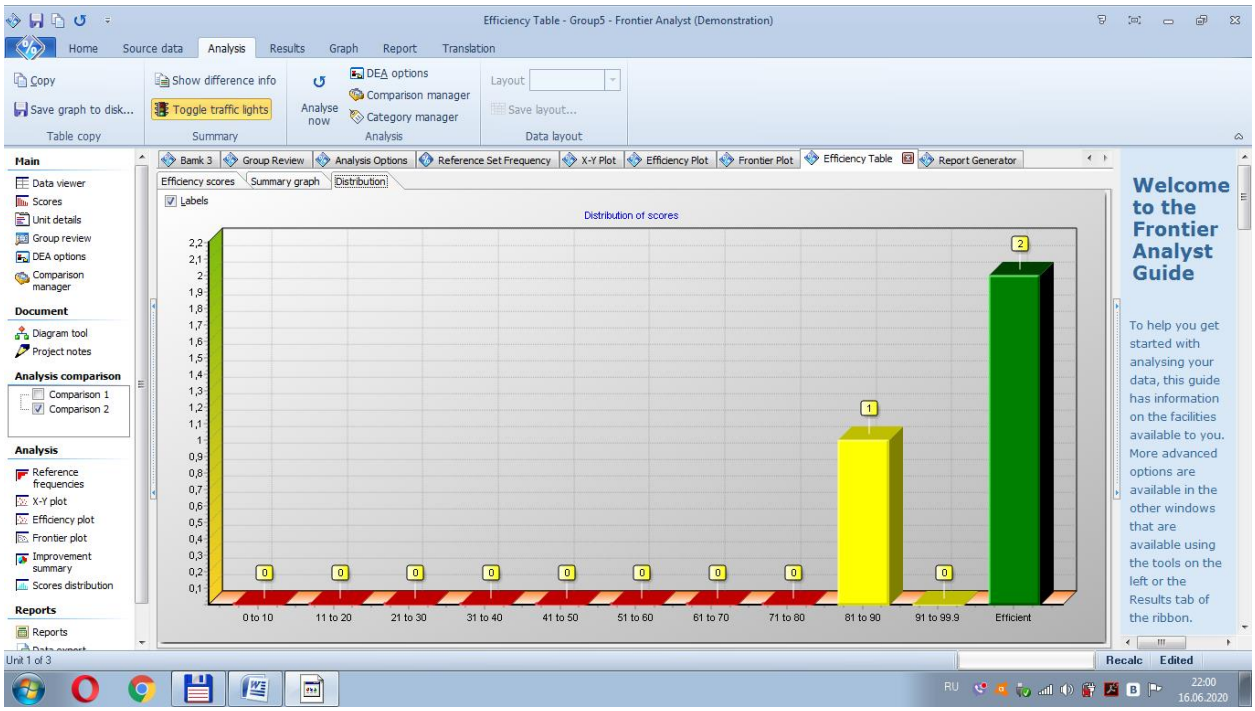


Рисунок Д.20 - Графік розподілу оцінок ефективності функціонування фінансового моніторингу п’ятої групи банків України станом на 2019 рік для CCR-моделі

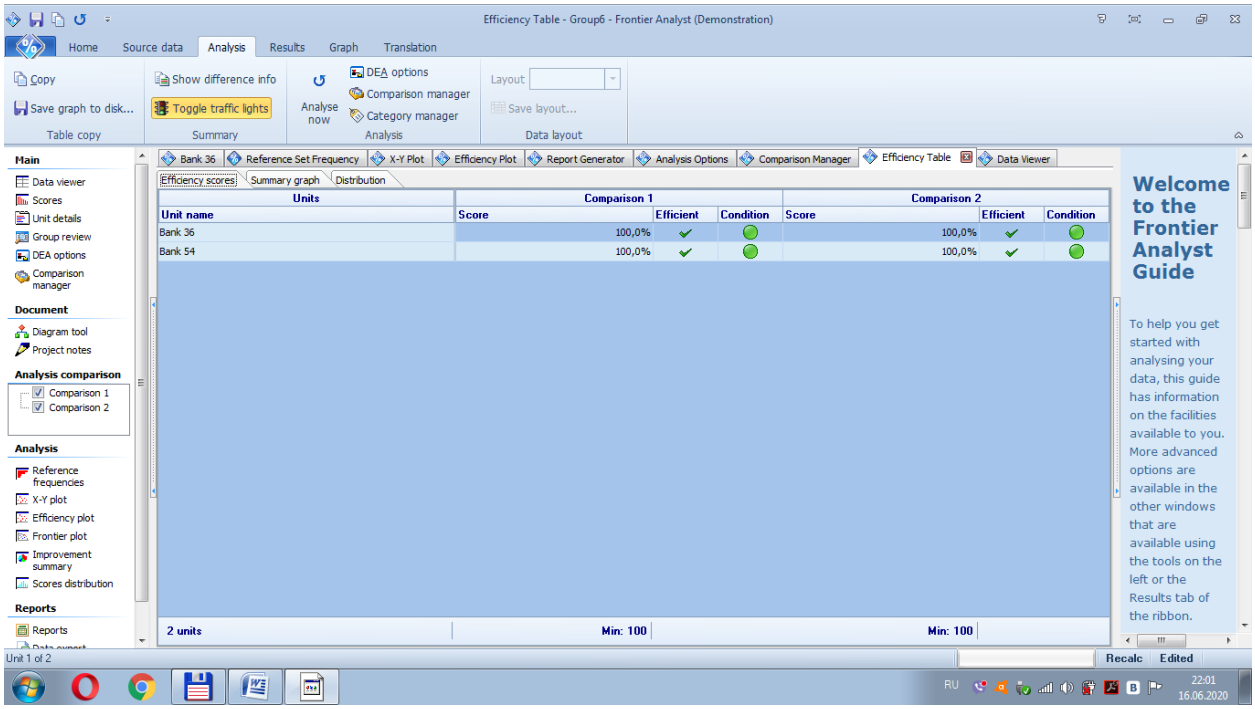


Рисунок Д.21 – Ефективність функціонування шостої групи банків України станом на 2019 рік для ВСС-моделі та для CCR-моделі

