УДК 004.056.5;343.72:[336.7+351.853]
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

(проміжний)

Начальник НДЧ
канд. фіз.-мат. наук, с.н.с. Д.І. Курбатов

Керівник НДР
завідувач кафедри економічної кібернетики
доктор екон. наук, доцент О.В. Кузьменко

2018

Рукопис закінчений 26 грудня 2018 р.
Результати цієї роботи розглянуті науковою радою СумДУ,
протокол від 2018.12.27 №6

СПИСОК АВТОРІВ

Зав. кафедри економічної кібернетики, доктор екон. наук, доцент (керівник)	26.12.2018	Кузьменко О.В. (підрозділи 3.1, 3.2, 4.1, 4.2)
Професор кафедри економічної кібернетики, доктор екон. наук, професор	26.12.2018	Лєонов С.В. (підрозділи 1.1, 1.2, 4.2)
Доцент кафедри економічної кібернетики, канд. екон. наук, доцент	26.12.2018	Яровенко Г.М. (вступ, підрозділи 2.1, 2.2, 2.3, 4.1, 4.2, 4.3, висновки)
Доцент кафедри банківської справи, фінансів та страхування, канд. екон. наук, доцент	26.12.2018	Криклій О.А. (підрозділ 3.3)
Ст.викл. кафедри економічної кібернетики, канд. екон. наук	26.12.2018	Синявська О.О. (підрозділ 1.2, 1.3)
Аспірант кафедри економічної кібернетики	26.12.2018	Доценко Т.В. (підрозділи 3.1, 3.2, 4.2)
Студент кафедри економічної кібернетики	26.12.2018	Бояджян М.М. (підрозділ 2.1, 4.1)
Студент кафедри економічної кібернетики	26.12.2018	Клімов С.В. (підрозділ 4.3)

РЕФЕРАТ

Звіт про НДР: 199 с., 68 рис., 35 табл., 66 формул, 60 джерел, 3 додатки.

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

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.

Проаналізовано кіберзагрози як обєкт моделювання, проведено первинний та кластерний аналіз даних. Розроблено: математичні моделі ймовірності виникнення ознак кібершахрайських операцій із використанням Data Mining; інформаційні моделі виявлення ознак шахрайства з боку зовнішніх та внутрішніх шахраїв; математичні портрети потенційних жертв та шахраїв. Проведено кількісний аналіз збитків банківської системи в результаті кібершахрайств. Змодельовано кількісну оцінку рівня операційного ризику банку в сфері інформаційної безпеки. Розроблено: модель впливу макроекономічних факторів на формування схильності до шахрайства в банківській сфері; гравітаційну модель оцінки привабливості країни для легалізації кримінальних доходів; прототип автоматизованого модулю процесу виявлення шахрайських операцій з банківськими картками.

ЗМІСТ

ВСТУП

Банкоцентричність фінансового ринку, велика концентрація грошей, різноманітність on-line послуг, значне клієнтське поле – усе це робить банки привабливими для кіберзлочинців та призводить до «інтелектуалізації» банківських шахрайств. Це 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. Вирішення проблем боротьби з кіберзлочинністю та захисту прав споживачів фінансових послуг визнані міжнародними регуляторами та експертною спільнотою пріоритетними науковими проблемами світового рівня. 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.

Наявність неконтрольованих шахрайських операцій в банківській сфері, відсутність дієвих систем та інструментарію кібербезпеки щодо їх виявлення, відслідковування та попередження, сприяють зменшенню довіри до фінансових інституцій, порушенню законних прав споживачів фінансових послуг, що суттєво зменшує рівень фінансово-економічної безпеки України. 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.

За останні роки збитки від фінансових шахрайств зросли кардинально. Це має негативні наслідки для клієнтів фінансово-економічних агентів, які стають основним об’єктом шахрайств та втрачають кошти. Банкам шахрайство наносить також значну шкоду, що проявляється у втраті клієнтів, необхідності відшкодовувати вкрадені кошти, збільшенні коштів на модернізацію служби кібербезпеки та посилення захисних заходів. Поширеними є: шахрайства з банківськими картками, як найбільш простий, доступний та масовий спосіб платежу, що робить його можливим для підробки карток, пристроїв, що зчитують інформацію, викрадання даних з карт; Інтернет-шахрайства, коли Інтернет, який є платформою для клієнтів банку, через яку здійснюють онлайн-платежі, використовується шахраями як інструмент для крадіжки особистих фінансових даних клієнтів; соціальна інженерія, коли шахрай від імені банку дізнається у клієнта всю його інформацію та викрадає кошти з його рахунку. В арсеналі шахраїв досить багато способів шахрайства із залученням психологічних інструментів, комп’ютерних програм, різних технічних пристроїв, баз даних з інформацією про клієнтів тощо.

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 в процесі руху грошових коштів через банківську систему, що супроводжується застосуванням сучасних інформаційних технологій.

Предмет дослідження – методологічні та методичні підходи до побудови ефективної системи боротьби з банківськими кіберзлочинами на мікрорівні (банки) та макрорівні (забезпечення стійкості загальнодержавного фінансового кіберпростору).

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, 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 обєкт 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.

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.

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». 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».

За результатами наукового дослідження опубліковано 4 статті та 2 подано до друку у журналах, що індексуються БД Scopus та/або Web of Science, 7 статей у фахових виданнях, 12 тез доповідей у матеріалах міжнародних та вітчизняних конференцій. Подано до друку колективну монографію за тематикою НДР.

1 ДОСЛІДЖЕННЯ ВИДІВ КІБЕРЗАГРОЗ, ШАХРАЙСТВ, ТА ПРИЧИН, ЯКІ ОБУМОВЛЮЮТЬ ЇХ ПОЯВЛЕННЯ

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).

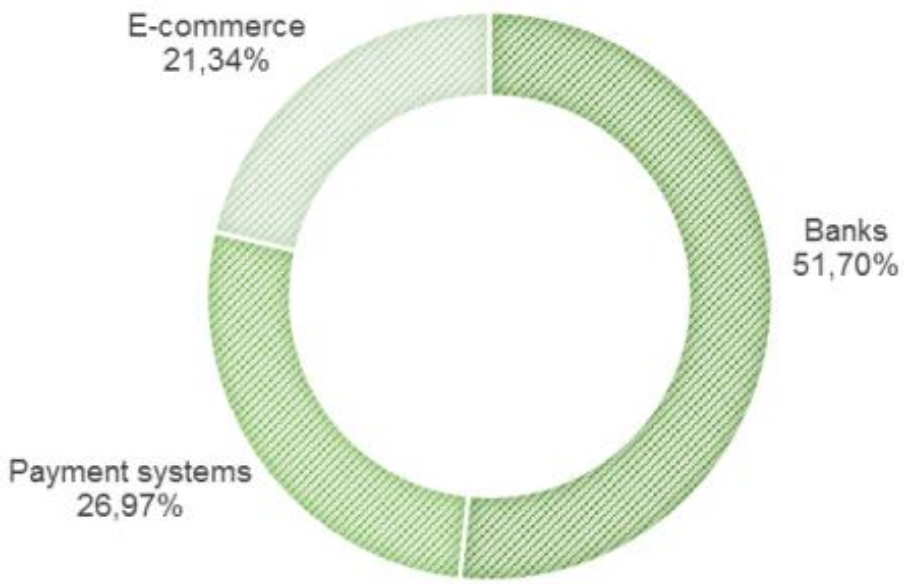


Рисунок 1.1 – Цільовий розподіл фішингу у фінансовому секторі

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).

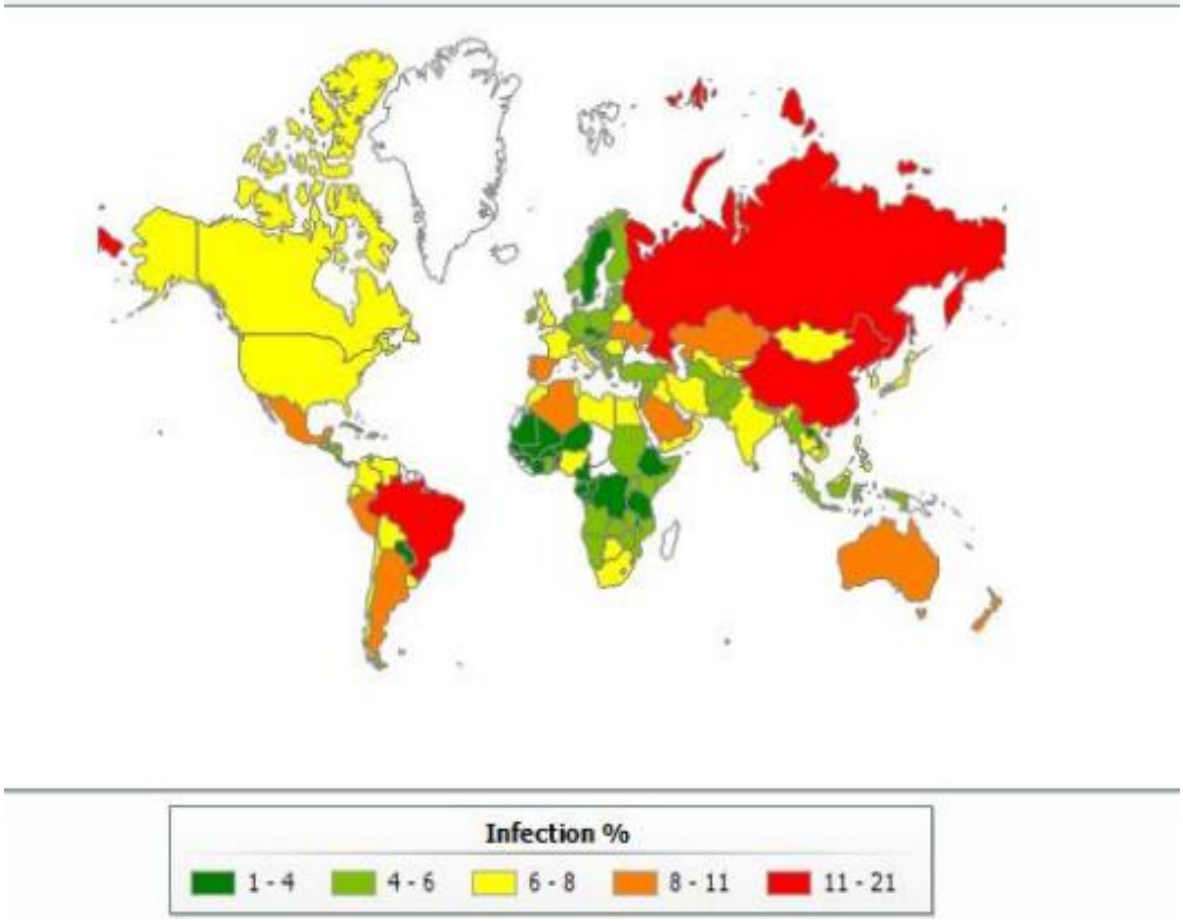


Рисунок 1.2 – Географічне розповсюдження фішингу – перший квартал 2017 року

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%).

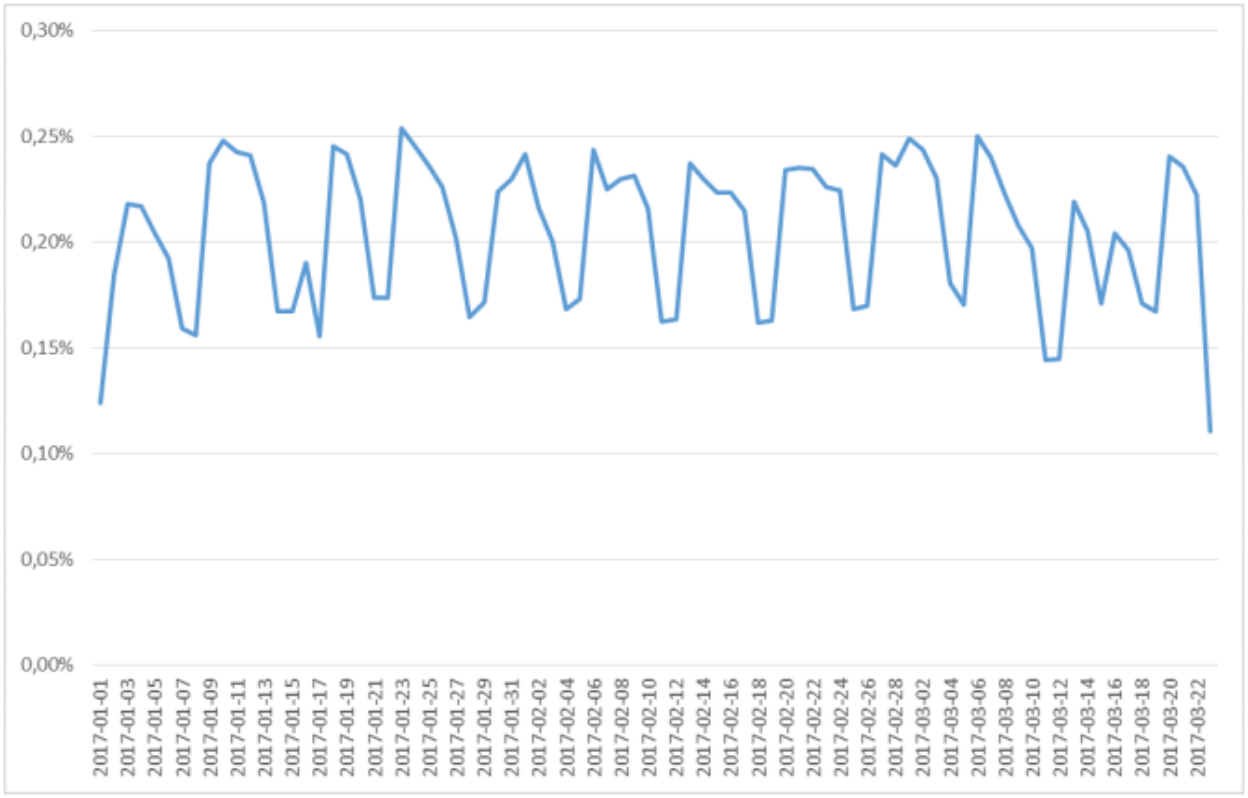


Рисунок 1.3 – Статистика фішингових атак – перший квартал 2017 року

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

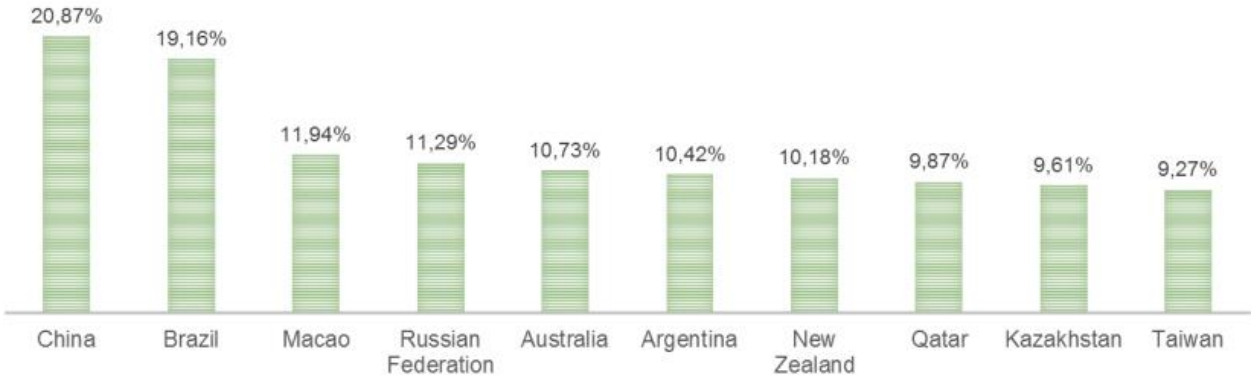


Рисунок 1.4 – Країни з найвищим рівнем жертв від фішингу

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 [10].

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].