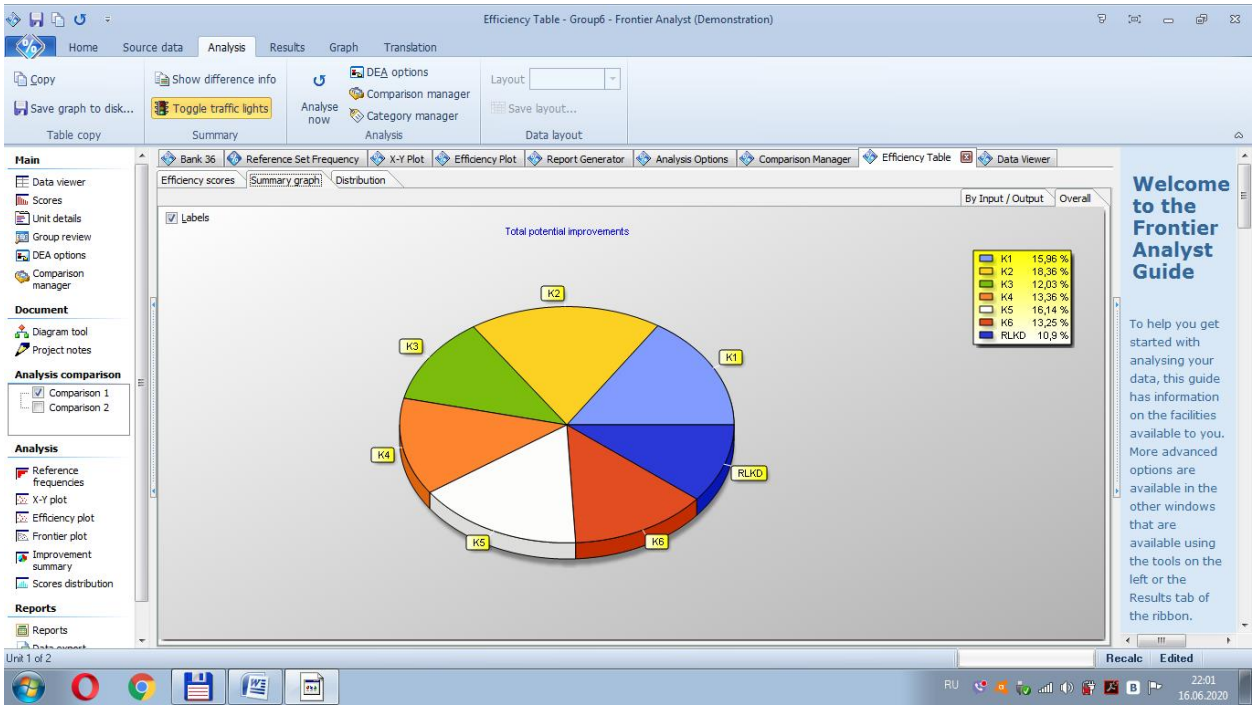


Рисунок Д.22 – Потенціал покращення ефективності функціонування фінансового моніторингу шостої групи банків України станом на 2019 рік для ВСС-моделі