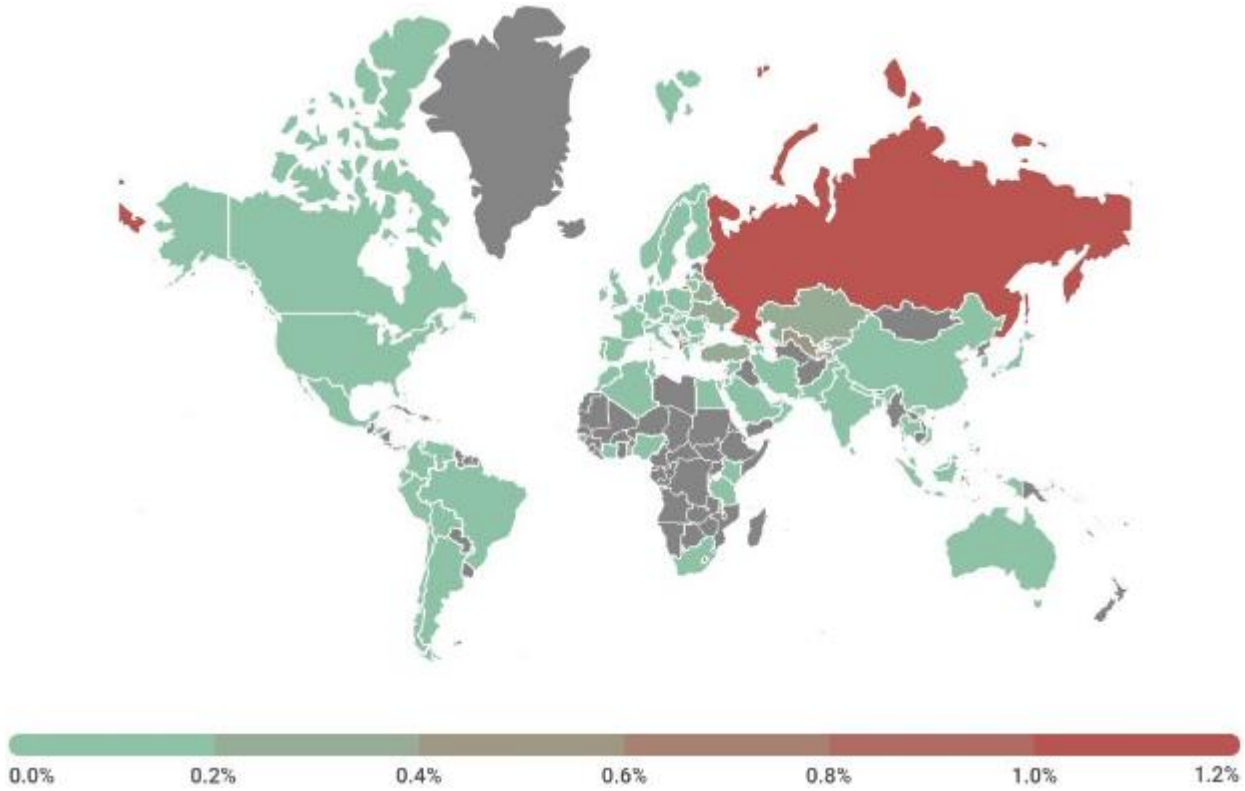


Рисунок 1.5 – Географія загроз мобільного банкінгу у 3-му кварталі 2017

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 даних з EMV-чіпа карти. Таким чином викрадається наступна інформація: 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 роботи банкомату і модифікації його 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.

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 «Х». 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 користувачав мобільного та інтернет-банкінгу банку «А».

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.

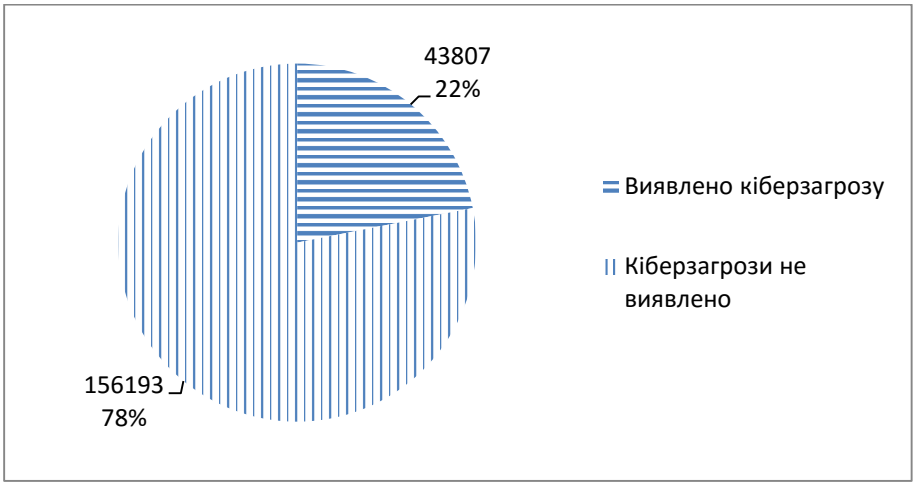


Рисунок 1.6 – Розподіл транзакцій за ймовірністю виникнення ознак кіберзагроз

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%).

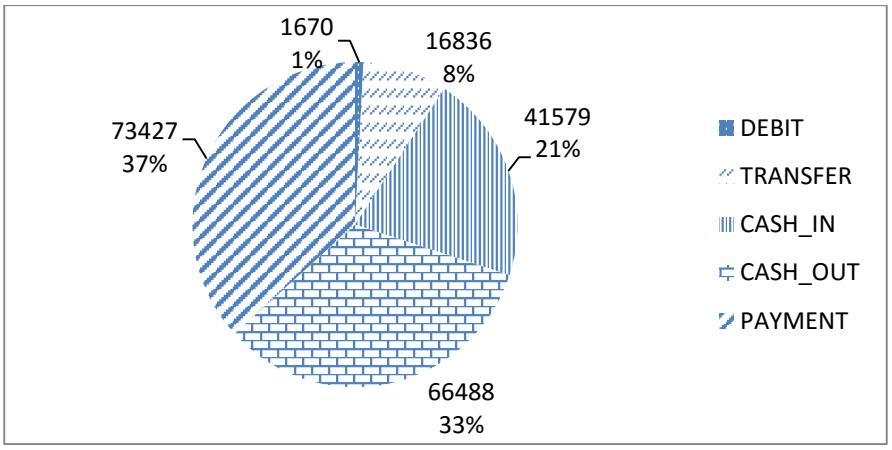


Рисунок 1.7 – Розподіл транзакцій за їх типами

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.

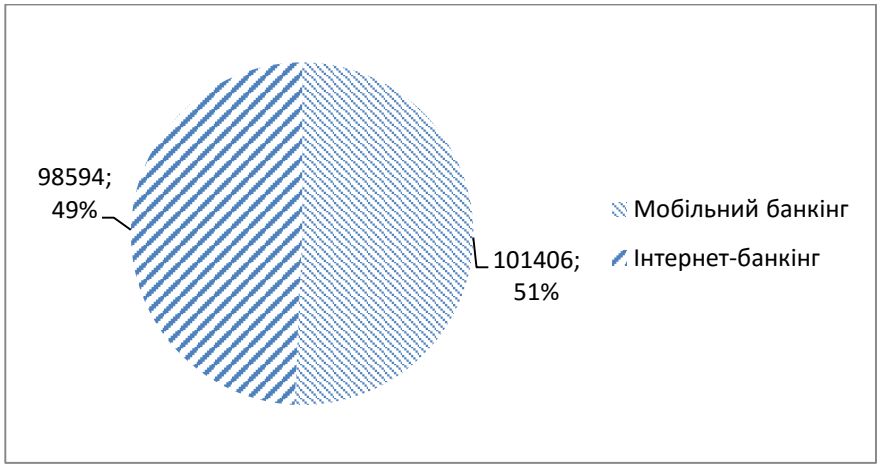


Рисунок 1.8 – Розподіл транзакцій за типами пристроїв, з яких вони виконувались

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.

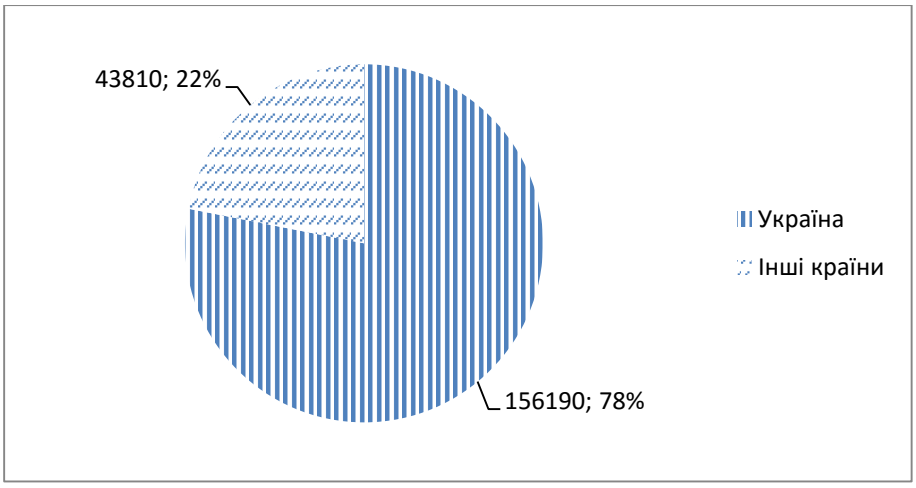


Рисунок 1.9 – Розподіл транзакцій за місцеположенням пристрою, з якого проводилась транзакція

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 [11].

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.

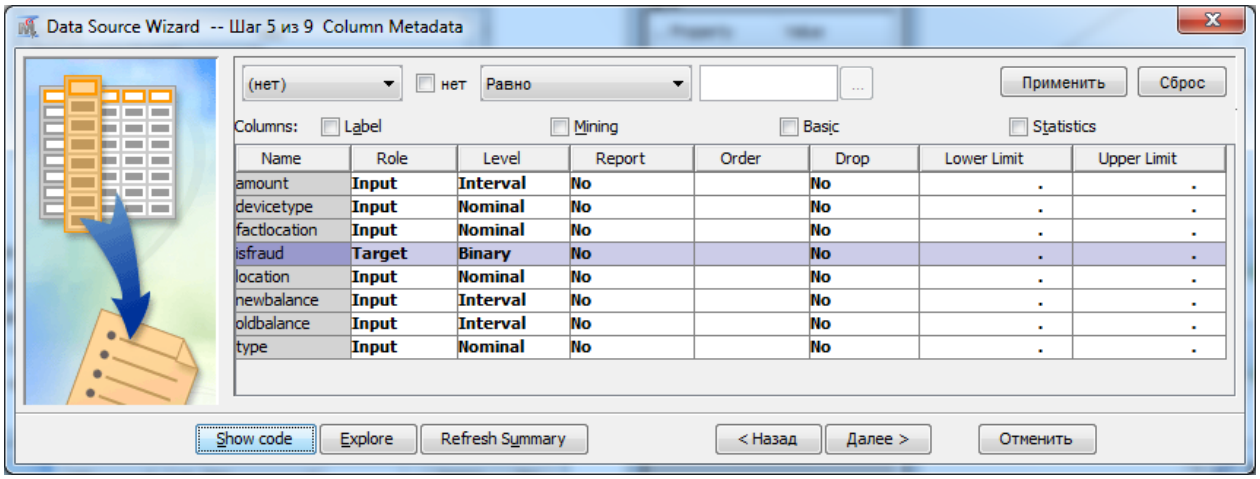


Рисунок 1.10 – Визначення ролей вхідних змінних

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).

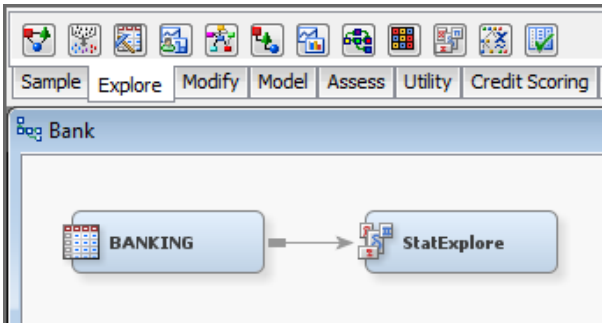


Рисунок 1.11 – Об’єднання інструмента StatExplore з джерелом даних

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).

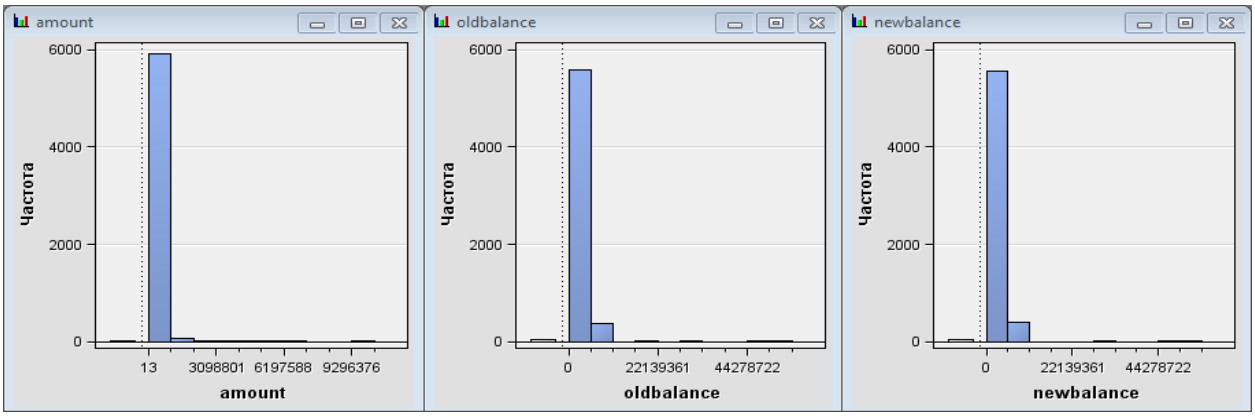


Рисунок 1.15 – Перевірка нормального закону розподілу у вхідних інтервальних змінних

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).

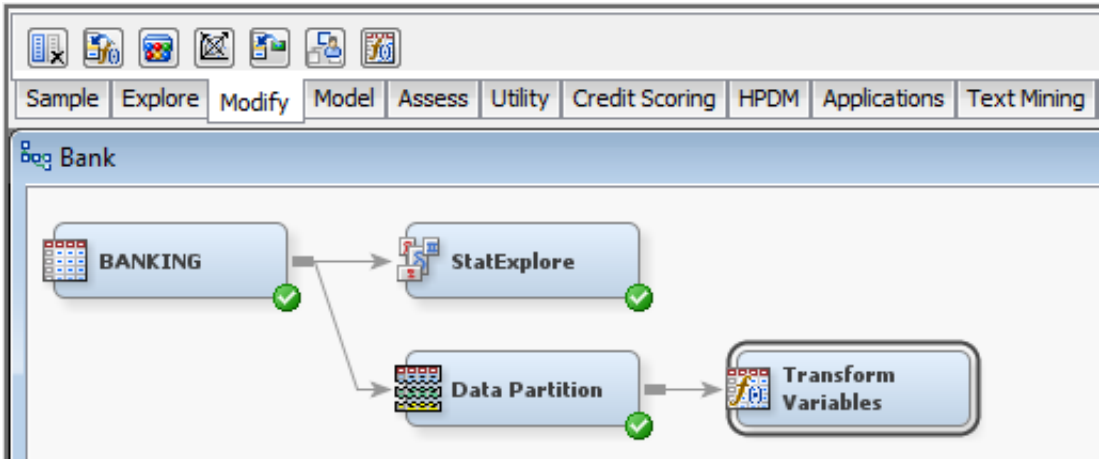
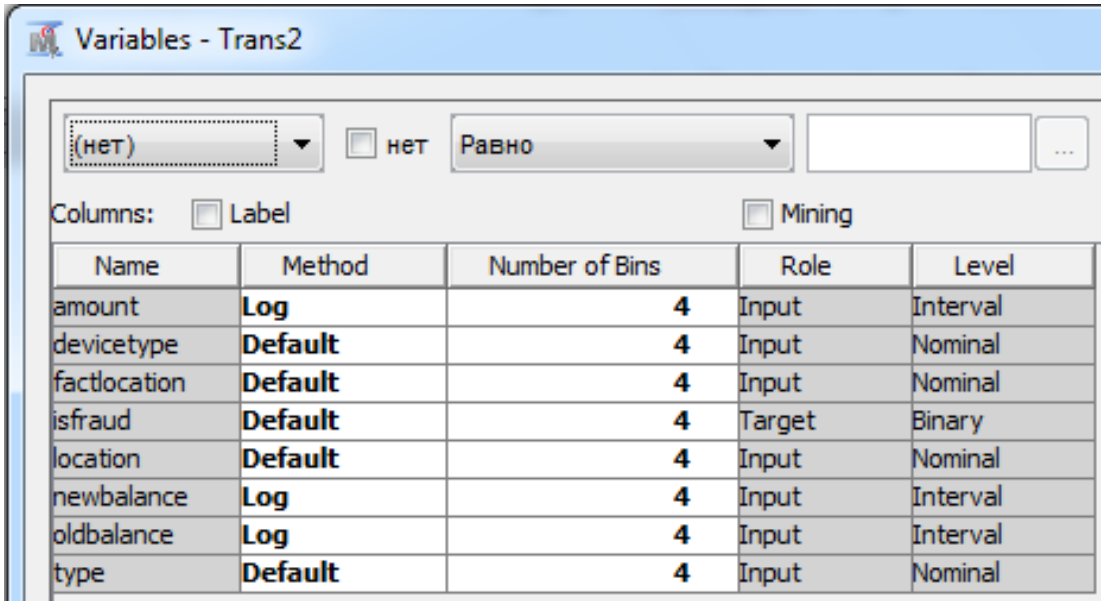


Рисунок 1.16 – Додавання вузла Transform Variables в робочу область

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



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.