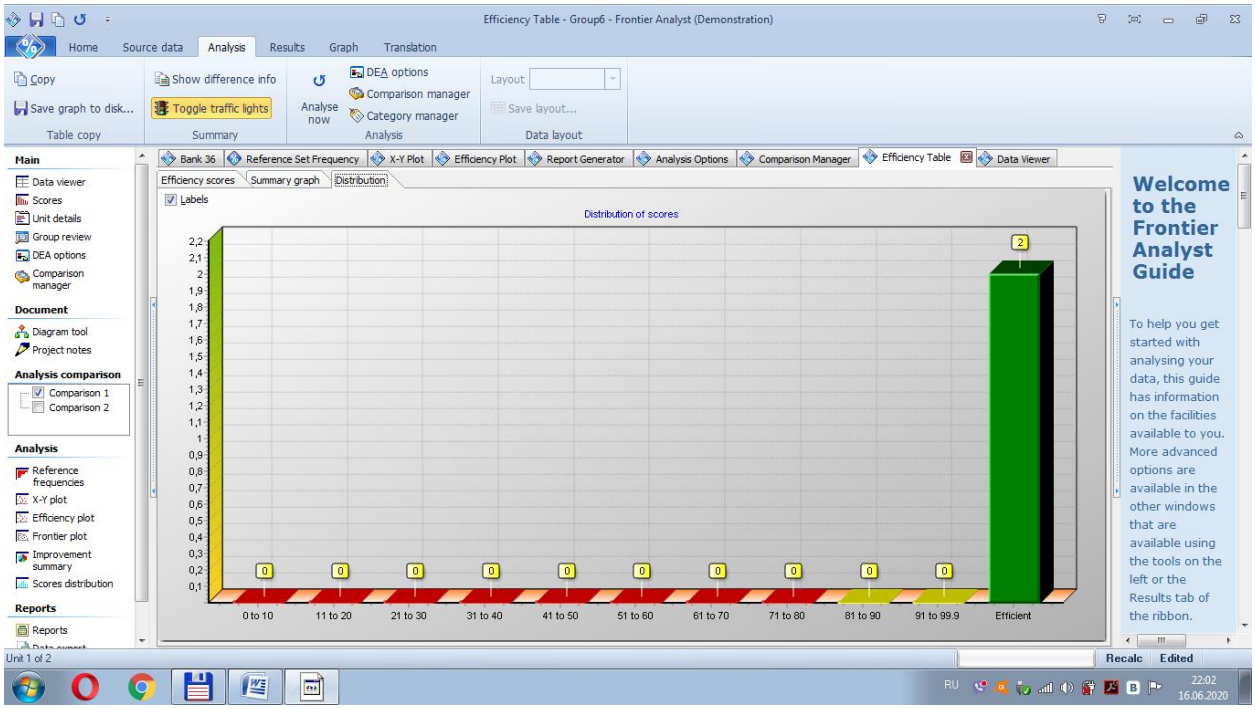


Рисунок Д.23 - Графік розподілу оцінок ефективності функціонування фінансового моніторингу шостої групи банків України станом на 2019 рік для ВСС-моделі

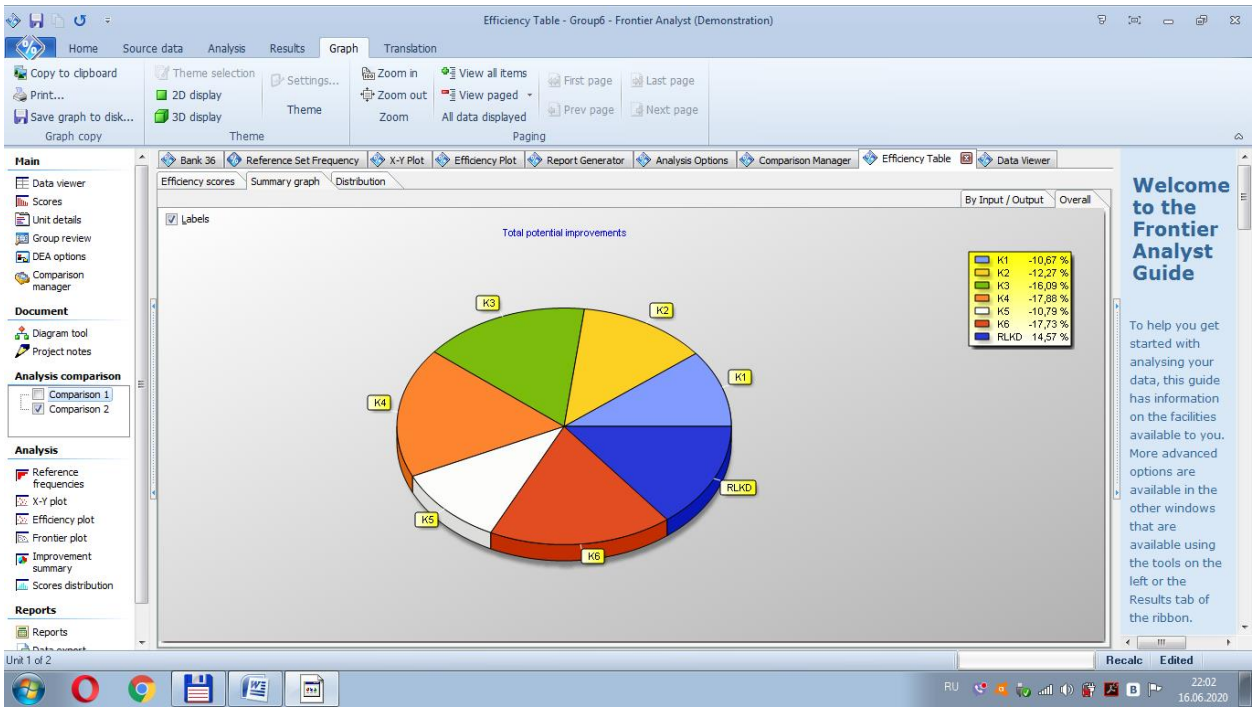


Рисунок Д.24 – Потенціал покращення ефективності функціонування фінансового моніторингу шостої групи банків України станом на 2019 рік для CCR-моделі

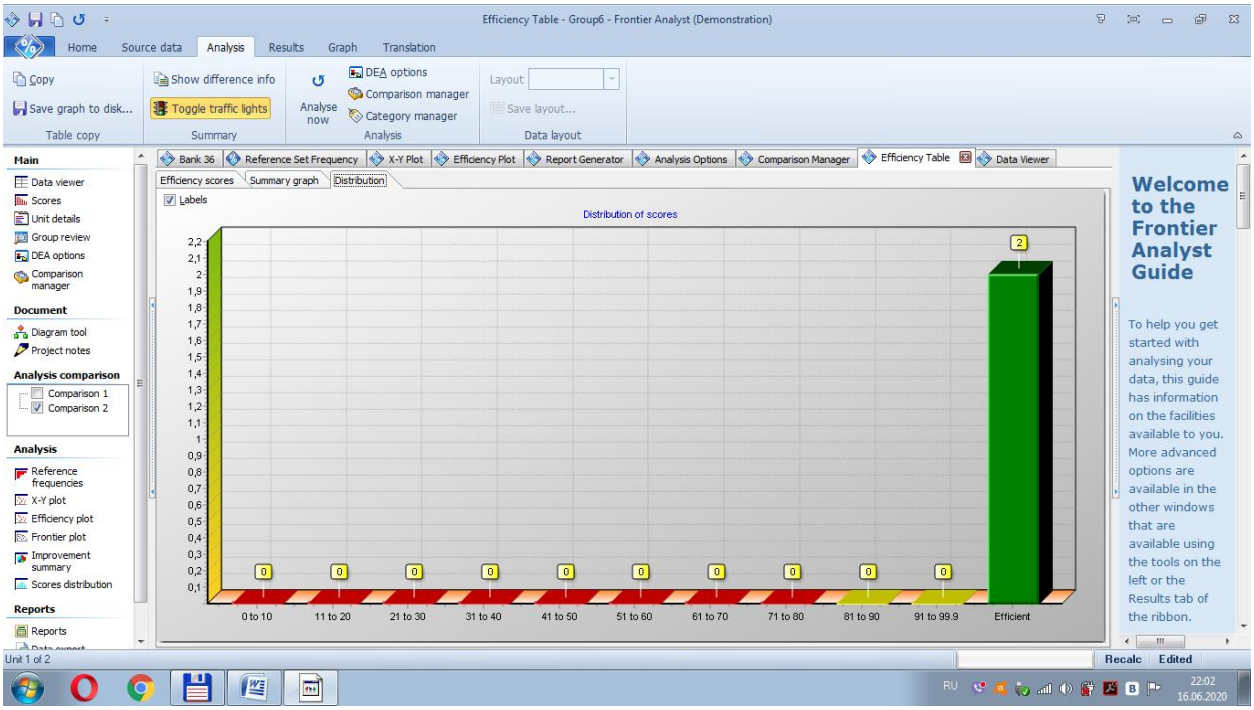


Рисунок Д.25 - Графік розподілу оцінок ефективності функціонування фінансового моніторингу шостої групи банків України станом на 2019 рік для CCR-моделі

Додаток Е

Аналіз результативності та потенціалу покращення фінансового моніторингу банків

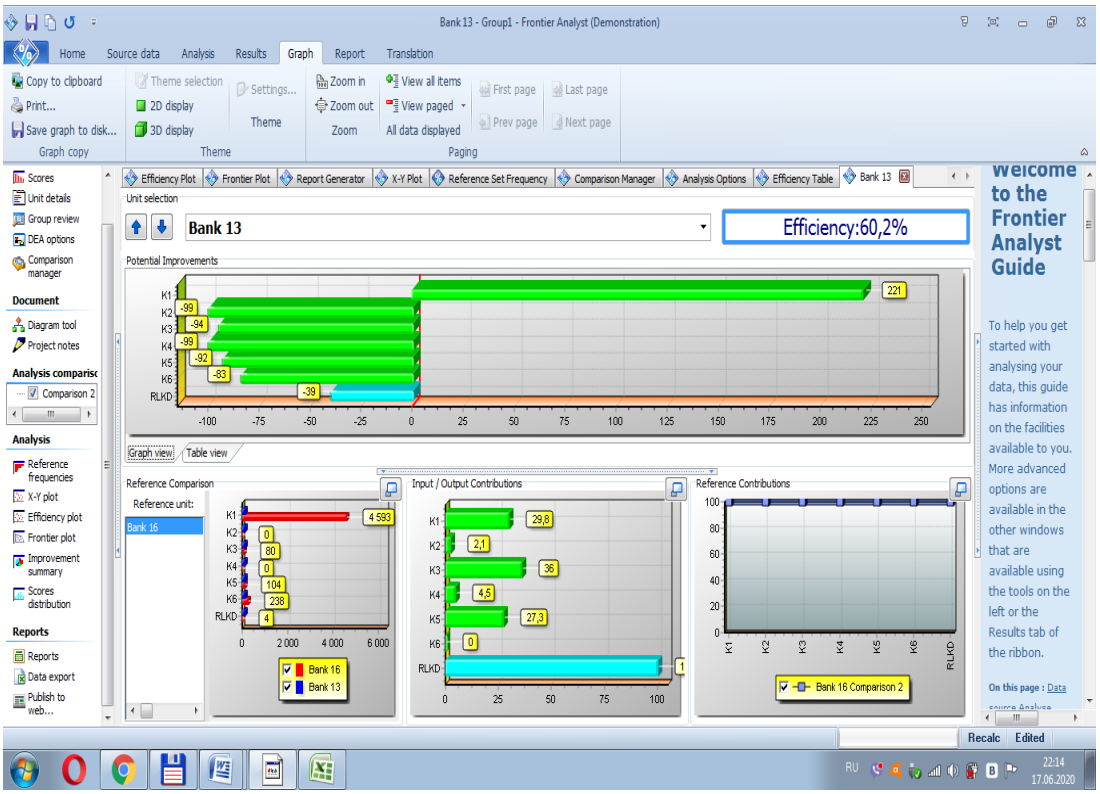
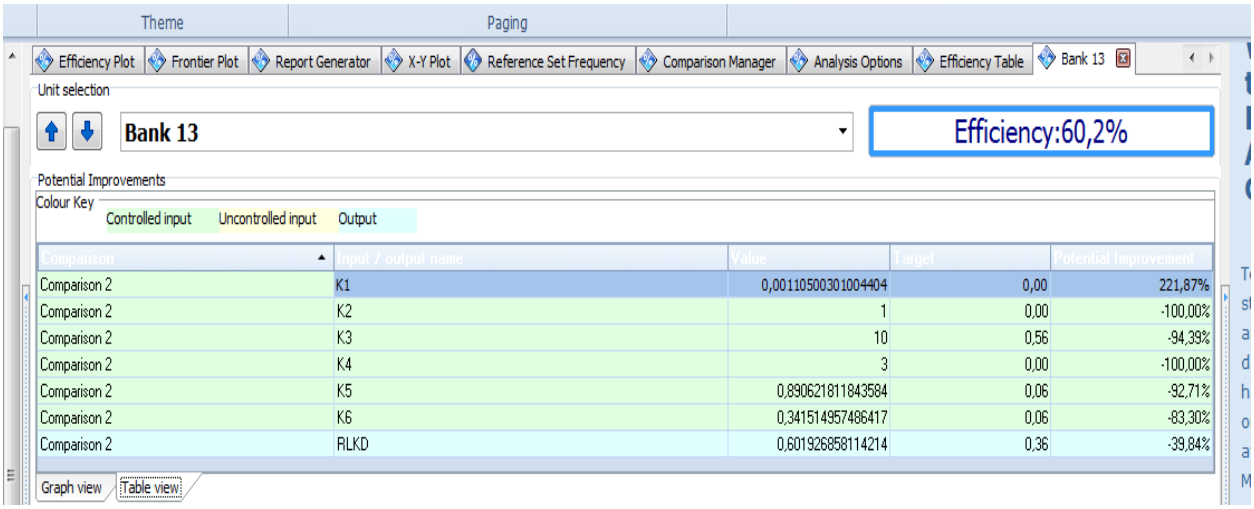