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 [12].

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 [13].

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 [14].

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 [12].

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 [15].

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).

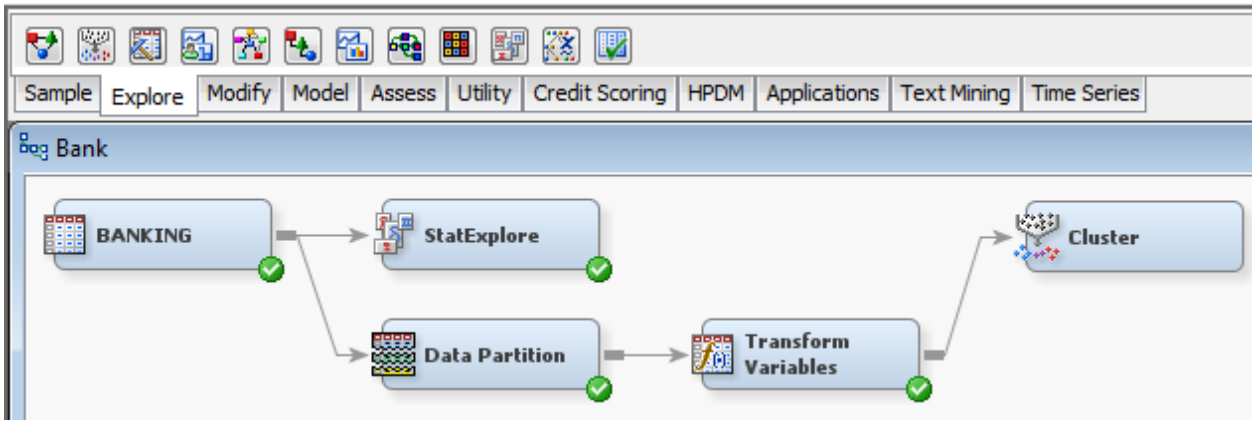


Рисунок 1.18 – Додавання інструмента Cluster в робочу область діаграми

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.

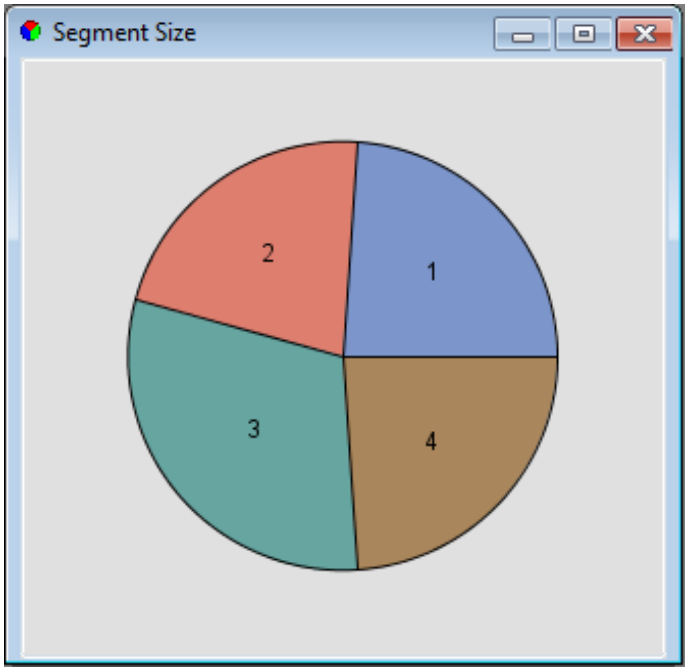


Рисунок 1.19 – Розподіл даних на кластери в пакеті SAS Enterprise Miner

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).

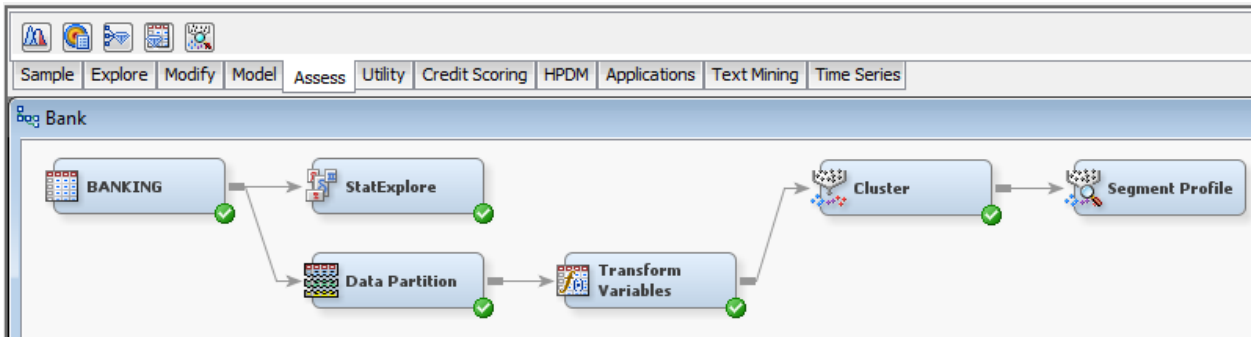


Рисунок 1.20 – Додавання інструменту Segment Profile в область діаграми

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.

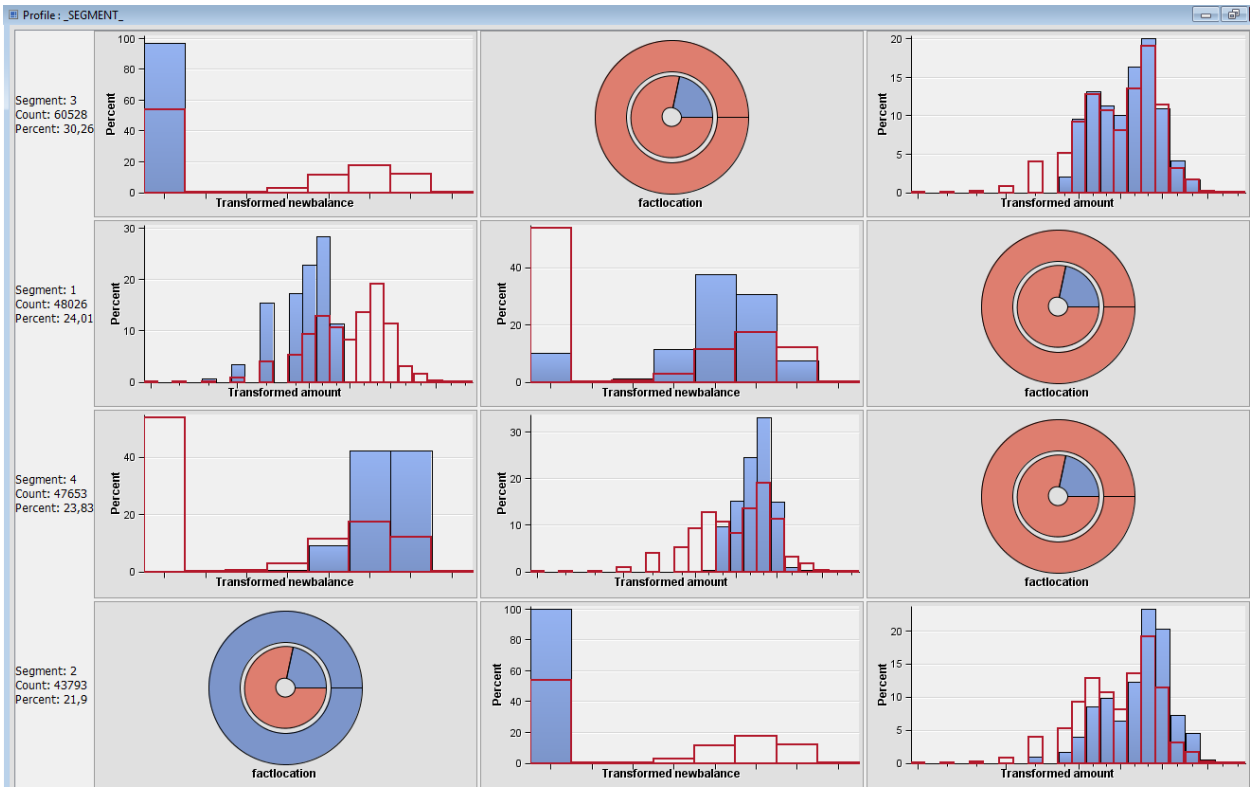


Рисунок 1.21 – Профільний аналіз кластерів в пакеті SAS Enterprise Minner

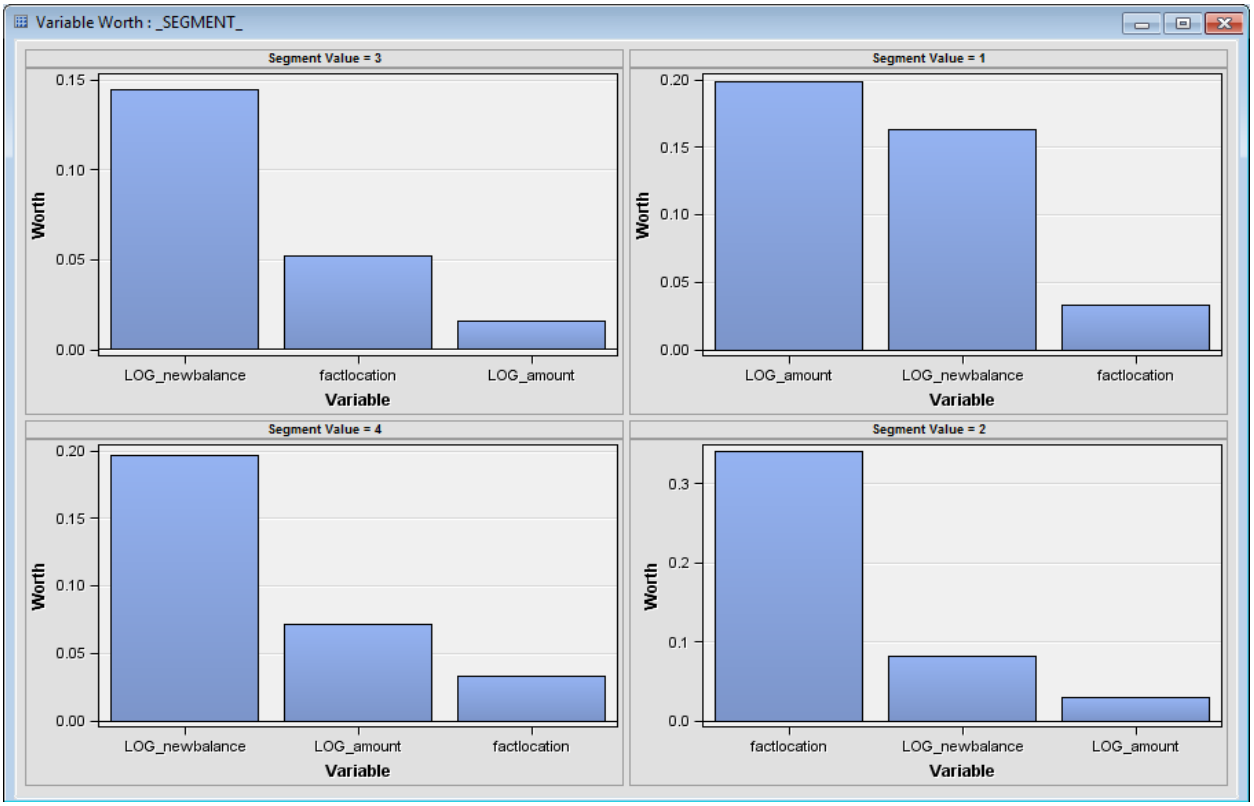


Рисунок 1.22 – Вага кожної змінної у формуванні відповідного кластеру в пакеті SAS Enterprise Miner

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.

2 РОЗРОБКА МОДЕЛЕЙ ЙМОВІРНОСТІ ВИНИКНЕННЯ ШАХРАЙСЬКИХ ОПЕРАЦІЙ, ЯК ОДНОГО ІЗ РІЗНОВИДІВ КІБЕРЗАГРОЗ, В КОМЕРЦІЙНИХ БАНКАХ

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 кіберзагрози, 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, дані та висунуті гіпотези було розроблено концептуальну модель виявлення ознак кіберзагроз в транзакціях користувачів мобільного та інтернет-банкінгу (рис. 2.1).

Рисунок 2.1 – 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 2.2. [16]

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 2.2 – 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 2.1):

$$P = \frac{1}{1 + E^{-(-3{,}4+5{,}11X_{3.2}-0{,}89X_5+0{,}87X_6)}} \qquad (2.1)$$

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. 2.3). [16]

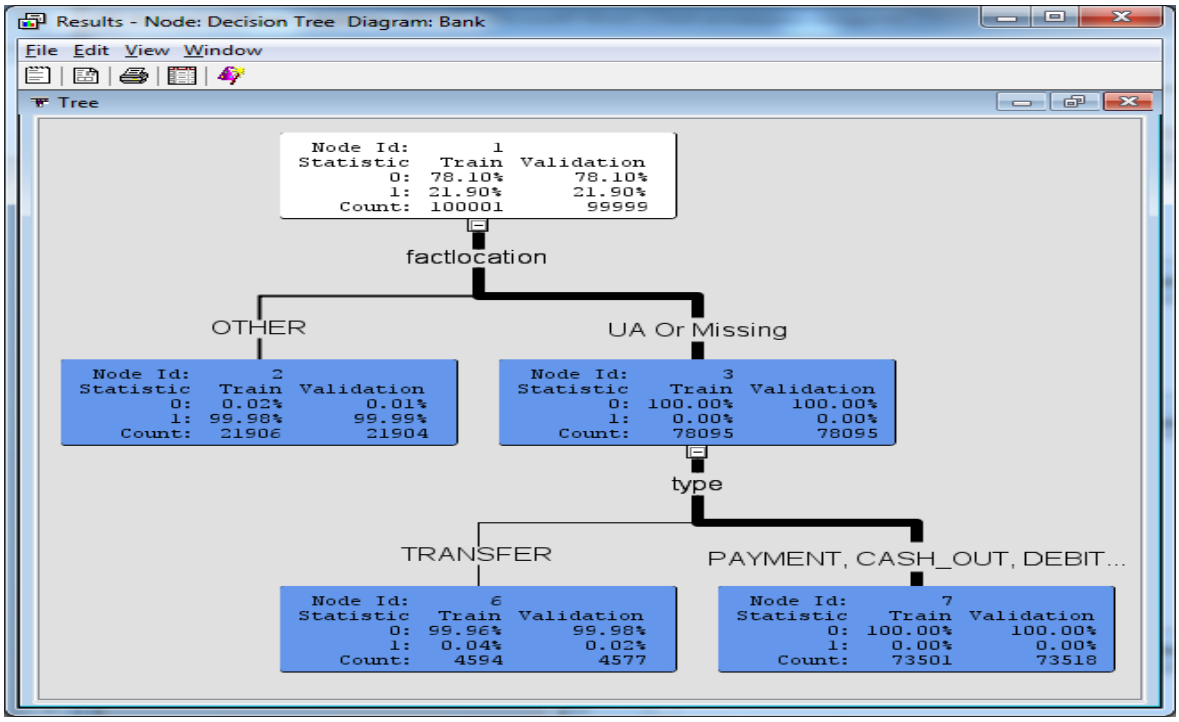


Рисунок 2.3 – Результат побудови дерева рішень

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. 2.4). [16]

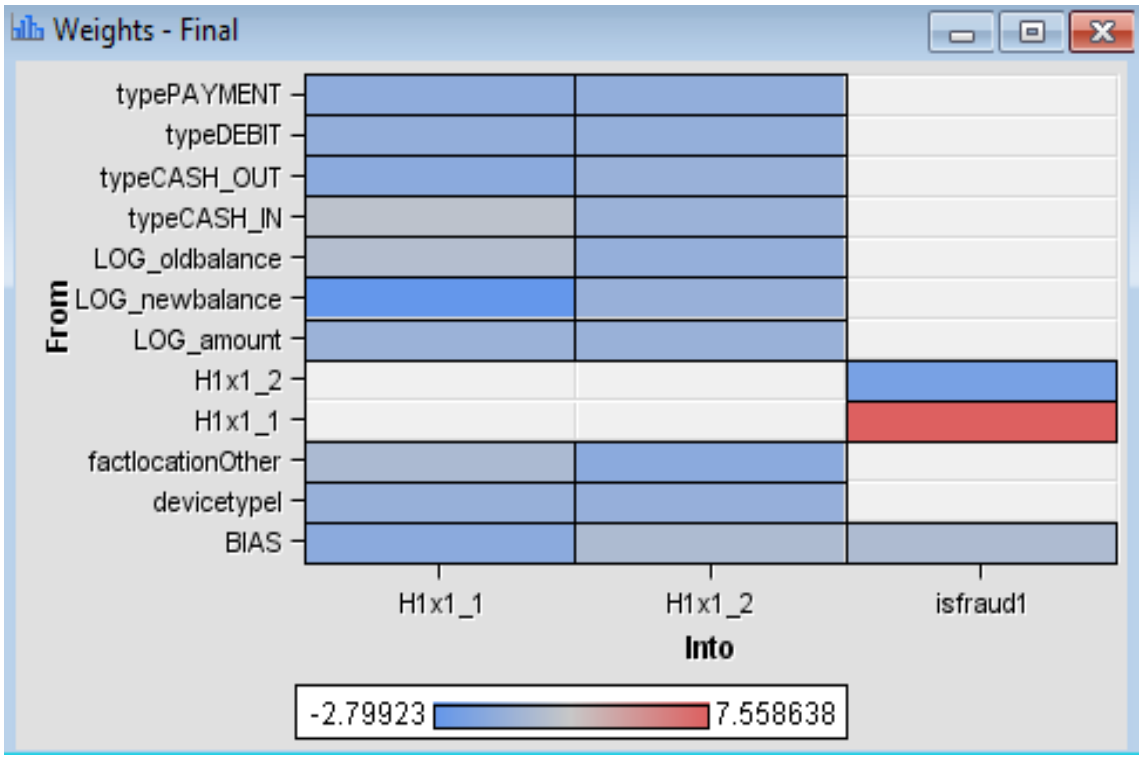


Рисунок 2.4 – Архітектура побудованої нейронної мережі

Отримані вагові коефіцієнти нейронної мережі представлено на рисунку 2.5.

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 2.5 – Вагові коефіцієнти нейронної мережі

Математичну інтерпретацію отриманої нейронної мережі наведено у формулах 2.2-2.4:

$$Y = 1{,}02 + 7{,}56 \cdot H_1 x_1 - 1{,}76 \cdot H_2 x_2; \quad (2.2)$$

$$H_1 = \tanh(-0{,}78 + 0{,}04 \cdot LOGX_1 - 0{,}13 \cdot X_{2.2} + 0{,}87 \cdot X_{3.2} - 2{,}8 \cdot LOGX_5 + 1{,}36 \cdot LOGX_6 + 1{,}78 \cdot X_{7.1} - 0{,}76 \cdot X_{7.2} - 0{,}35 \cdot X_{7.3} - 0{,}58 \cdot X_{7.4}); \quad (2.3)$$

$$H_2 = \tanh(0{,}99 - 0{,}05 \cdot LOGX_1 - 0{,}23 \cdot X_{2.2} - 0{,}78 \cdot X_{3.2} - 0{,}11 \cdot LOGX_5 - 0{,}25 \cdot LOGX_6 + 0{,}05 \cdot X_{7.1} - 0{,}07 \cdot X_{7.2} - 0{,}3 \cdot X_{7.3} - 0{,}4 \cdot X_{7.4}). \quad (2.4)$$

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. 2.1). [16]

Таблиця 2.1 – 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 2.1, 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 2.6 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.

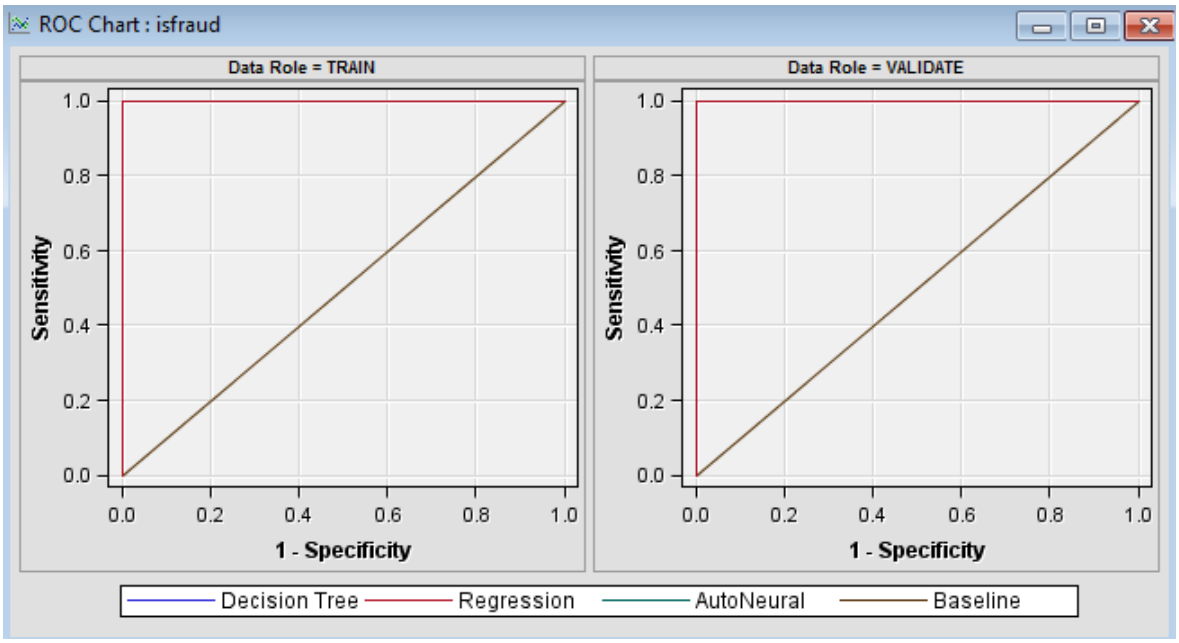


Рисунок 2.6 – ROC-криві дерева рішень, регресії та нейронної мережі

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. 2.2).

Таблиця 2.2 – 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 2.2 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.

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. [17]

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. [18]

Так, розподіл шахрайств від першої сторони за видами фінансових продуктів в Великій Британії за 2015-2018 роки представлений на рисунку 2.7. [19]

Шахрайства від першої сторони найбільш ймовірно припадають на шахрайства з поточними банківськими рахунками (Current Accounts) та іпотеку (Mortgages) (рис. 2.7). 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. [20]

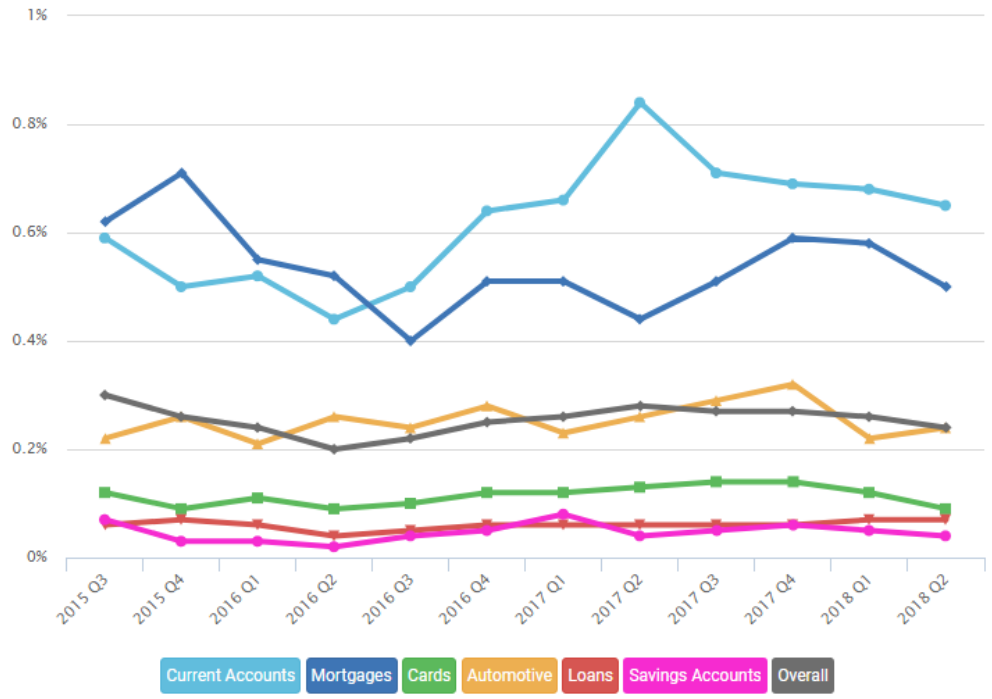


Рисунок 2.7 – Розподіл шахрайств від першої сторони за видами фінансових продуктів в Великій Британії за 2015-2018 роки

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. 2.8). 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.

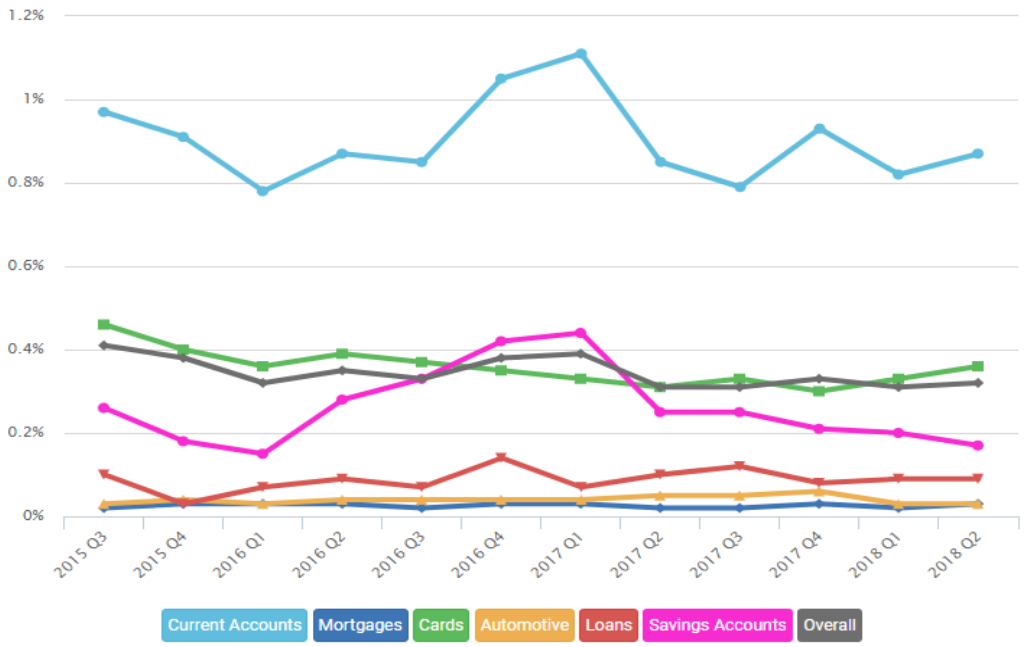


Рисунок 2.8 – Розподіл шахрайств від третьої сторони за видами фінансових продуктів у Великій Британії за 2015-2018 роки

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 2.9. 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. 2.9) 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.

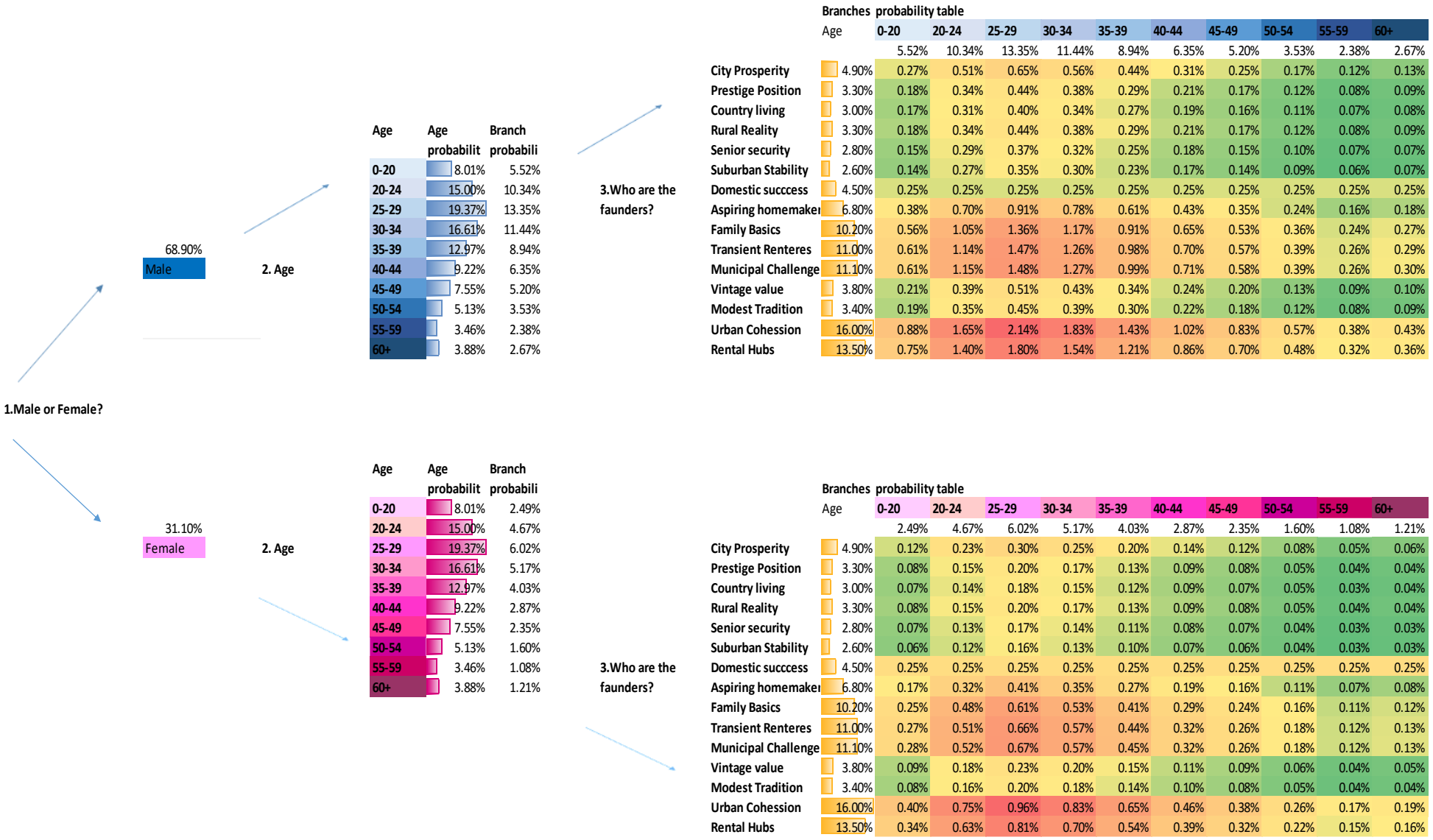


Рисунок 2.9 – Модель портрету потенційного шахрая від першої сторони за ознаками статі, віку та соціальної групи [21]

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. 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 2.10. 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.