Рисунок Е.1 – Аналіз результативності та потенціалу покращення фінансового моніторингу Банку13 станом на 2019 рік для CCR-моделі



Comparison	Input / output name	Value	Target	Potential Improvement
Comparison 2	K1	0,00110500301004404	0,00	221,87%
Comparison 2	K2	1	0,00	-100,00%
Comparison 2	K3	10	0,56	-94,39%
Comparison 2	K4	3	0,00	-100,00%
Comparison 2	K5	0,890621811843584	0,06	-92,71%
Comparison 2	K6	0,341514957486417	0,06	-83,30%
Comparison 2	RLKD	0,601926858114214	0,36	-39,84%

Рисунок Е.2 - Потенціал покращення фінансового моніторингу Банку13 станом на 2019 рік для CCR-моделі

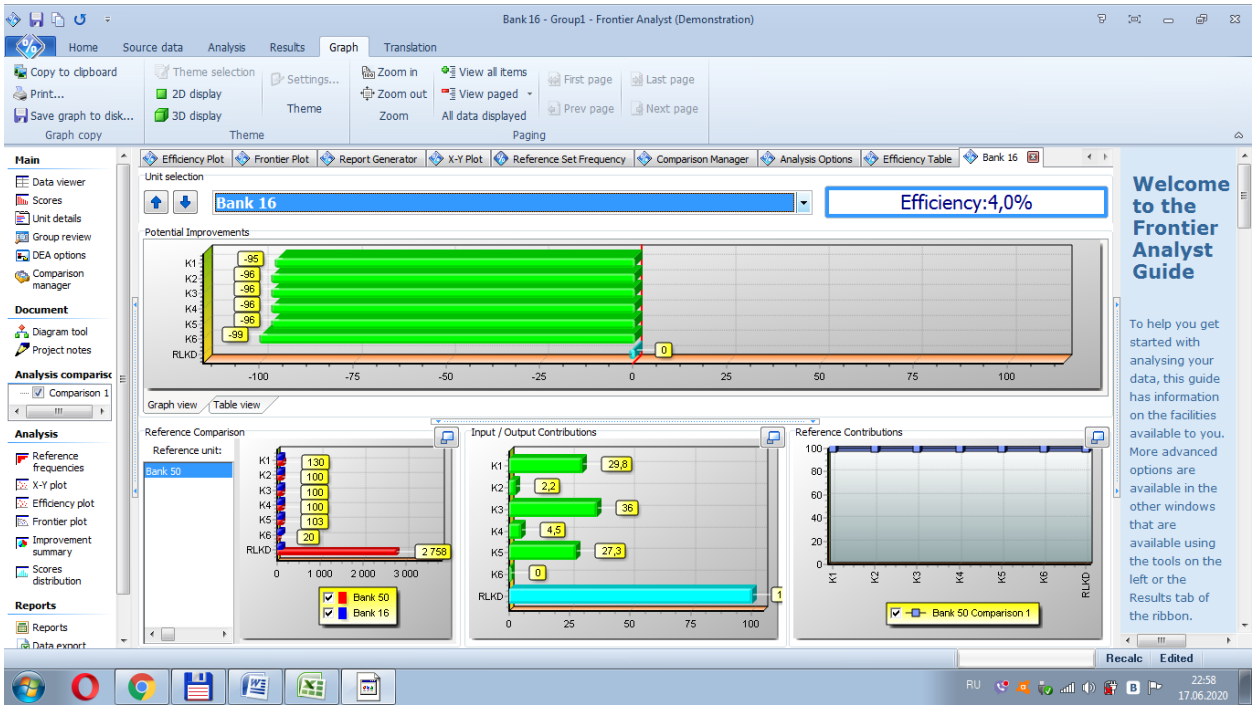
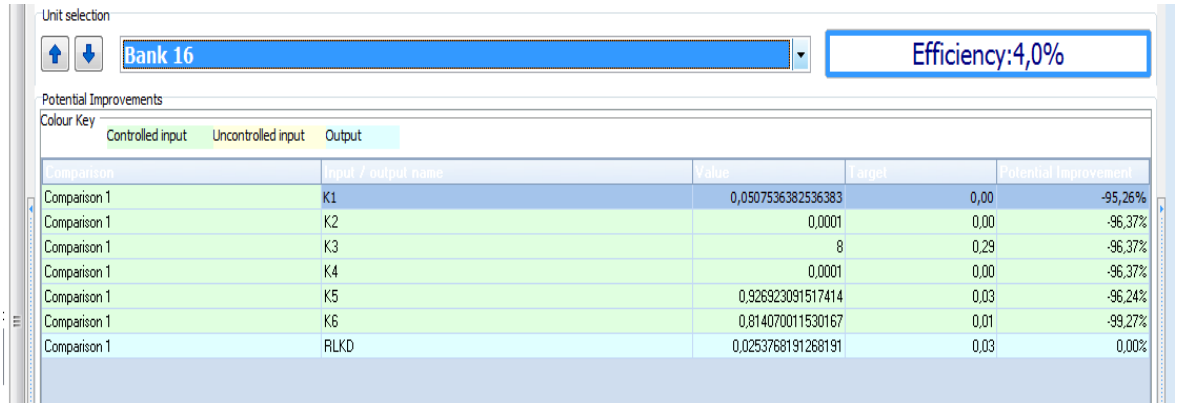