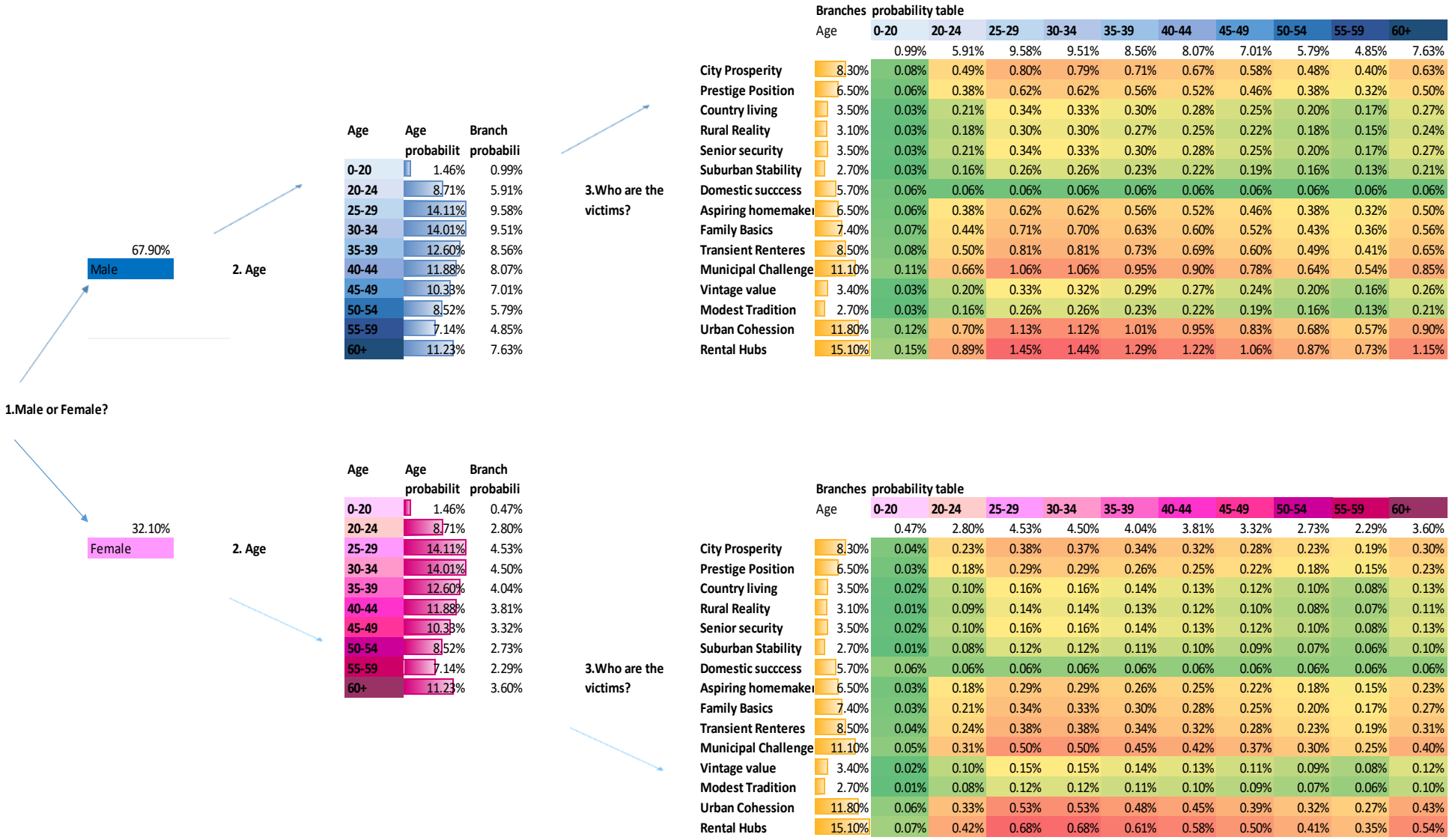


Рисунок 2.10 – Модель портрету потенційної жертви шахрайства від третьої сторони за ознаками статі, віку та соціальної групи [21]

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. 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.

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. 2.11).

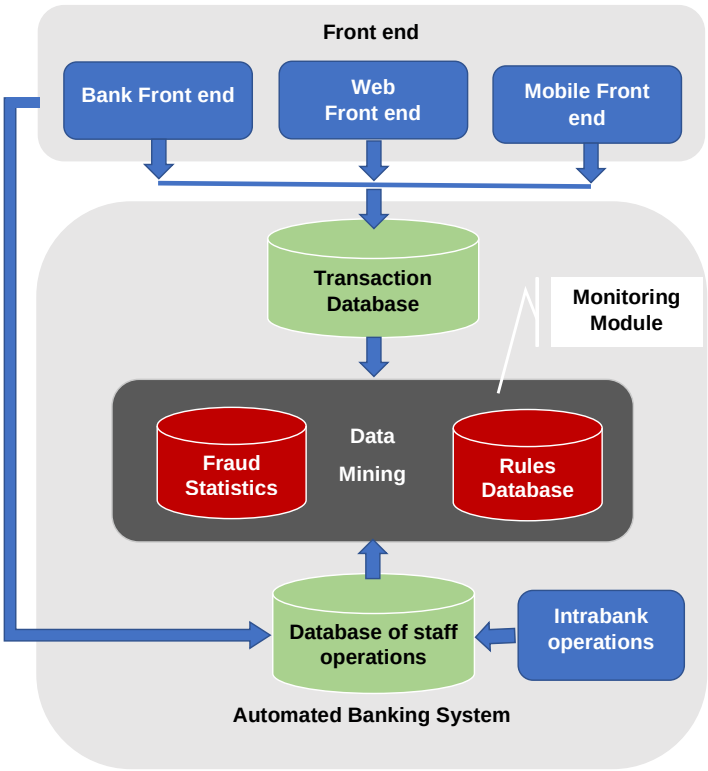


Рисунок 2.11 – Архітектура автоматизованої банківської системи з урахуванням модулю моніторингу

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 2.11). 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 2.12). [22]

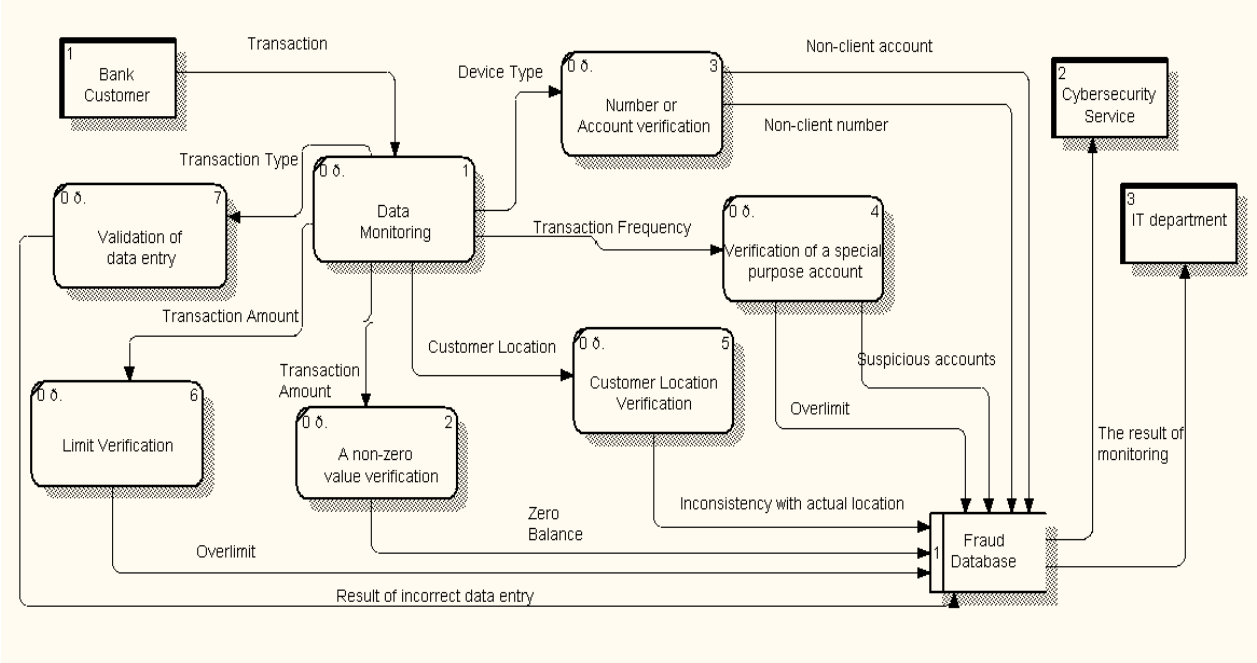


Рисунок 2.12 – Інформаційна модель виявлення ознак шахрайств клієнтів

Модель побудовано у нотації DFD (data flow diagrams) [23], 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 2.12 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 2.12) розроблено схему процесу здійснення операції клієнтом з урахуванням її перевірки на ознаки шахрайства у нотації BPMN 2.0 (Business Process Model and Notation) [24] із використанням програмного забезпечення “Bizagi Modeller” (рисунок 2.13).

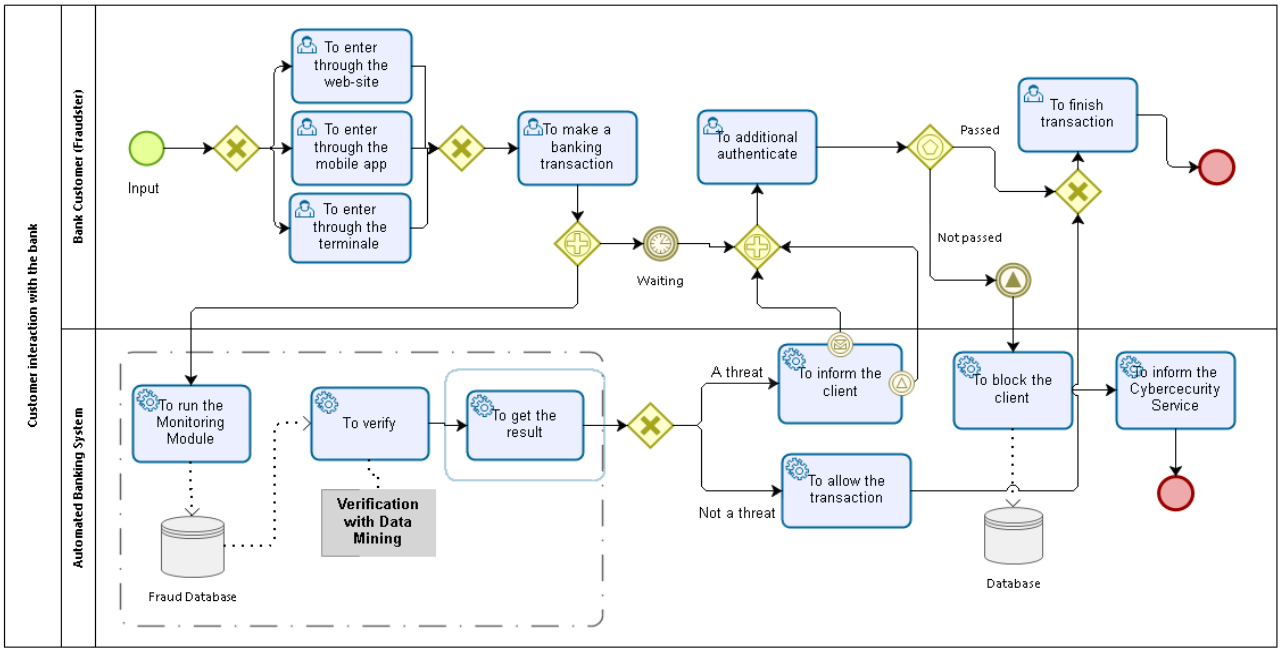


Рисунок 2.13 – Схема процесу здійснення операції клієнтом банку [22]

Процес виглядатиме наступним чином (рисунок 2.13):

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 2.13, 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 2.14).

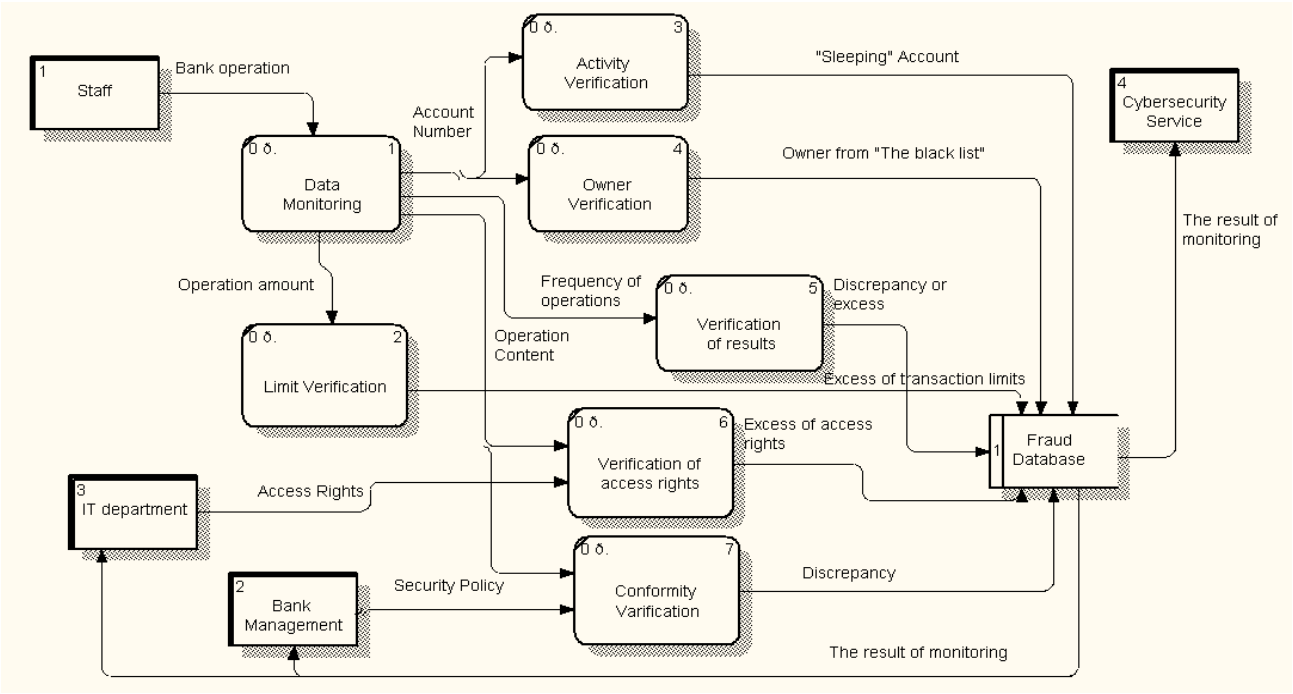


Рисунок 2.14 – Інформаційна модель виявлення ознак шахрайств персоналу банку [22]

Модель, представлена на рисунку 2.14, 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 2.14) розроблено схему процесу здійснення операції персоналом з урахуванням її перевірки на ознаки шахрайства у нотації BPMN 2.0 (рисунок 2.15).

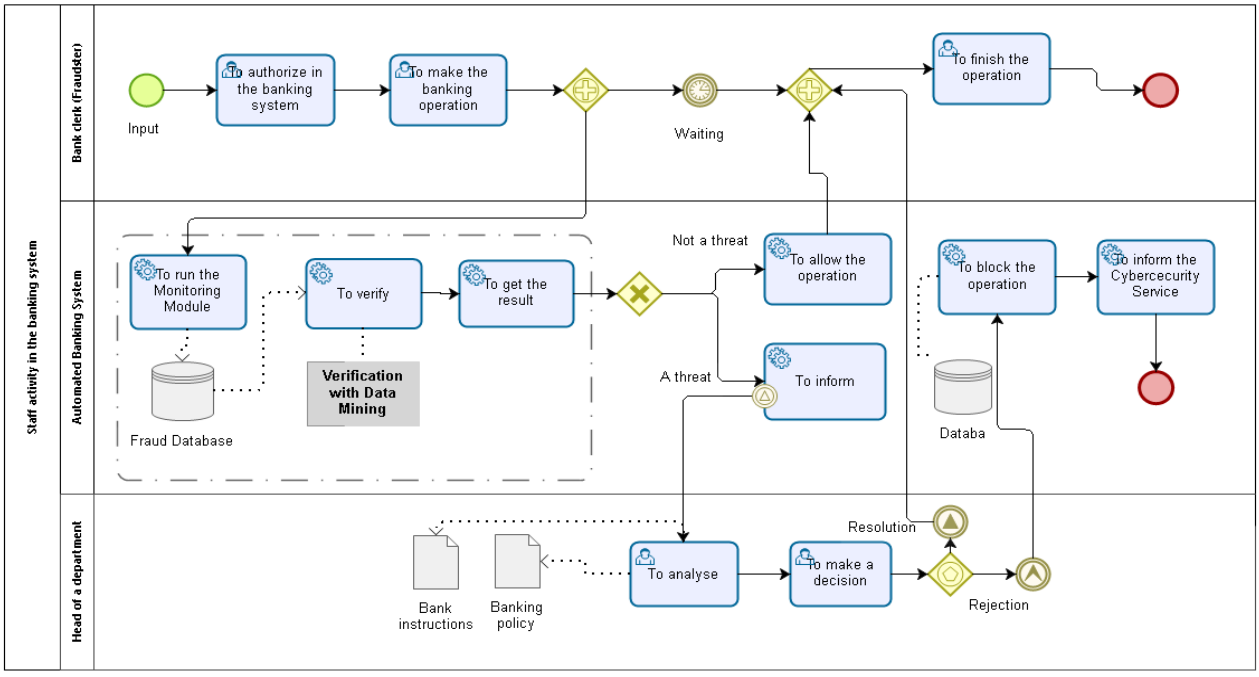


Рисунок 2.15 – Схема процесу здійснення операцій персоналом банку [22]

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 4;

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.

3 ОЦІНКА РІВНЯ ВТРАТ КОМЕРЦІЙНИХ БАНКІВ ВІД ШАХРАЙСЬКИХ ОПЕРАЦІЙ

3.1 Кількісний аналіз збитків банківської системи в результаті кібершахрайств

За даними Національного банку України збитки вітчизняних банків в 2017 р. 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 [25]:

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. 3.1).

Таблиця 3.1 – 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. 3.1 необхідно зазначити, що їх визначення проводиться наступним чином (формула 3.1-3.5):

$$r_{lj} = \begin{cases} 1, \text{якщо } l-\text{й релевантний фактор ризиків надає } j-\text{ту перевагу} \\ 0, \text{якщо } l-\text{й релевантний фактор ризиків не надає } j-\text{тої переваги} \end{cases} \quad (3.1)$$

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 3.2 – 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 3.3).

Таблиця 3.3 – 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 (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	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 3.3, пропонується обраховувати наступним чином:

$$v_{lj} = \begin{bmatrix} L_{lj}|_{1-r_{lj}=1} \\ 0|_{1-r_{lj}=0} \end{bmatrix} \quad (3.2)$$

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;

$v_{lj}\big|_{l=6\div16,\,j=1\div6}$ - 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;

$v_{lj}\big|_{l=17\div19,\,j=1\div6}$ - індикатор витрат банку як результат настання негативних наслідків дії групи ризиків нтернет 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;

$v_{lj}\big|_{l=20\div25,\,j=1\div6}$ - 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 3.3 та формул 3.2, перейдемо послідовно до побудови *витратних матриць:*

$$L = \begin{matrix} min\left\{L_{lj}|_{1-r_{lj}=1}\right\} \\ max\left\{L_{lj}|_{1-r_{lj}=1}\right\} \end{matrix} \begin{matrix} min\left\{L_{lj}|_{1-r_{lj}=1}\right\} & max\left\{L_{lj}|_{1-r_{lj}=1}\right\} \\ \begin{pmatrix} min\left\{L_{lj}|_{1-r_{lj}=1}\right\} + \\ +min\left\{L_{lj}|_{1-r_{lj}=1}\right\} \end{pmatrix} & \begin{pmatrix} min\left\{L_{lj}|_{1-r_{lj}=1}\right\} + \\ +max\left\{L_{lj}|_{1-r_{lj}=1}\right\} \end{pmatrix} \\ \begin{pmatrix} max\left\{L_{lj}|_{1-r_{lj}=1}\right\} + \\ +min\left\{L_{lj}|_{1-r_{lj}=1}\right\} \end{pmatrix} & \begin{pmatrix} max\left\{L_{lj}|_{1-r_{lj}=1}\right\} + \\ +max\left\{L_{lj}|_{1-r_{lj}=1}\right\} \end{pmatrix} \end{matrix} \tag{3.3}$$

Визначення ймовірностей їх отримання в кожній конкретній ситуації:

$$P = \begin{matrix} maxP\left[min\left\{L_{lj}|_{1-r_{lj}=1}\right\}\right] \\ minP\left[max\left\{L_{lj}|_{1-r_{lj}=1}\right\}\right] \end{matrix} \begin{matrix} maxP\left[min\left\{L_{lj}|_{1-r_{lj}=1}\right\}\right] & minP\left[max\left\{L_{lj}|_{1-r_{lj}=1}\right\}\right] \\ \begin{pmatrix} maxP\left[min\left\{L_{lj}|_{1-r_{lj}=1}\right\}\right] \times \\ \times maxP\left[min\left\{L_{lj}|_{1-r_{lj}=1}\right\}\right] \end{pmatrix} & \begin{pmatrix} maxP\left[min\left\{L_{lj}|_{1-r_{lj}=1}\right\}\right] \times \\ \times minP\left[max\left\{L_{lj}|_{1-r_{lj}=1}\right\}\right] \end{pmatrix} \\ \begin{pmatrix} minP\left[max\left\{L_{lj}|_{1-r_{lj}=1}\right\}\right] \times \\ \times maxP\left[min\left\{L_{lj}|_{1-r_{lj}=1}\right\}\right] \end{pmatrix} & \begin{pmatrix} minP\left[max\left\{L_{lj}|_{1-r_{lj}=1}\right\}\right] \times \\ \times minP\left[max\left\{L_{lj}|_{1-r_{lj}=1}\right\}\right] \end{pmatrix} \end{matrix} \tag{3.4}$$

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:

$$R = \begin{Bmatrix} \begin{pmatrix} min\left\{L_{lj}|_{1-r_{lj}=1}\right\}+ \\ +min\left\{L_{lj}|_{1-r_{lj}=1}\right\} \end{pmatrix} & \begin{pmatrix} min\left\{L_{lj}|_{1-r_{lj}=1}\right\}+ \\ +max\left\{L_{lj}|_{1-r_{lj}=1}\right\} \end{pmatrix} & \begin{pmatrix} max\left\{L_{lj}|_{1-r_{lj}=1}\right\}+ \\ +max\left\{L_{lj}|_{1-r_{lj}=1}\right\} \end{pmatrix} \\ \begin{pmatrix} maxP\left[min\left\{L_{lj}|_{1-r_{lj}=1}\right\}\right]\times \\ \times maxP\left[min\left\{L_{lj}|_{1-r_{lj}=1}\right\}\right] \end{pmatrix} & \begin{pmatrix} minP\left[max\left\{L_{lj}|_{1-r_{lj}=1}\right\}\right]\times \\ \times maxP\left[min\left\{L_{lj}|_{1-r_{lj}=1}\right\}\right] \end{pmatrix} & \begin{pmatrix} minP\left[max\left\{L_{lj}|_{1-r_{lj}=1}\right\}\right]\times \\ \times minP\left[max\left\{L_{lj}|_{1-r_{lj}=1}\right\}\right] \end{pmatrix} \end{Bmatrix} \quad (3.5)$$

$$\begin{Bmatrix} L \\ P(R \le L) \end{Bmatrix} = \begin{Bmatrix} \begin{pmatrix} min\left\{L_{lj}|_{1-r_{lj}=1}\right\}+ \\ +min\left\{L_{lj}|_{1-r_{lj}=1}\right\} \end{pmatrix} & \begin{pmatrix} min\left\{L_{lj}|_{1-r_{lj}=1}\right\}+ \\ +max\left\{L_{lj}|_{1-r_{lj}=1}\right\} \end{pmatrix} & \begin{pmatrix} max\left\{L_{lj}|_{1-r_{lj}=1}\right\}+ \\ +min\left\{L_{lj}|_{1-r_{lj}=1}\right\} \end{pmatrix} \\ \begin{pmatrix} maxP\left[min\left\{L_{lj}|_{1-r_{lj}=1}\right\}\right]\times \\ \times maxP\left[min\left\{L_{lj}|_{1-r_{lj}=1}\right\}\right] \end{pmatrix} & \begin{pmatrix} maxP\left[min\left\{L_{lj}|_{1-r_{lj}=1}\right\}\right]\times \\ \times maxP\left[min\left\{L_{lj}|_{1-r_{lj}=1}\right\}\right]+ \\ +minP\left[max\left\{L_{lj}|_{1-r_{lj}=1}\right\}\right]\times \\ \times maxP\left[min\left\{L_{lj}|_{1-r_{lj}=1}\right\}\right] \end{pmatrix} & 1 \end{Bmatrix} \quad (3.6)$$

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.

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 3.7) [26]:

$$NK_i = \frac{K_i}{\overline{K_i}} \tag{3.7}$$

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 3.8) [26]. 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.

$$K_i = \beta_0 + \beta_1 F_{1i} + \beta_2 F_{2i} + \beta_3 F_{3i} + \beta_4 F_{4i} + \varepsilon \qquad (3.8)$$

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 3.9) [26]:

$$K_i = \alpha_1 F_{1i} + \alpha_2 F_{2i} + \alpha_3 F_{3i} + \alpha_4 F_{4i} + \varepsilon \quad (3.9)$$

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 (3.9) визначаються за наступною формулою (3.10) [26]:

$$\alpha_m = \beta_m \frac{\sigma_{F_j}}{\sigma_{K_i}} \quad (3.10)$$

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 (3.11) і (3.12) [26]:

$$\sigma_{F_j} = \sqrt{\overline{F_j^2} - \overline{F_j}^2}, \quad (3.11)$$

$$\sigma_{K_i} = \sqrt{\overline{K_i^2} - \overline{K_i}^2}. \quad (3.12)$$

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 3.13) [26], що характеризує питому вагу впливу інцидентів на рівень операційного ризику інформаційної безпеки.

$$\alpha_m^* = \frac{\alpha_m}{\sum_{m=1}^{4} \alpha_m}, \tag{3.13}$$

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 3.4.

Таблиця 3.4 - 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}

За допомогою даних таблиці 3.4 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 3.5 – 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	$\alpha_1 NK_n$	$\alpha_2 NK_n$	$\alpha_3 NK_n$	$\alpha_4 NK_n$

Отже, вище 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.

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 банківської установи, 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 (3.14) [26]:

$$NKbin_i \begin{cases} = 1; \alpha_m^* \overline{NK_m} \geq \alpha_m^* NK_i, \\ = 0; \alpha_m^* NK_i < \alpha_m^* \overline{NK_m} \end{cases}, \quad (3.14)$$

де $NKbin_i$ - бінарні характеристики по певному показнику кількісної оцінки ступеня операційного ризику банку в сфері інформаційної безпеки 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 3.6.

Таблиця 3.6 – 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	$NKbin_{k1}$	$NKbin_{k2}$	$NKbin_{k3}$	$NKbin_{k4}$
	…	…	…	…
	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 3.15) [26]:

$$EO_j = \sum_{i=1}^{n} NKbin_{ij}\,, \tag{3.15}$$

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 3.16) [26]:

$$EO = \sum_{j=1}^{4} \sum_{i=1}^{n} NKbin_{ij}, \tag{3.16}$$

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 вкючає 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 ($p_{OR}(H1)$) 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 3.17-3.18) [26]:

$$p_K(H1j)=\frac{1}{1+e^{\{\lambda_0+L\}}} \qquad (3.17)$$

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

$$\lambda_{ij} = \ln\left(\frac{b_{ij}(1-g_{ij})}{g_{ij}(1-b_{ij})}\right), i = 1,...,n \qquad (3.18)$$

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

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 3.19 [26]:

$$g_{ij} = \frac{\sum_i NKbin_{ij}}{n}, \qquad b_{ij} = 1 - g_{ij} \tag{3.19}$$

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 3.7):

Таблиця 3.7 – 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 $j=4$
A	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)	$0 \le p_K(H1j) < fsr\{\min_s\{p_B(H1)_s\} \div fsr\{p_B(H1)_s\}\}$			
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)	$p_B(H1)$			

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. $S(p_K(H1j)) = \frac{p_K(H1j)}{\sum_{j=1}^{4} p_K(H1j)} \times 100\%$

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.

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) $p_B(H1)$ за формулою (13).

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 3.20-3.21) [26]:

$$p_B(H1) = \frac{1}{1 + e^{\{\lambda_0 + L\}}} \qquad (3.20)$$

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

$$\lambda_j = \ln\left(\frac{b_j(1-g_j)}{g_j(1-b_j)}\right), j = 1,...,4 \qquad (3.21)$$

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

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.

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 [27].

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 [25].

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 [29]:

– 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 [30], 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. 1.2).

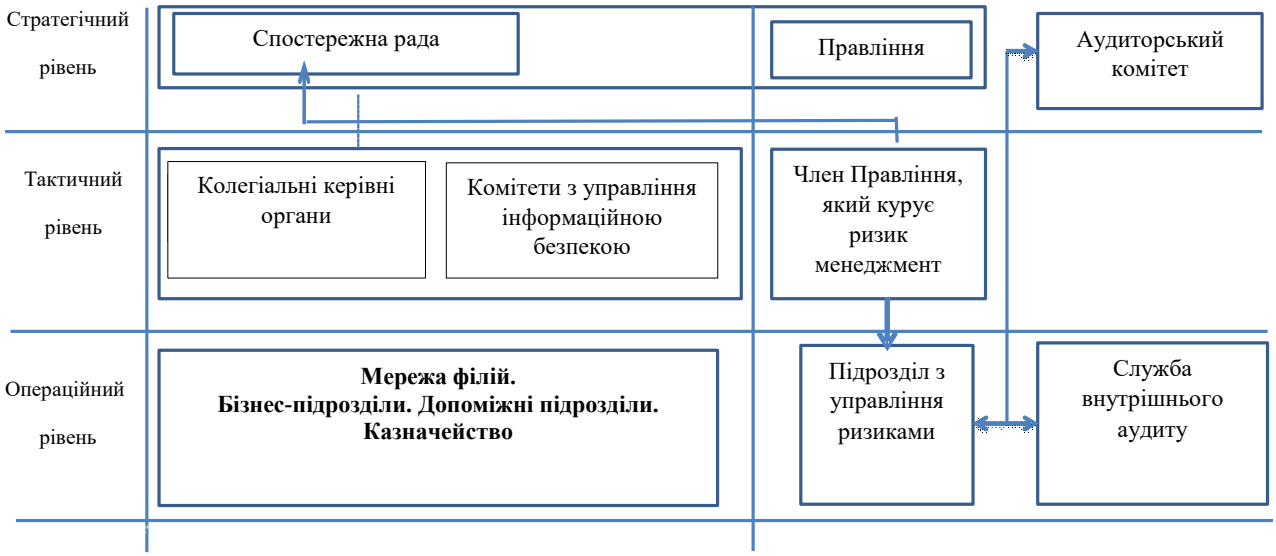


Рисунок 3.1 – Організаційно-управлінська підсистема управління ризиками ІБ банку

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 [30, 31].

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 [31].

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 [30]. 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 [31]. Також на цей підрозділ покладаються функції розробки внутрішньої нормативної бази.

Операційний рівень включає функції управління ризиками ІБ, що здійснюються у підрозділах банку шляхом здійснення 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 – інциденти ризиків ІБ;
- участь у наступному контролі якості даних про операційні події – інциденти ризиків ІБ;
- 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 безпосередньо управління ІБ банку, її роль зводиться до оцінки адекватності цих систем цілям та задачам банку в цій сфері [31].

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. 3.2).

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 [30].

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 [30].

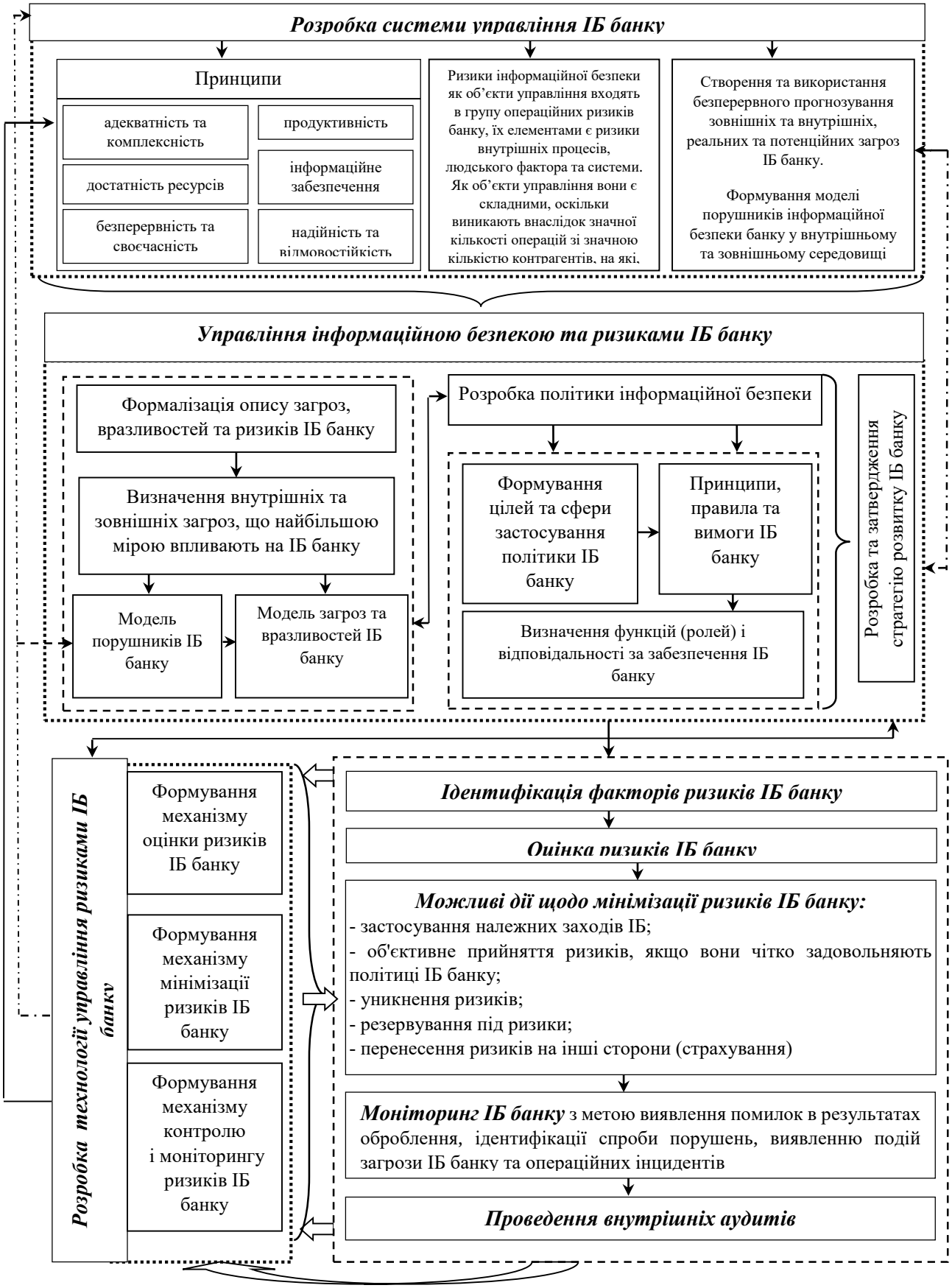


Рисунок 3.2 – Основні функції управління ІБ та ризиками ІБ банку

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 [30].