Рисунок Е.3 – Аналіз результативності та потенціалу покращення фінансового моніторингу Банку13 станом на 2019 рік



Comparison	Input / output name	Value	Target	Potential Improvement
Comparison 1	K1	0,0507536382536383	0,00	-95,26%
Comparison 1	K2	0,0001	0,00	-96,37%
Comparison 1	K3	8	0,29	-96,37%
Comparison 1	K4	0,0001	0,00	-96,37%
Comparison 1	K5	0,926923091517414	0,03	-96,24%
Comparison 1	K6	0,814070011530167	0,01	-99,27%
Comparison 1	RLKD	0,0253768191268191	0,03	0,00%

Рисунок Е.4 - Потенціал покращення фінансового моніторингу Банку13 станом на 2019 рік

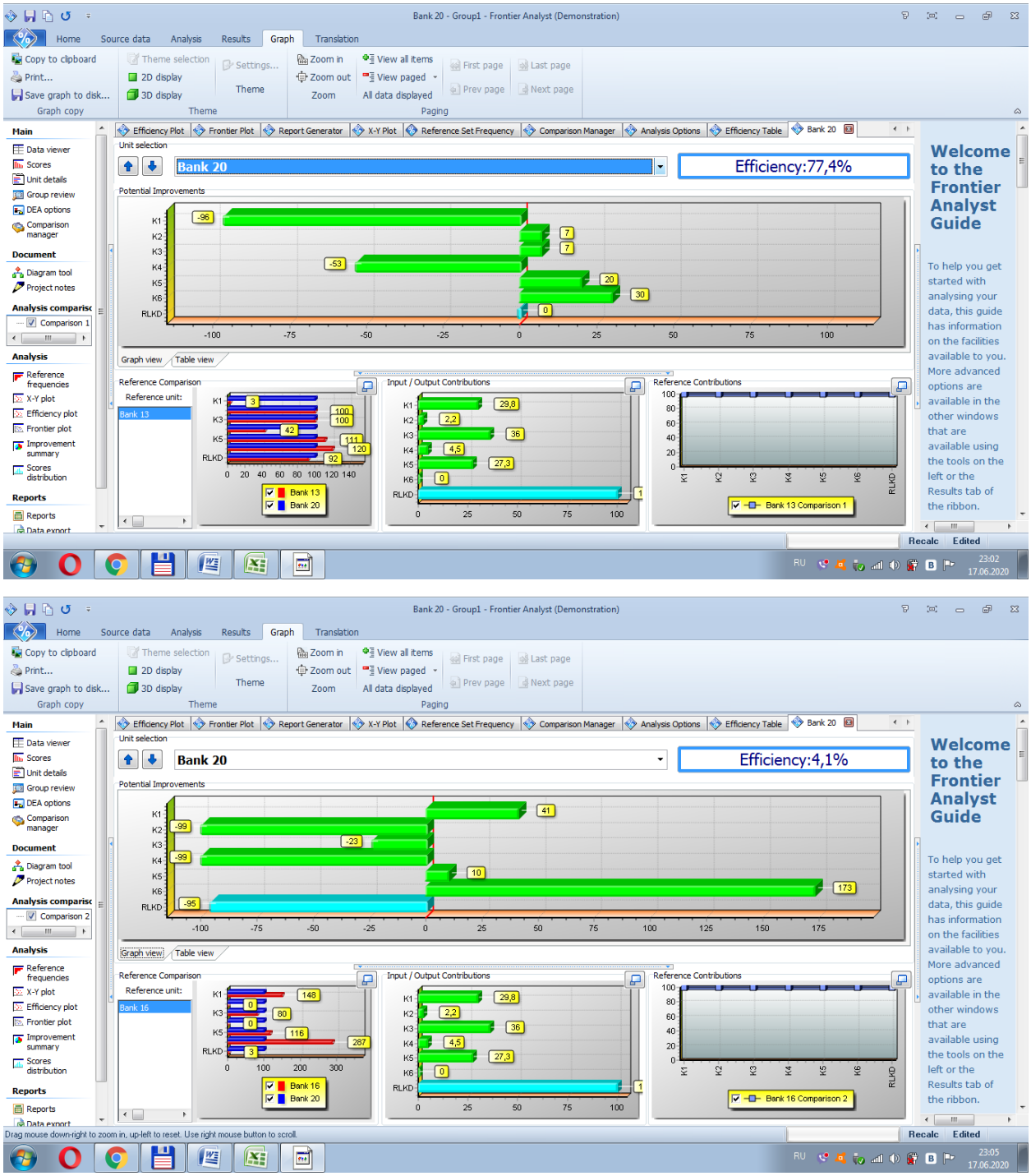


Рисунок Е.5 – Аналіз результативності та потенціалу покращення фінансового моніторингу Банку20 станом на 2019 рік