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. 3.8).

Таблиця 3.8 – 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	

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. 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 проводиться для завчасного розпізнавання негативних тенденцій в окремих бізнес-процесах або діяльності банку у цілому та прийняття відповідних рішень, спрямованих на мінімізацію / запобігання втрат від реалізації ризиків ІБ.

Аналіз КІР застосовуються, 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 на цій основі 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: саме страхування ВВВ; страхування від електронних та комп'ютерних злочинів; страхування професійної відповідальності фінансового інституту.

Основною статтею ВВВ є страхування від збитків у результаті шахрайства персоналу. Поліс ВВВ 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 ВВВ, 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:

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

2. 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;

3. 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.

4 РОЗРОБКА КОМПЛЕКСУ ПРЕВЕНТИВНИХ ЗАХОДІВ ДО ПОПЕРЕДЖЕННЯ НАСТАННЯ СИТУАЦІЙ, ЯКІ КЛАСИФІКУЮТЬСЯ ЯК КІБЕРЗАГРОЗА АБО ШАХРАЙСТВО

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 населення країни більше схильне до шахрайських операцій ніж у суспільстві, в якому вища заробітна плата.

– 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, то вона впливає і сильно заважає ефективному державному управлінню, тому можемо гіпотетично 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 роботи, виробництво товарів, різних витрат та інвестицій. тоді в населення виникає схильність до здійснення шахрайства більше ніж в суспільстві, яке має вільні економічні права.

– Країна в якій економічний розвиток не на високому рівні, купівельна спроможність населення низька, то можливе 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 4.1).

Рисунок 4.1 – 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 4.1.

Таблиця 4.1 – 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. Бузуется 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 [32]. 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:

$$t_{y(\text{e})} = \beta_1 \cdot t_{x3} + \beta_2 \cdot t_{x12} + \beta_2 \cdot t_{x11} + \beta_2 \cdot t_{x8} + \beta_2 \cdot t_{x9} + \beta_2 \cdot t_{x1} + \quad (4.1)$$

$$+\beta_2 \cdot t_{x17} + \varepsilon,$$

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:

$$t_{y(\text{п})} = \beta_1 \cdot t_{x18} + \beta_2 \cdot t_{x3} + \beta_2 \cdot t_{x2} + \beta_2 \cdot t_{x4} + \beta_2 \cdot t_{x7} + \beta_2 \cdot t_{x20} + \varepsilon, \quad (4.2)$$

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:

$$t_{y(\text{с})} = \beta_1 \cdot t_{x4} + \beta_2 \cdot t_{x5} + \beta_2 \cdot t_{x7} + \beta_2 \cdot t_{x9} + \beta_2 \cdot t_{x10} + \beta_2 \cdot t_{x13} + \quad (4.3)$$

$$+\beta_1 \cdot t_{x14} + \beta_2 \cdot t_{x15} + \beta_2 \cdot t_{x16} + \beta_2 \cdot t_{x17} + \beta_2 \cdot t_{x19} + \varepsilon,$$

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:

$$t_j = \frac{xi - \bar{x}i}{\sigma xi} \tag{4.4}$$

де xi значення в xi спостереженні

$$t_y = \frac{y - \bar{y}}{\sigma y} \tag{4.5}$$

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

Для відбору найбільш значущих факторі було використано пошагову або гребневу регресію. Гребнева 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 [32].

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 [33]:

– адитивної

$$F(x_i) = \sum_{j=1}^{n} \omega_j \cdot x_{ij} \tag{4.6}$$

– мультиплікативної

$$F(x_i) = \prod_{j=1}^{n} x_{ij}^{\omega_j} \tag{4.7}$$

Які вважаються найпоширенішими [34] для формування класичного виду адитивно-мультиплікативної згортки.

Недоліки методів згортки:

– на адекватність впливає розподіл альтернатив у вибірці критеріїв [34];

– недостане значення одного критерію може компенсуватися значенням іншого критерія [35];

– часткові функції корисносіт повинні бути односпрямовані [36].

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 [37]. Тому необхідно критерії поділити на:

Стимулятори:

$$f_j(x) \to max, \qquad j = \overline{1,k}, x \epsilon S \tag{4.8}$$

Дестимулятори:

$$f_j(x) \to min, \qquad j = \overline{1,k}, x \epsilon D \tag{4.9}$$

де S та D – множина критеріїв.

Нормування стимуляторів проводиться за формулою:

$$x'_{ij} = \frac{x_{ij}}{x_{maxj}} \tag{4.10}$$

Нормування дистимуляторів проводиться за наступною формулою:

$$x'_{ij} = \frac{x_{ij}}{x_{minj}} \tag{4.11}$$

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

$$\rho(y,z) \geq 0 \ ,\rho(y,z) = 0, y \Leftrightarrow z; \tag{4.12}$$

$$\rho(y,z) = \rho(z,y); \tag{4.13}$$

$$\rho(y,z) \le \rho(w,y) + \rho(y,z). \quad (4.14)$$

Метрика Мінковського має наступний вигляд:

$$\rho(y,z) = \left(\sum_{i=1}^{n} a_i^s \cdot |y_i - z_i|^r\right)^{1/r} \quad (4.15)$$

Функція корисності матиме вигляд:

$$F(x_i) = 1 - \sqrt[n]{\sum_{j=1}^{k} \omega_j \cdot \left|1 - \frac{x_{ij}}{x_{maxj}}\right|^n + \sum_{j=k+1}^{n} \omega_j \cdot \left|1 - \frac{x_{minj}}{x_{ij}}\right|^n} \quad (4.16)$$

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. [38-40]

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 4.2).

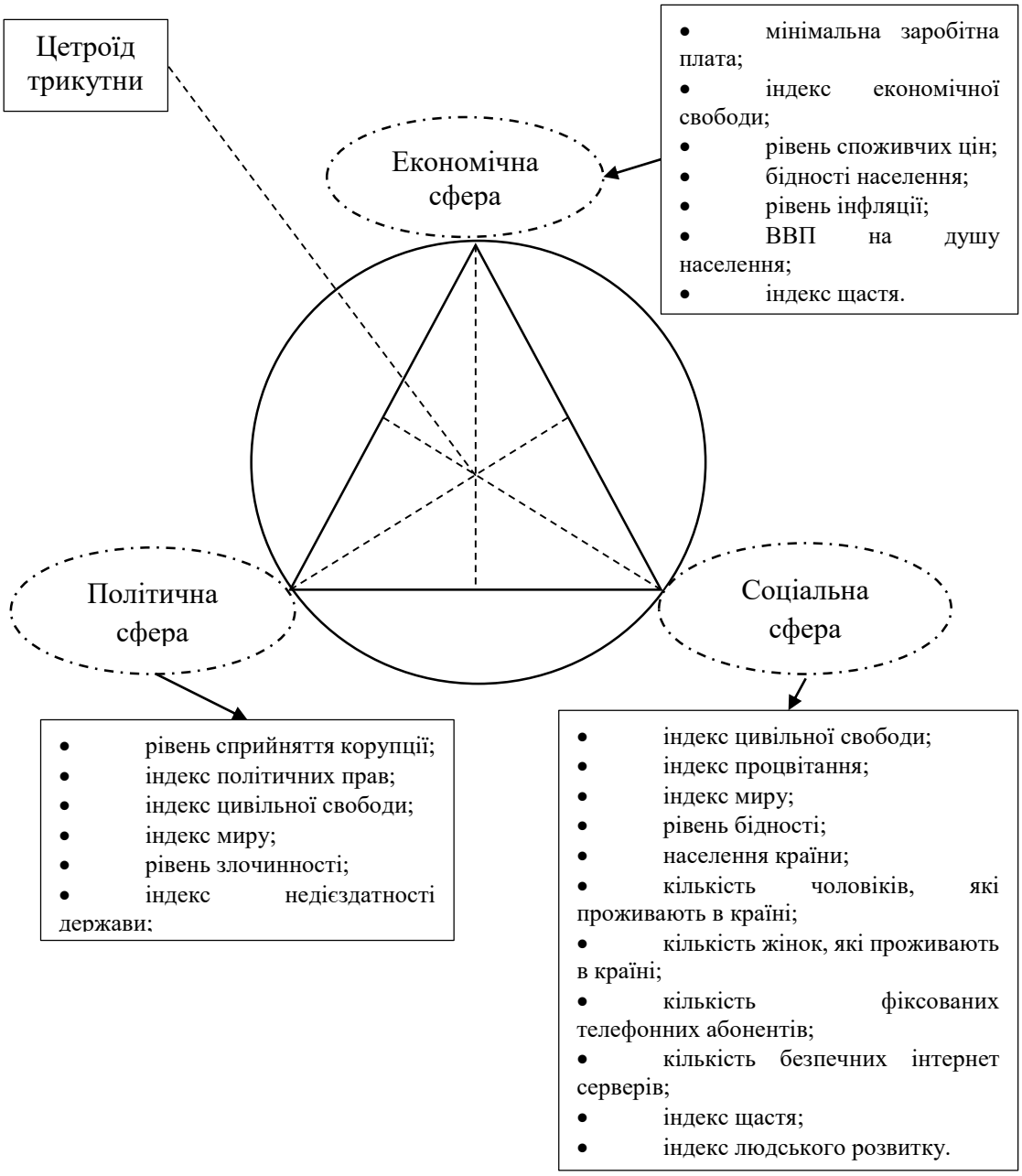


Рисунок 4.2 – Трикутник

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.

$$R_t = \frac{n_{et} \cdot n_{st} \cdot}{\sqrt{\left(n_{et} + n_{st} + n_{pt}\right) \cdot \left(-n_{et} + n_{st} + n_{pt}\right) \cdot \left(n_{et} + n_{st} - n_{pt}\right) \cdot}} \qquad (4.17)$$

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

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 наступній формулі:

$$\sin \alpha_{et} = \frac{n_{et}}{2 \cdot R_t} \qquad (4.18)$$

$$\sin \alpha_{st} = \frac{n_{st}}{2 \cdot R_t} \qquad (4.19)$$

$$\sin \alpha_{pt} = \frac{n_{pt}}{2 \cdot R_t} \qquad (4.20)$$

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, цетроїда лежить в середині

трикутника, то схильність до шахрайства є низькою. Коли трикутник тупокутний, центроїда лежить поза трикутником, то схильність до шахрайства є високою [38-39].

Реалізацію моделі проведемо в програмному забезпечені STATISTICA. На рисунку 4.3 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 4.3 – 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 4.4.

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 4.4 – 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 4.5.

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 4.5 – Результати регресійної моделі для соціального стану

В результаті проведення первинного аналізу були отримані найбільш вагомі змінні:

— економічні

$$F_{\text{e}} = b_{i1} \cdot X_1 + b_{i2} \cdot X_3 + b_{i3} \cdot X_{12} \qquad (4.21)$$

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

$$F_i = b_{i1} \cdot X_4 + b_{i2} \cdot X_5 + b_{i2} \cdot X_7 + b_{i2} \cdot X_{10} + b_{i2} \cdot X_{17} + \\ + b_{i2} \cdot X_{19} \qquad (4.22)$$

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

$$F_i = b_{i1} \cdot X_2 + b_{i2} \cdot X_4 + b_{i3} \cdot X_{18} + b_{i4} \cdot X_{20} \quad (4.23)$$

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.4.6).

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 процвітання	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 4.6 – Відносна нормалізація показників

Як видно з рисунку 4.6 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. 4.7).

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 4.7 – 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. 4.8).

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 4.8 – 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. 4.9)

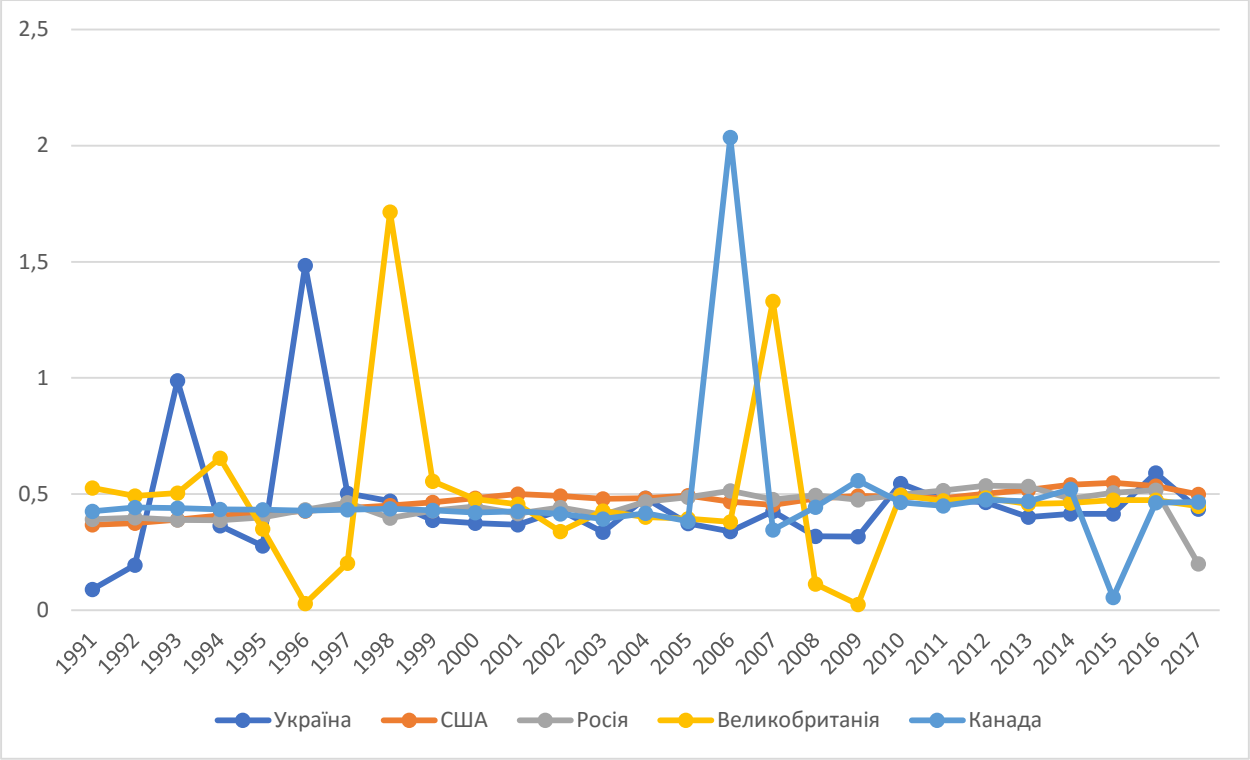


Рисунок 4.9 – Діаграма динаміки значень радіуса кола описаного навколо трикутника політичної та економічної ситуації України, США, Великобританії, Канади та Росії

На основі даних, які наведених на рисунку 4.9, 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. 4.9), 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 4.10.

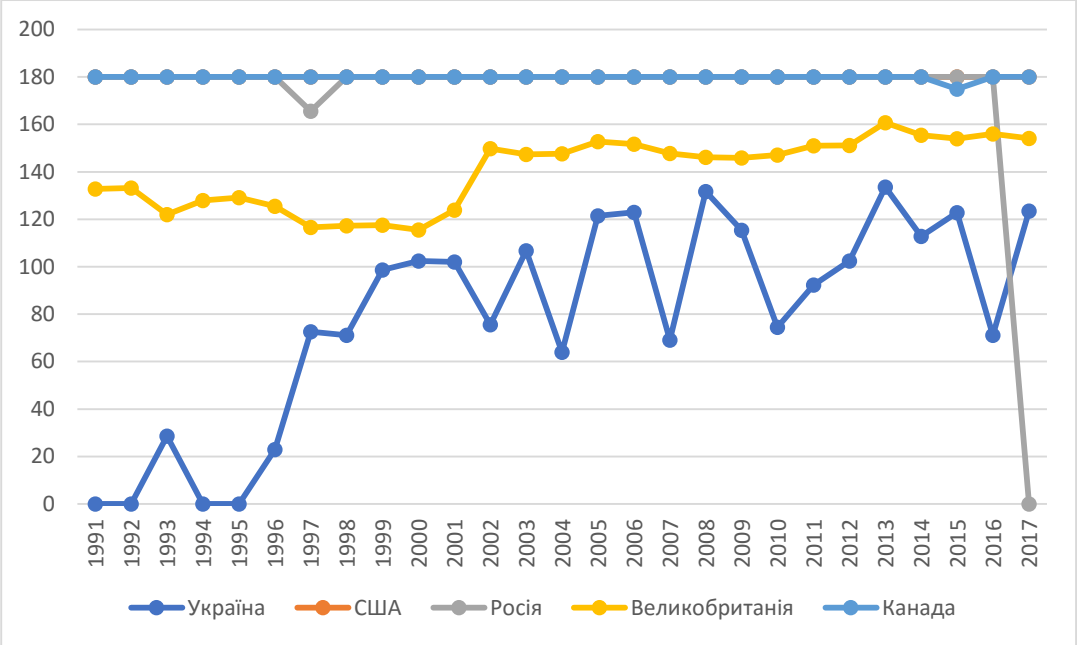


Рисунок 4.10 – Діаграма динаміки схильності до шахрайства в України, США, Великобританії, Канади та Росії

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 4.11. Як бачимо з рисунку Росія, Канада та США мають низьку схильність до шахрайства, а Україна та Великобританія мають високу схильність до шахрайства.