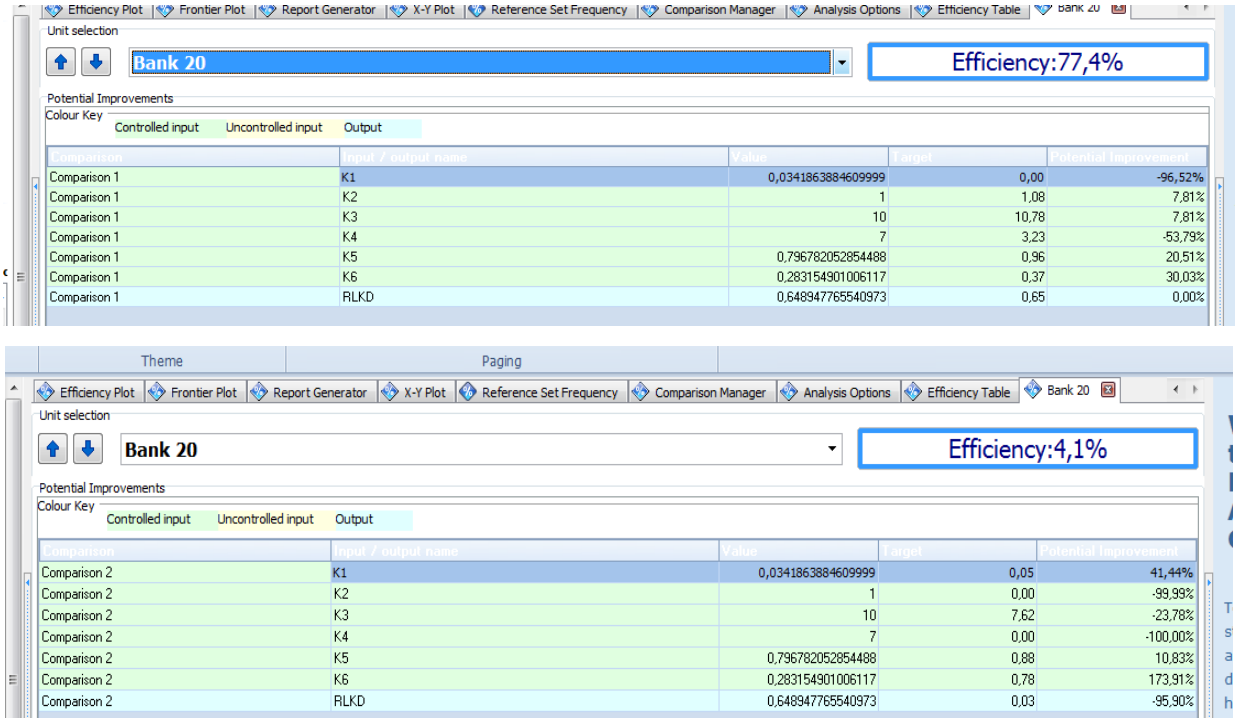


Рисунок Е.6 - Потенціал покращення фінансового моніторингу Банку20 станом на 2019 рік

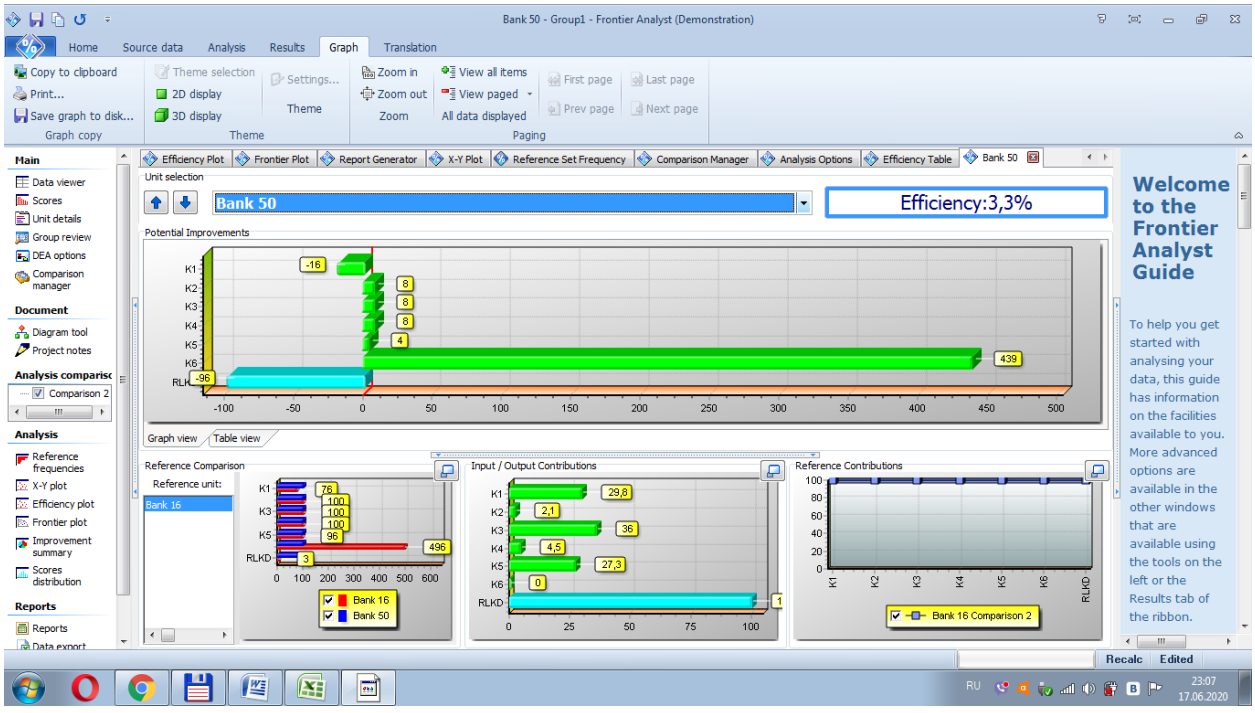


Рисунок Е.7 – Аналіз результативності та потенціалу покращення фінансового моніторингу Банку50 станом на 2019 рік

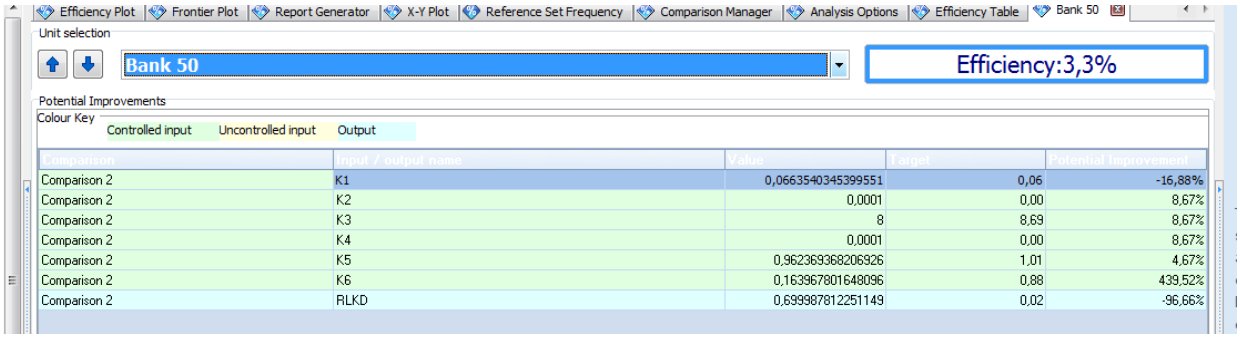


Рисунок Е.8 - Потенціал покращення фінансового моніторингу Банку50 станом на 2019 рік

Додаток Ж

Динаміка показників

Таблиця Ж.1 –Динаміка показників

Індикатор	Рік											
	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
Дефіцит державного бюджету, % до ВВП	1,4255	3,9342	5,9930	1,7737	3,6155	4,3400	4,5390	1,5538	2,2979	1,4118	1,9050	1,9558
Обсяг загального боргу, % до ВВП	19,1165	33,5681	40,0523	36,3991	36,6998	39,9118	69,3694	79,0619	80,9020	71,7798	60,9336	67,7056
Частки іноземного капіталу у статутному капіталі банків	36,7000	35,8000	40,6000	41,9000	39,5000	34,0000	32,5000	43,3000	51,2000	35,8000	28,1829	27,5144
Міжнародні резерви країни в місяцях імпорту	6,7000	4,4000	5,0000	3,6000	2,9000	2,4000	1,3000	3,2000	3,7000	3,6000	3,4000	3,1967
Рівень доларизації, частка іноземної валюти у грошовій масі, %	30,7300	31,7000	29,1900	30,3000	32,1000	27,1000	32,2000	32,2000	32,9000	31,9000	29,2000	29,0647
Контроль корупції	-0,8385	-1,0394	-1,0271	-1,0500	-1,0774	-1,1315	-0,9942	-0,9799	-0,8141	-0,7839	-0,8737	-0,8770
Політична стабільність та відсутність насильства / тероризму	0,0424	-0,3019	0,0131	-0,0704	-0,0923	-0,7773	-2,0208	-1,9618	-1,8565	-1,8702	-1,8262	2,5710

Продовження таблиці Ж.1

Індикатор	Рік											
	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
Верховенство права	-0,6813	-0,7588	-0,8076	-0,8188	-0,7829	-0,8045	-0,7910	-0,8136	-0,7663	-0,7114	-0,7178	-0,7212
Рівень інфляції, %	25,2265	15,8812	9,3729	7,9557	0,5687	-0,2389	12,0719	48,6999	13,9127	14,4383	10,9519	7,8867
Рівень безробіття,%	6,3629	8,8400	8,1000	7,8514	7,5288	7,1700	9,2700	9,1400	9,3500	9,5100	8,7994	9,0626
Індекс GINI	26,6000	25,3000	24,8000	24,6000	24,7000	24,6000	24,0000	25,5000	25,0000	26,0000	26,1000	26,0550
Рівень тіньової економіки, % ВВП	34,0000	39,0000	38,0000	34,0000	34,0000	36,0000	43,0000	40,0000	35,0000	32,0000	30,0000	29,6606