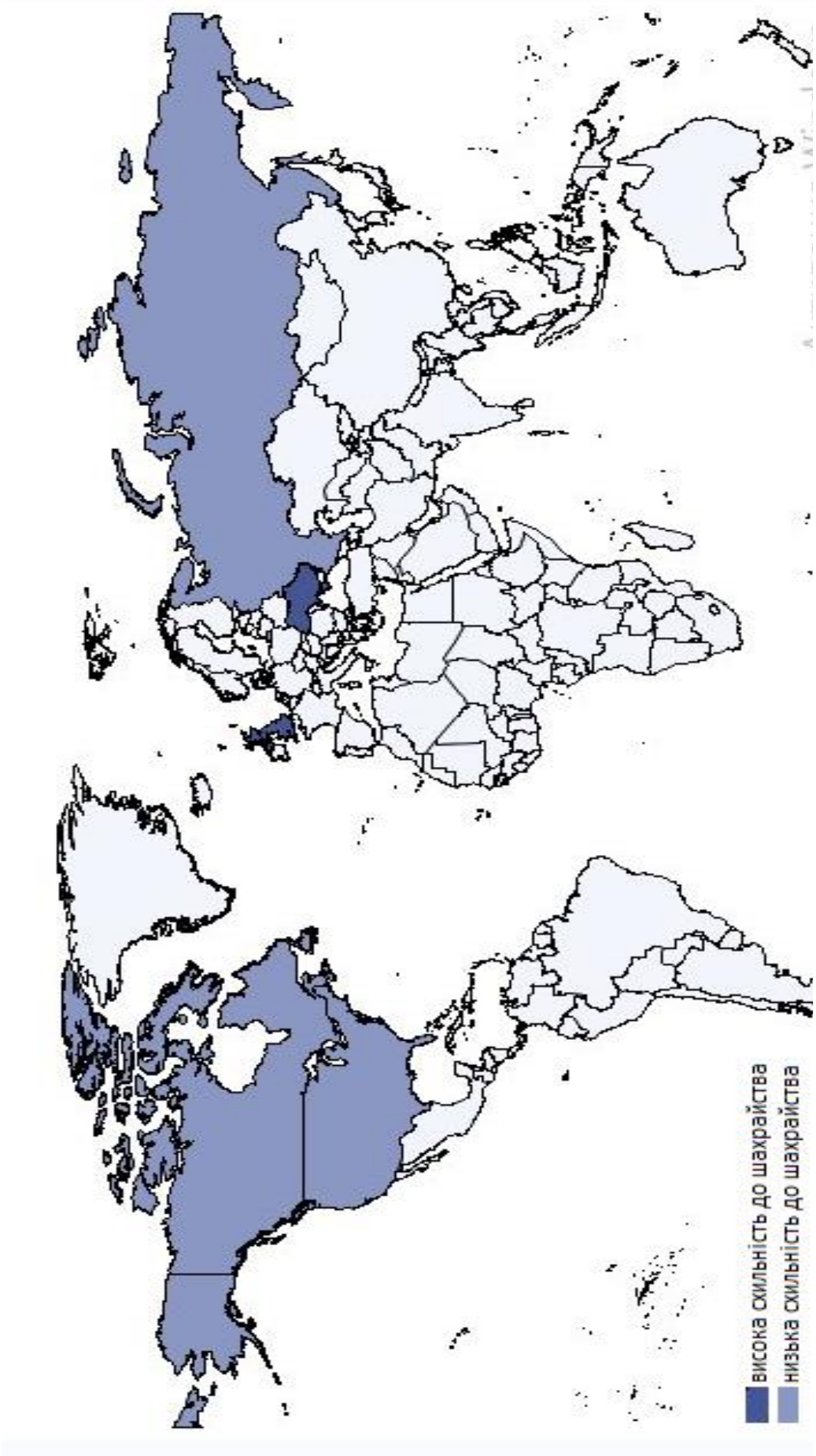


Рисунок 4.11 – Рівень впливу шахрайства по країнам

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 4.2:

Таблиця 4.2 – 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 4.24).

$$x_{ij}^{+} = \frac{x_{ij}}{x_{max_j}}, x_{ij}^{-} = \frac{x_{min_j}}{x_{ij}}, \quad (4.24)$$

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 4.25:

$$x_{ij}^{-} = \frac{x_{max_j} - x_{ij}}{x_{max_j} - x_{min_{ij}}}. \quad (4.25)$$

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 4.3:

Таблиця 4.3 – 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 4.4:

Таблиця 4.4 – 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

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.

Після цього в кожній матриці, в якій експерт поставив свої оцінки, для кожного фактору у рядку матриці знаходимо ваговий коефіцієнт за формулою 4.26:

$$\omega_i^k = \frac{\sqrt[n]{\prod_{j=1}^{n} a_{ij}^k}}{\sum_{i=1}^{n} \sqrt[n]{\prod_{j=1}^{n} a_{ij}^k}} \tag{4.26}$$

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:

$$K_{кон} = \frac{\sum_{j=1}^{n} d_j^2}{\frac{1}{12}\left[m^2(n^3 - n) - m\sum_{i=1}^{m} T_i\right]}; \tag{4.27}$$

де:

$$d_j = S_j - \frac{\sum_{j=1}^{n} S_j}{n}; \tag{4.28}$$

$$S_j = \sum_{i=1}^{m} R_{ij}; \tag{4.29}$$

m – кількість експертів, які прийняли участь в дослідженні;

n – кількість факторів дослідження;

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

$$T_i = \sum_{l=1}^{L}(t_l^3 - t_l); \tag{4.30}$$

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:

$$P_{\alpha\beta} = 1 - \frac{\sum_{j=1}^{n}\psi_j^2}{\frac{1}{6}\times(n^3 - n) - \frac{1}{12}(T_\alpha + T_\beta)}; \tag{4.31}$$

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

$$\psi_j = \left|R_{\alpha j} - R_{\beta j}\right|; \tag{4.32}$$

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:

$$\chi_p^2 = \frac{\sum_{j=1}^{n} d^2}{\frac{1}{12}\left[mn\times(n+1) - \frac{1}{n-1}\sum_{i=1}^{m}T_i\right]}. \tag{4.33}$$

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:

$$\omega_j = \frac{\sum_{i=1}^{m} \omega_i}{m}. \quad (4.34)$$

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 4.35):

$$IRA_i = 1 - \sqrt{\sum_{j=1}^{k} \omega_j \left|1 - x_{ij}^{+}\right|^2 + \sum_{j=k+1}^{n} \omega_j \left|1 - x_{ij}^{-}\right|^2}; \quad (4.35)$$

де IRA_i – інтегральна рейтингова оцінка характеристики рівня ризику легалізації для *i-ої* 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 4.36):

$$IRA(x_i) = 1 - \sqrt{\omega_1(1 - x_1^{-})^2 + \omega_3(1 - x_3^{-})^2 + \omega_5(1 - x_5^{-})^2 + \omega_7(1 - x_7^{-})^2 + \omega_2(1 - x_2^{+})^2 + \omega_4(1 - x_4^{+})^2 + \omega_6(1 - x_6^{+})^2} \quad (4.36)$$

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,

$$M_{ij} = k\frac{p_i p_j}{d_{ij}^2}, \tag{4.37}$$

де M_{ij} – показник взаємодії між об'єктами i 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 4.38):

$$SVA_k = \frac{IRA_k \cdot IRA_r}{d_{kr}^2}, \tag{4.38}$$

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 4.39):

$$d_{kr} = |LPI_k - LPI_r|,^{+} \tag{4.39}$$

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 4.40):

$$x_{ij}^{+} = \frac{x_{ij} - x_{min_j}}{x_{max_j} - x_{min_{ij}}}. \tag{4.40}$$

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:

$$SVA'_k = \exp(-\exp(-SVA_k)). \tag{4.41}$$

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 4.5:

Таблиця 4.5 – 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 4.6).

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.

Таблиця 4.6 – 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

Для проведення аналізу авторами було обрано три країни – Україну, Польщу та Германію. В таблиці 4.7 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 4.12 представлена карта привабливості легалізації доходів для України в різних країнах світу.

Дані таблиці 4.7 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.

Таблиця 4.7 – 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

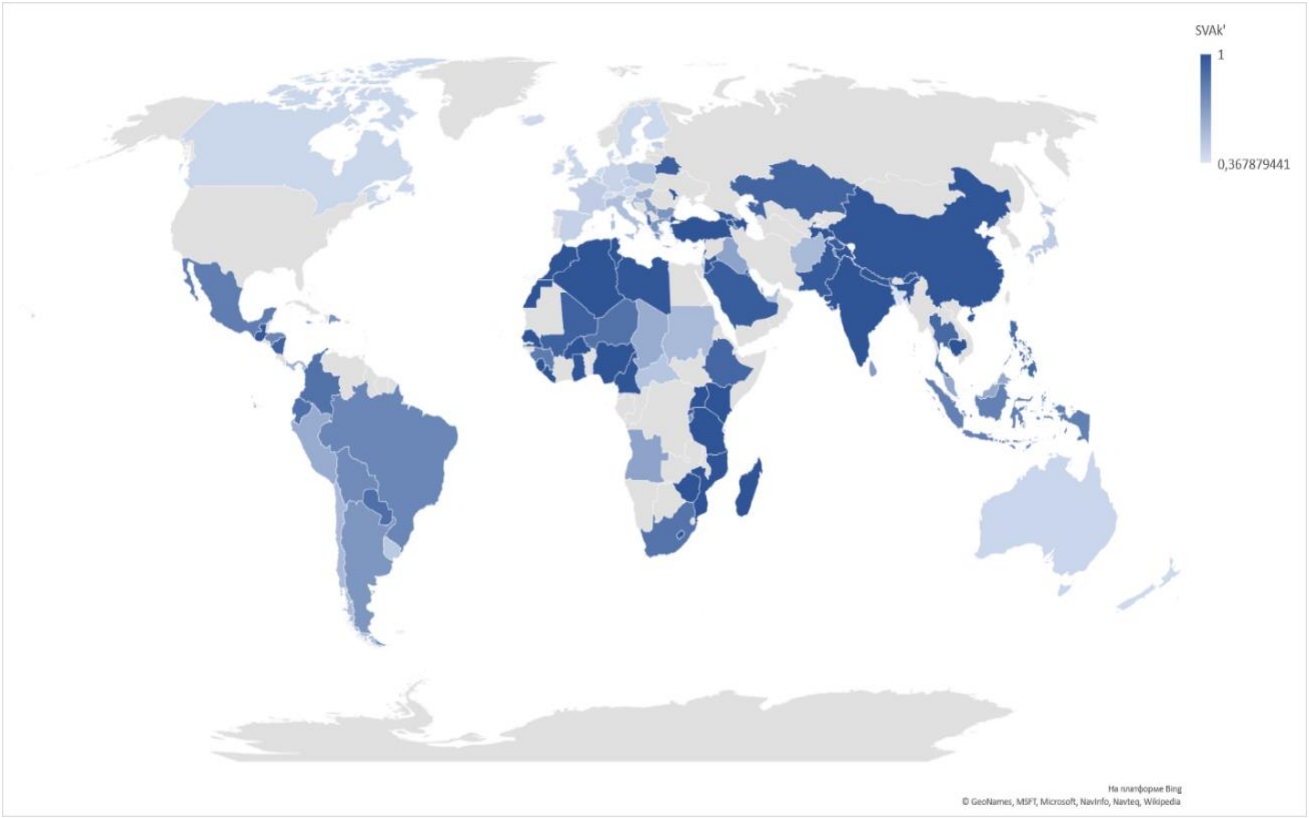


Рисунок 4.12 – Карта привабливості легалізації доходів для України в різних країнах світу

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. 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 4.8 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 4.13 представлена карта привабливості легалізації доходів для Польщі в різних країнах світу.

Таблиця 4.8 – 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

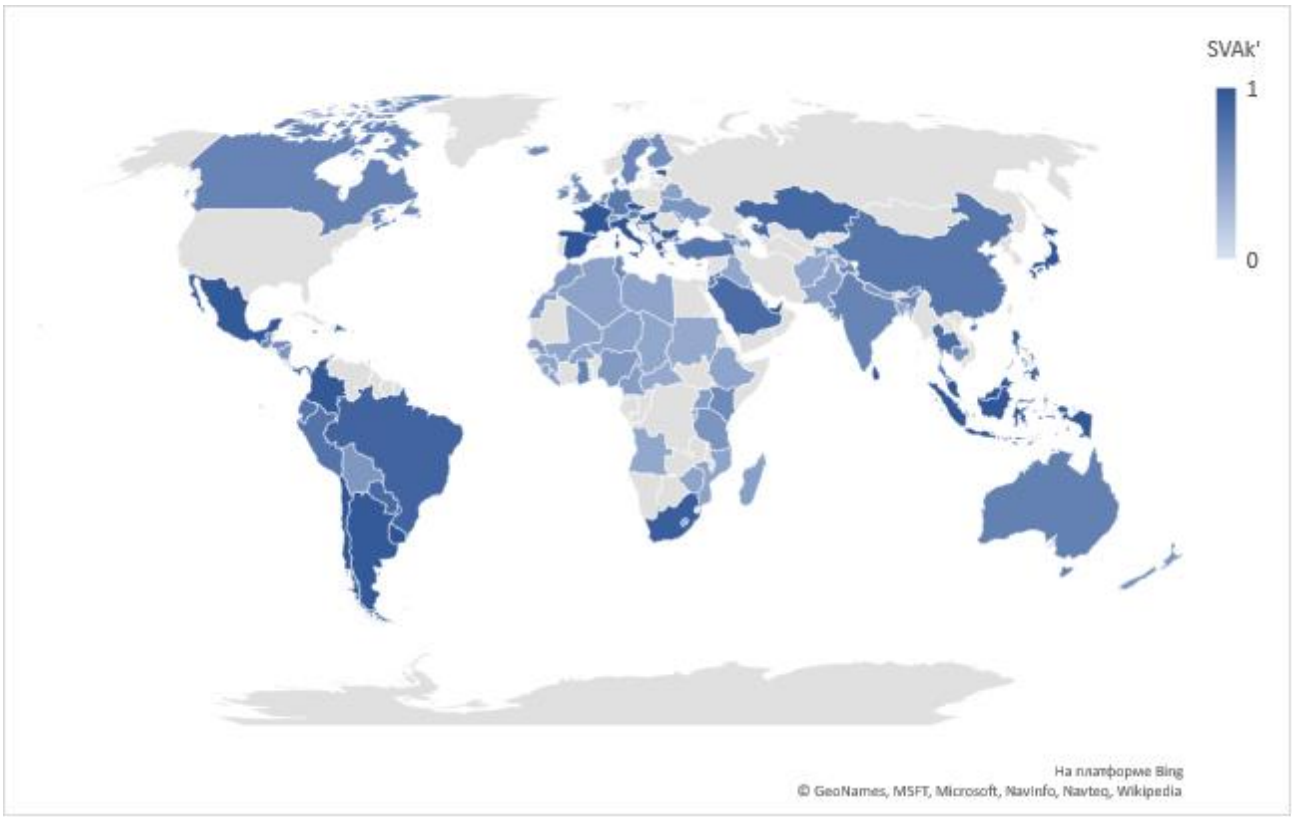


Рисунок 4.13 – Карта привабливості легалізації доходів для Польщі в різних країнах світу

Дані таблиці 4.8 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 4.13. Низький рівень ризику свідчить, що ці країни формують для Польщі умови, які є сприятливими для легалізації.

В таблиці 4.9 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 4.14 представлена карта привабливості легалізації доходів для Германії в різних країнах світу.

Таблиця 4.9 – 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

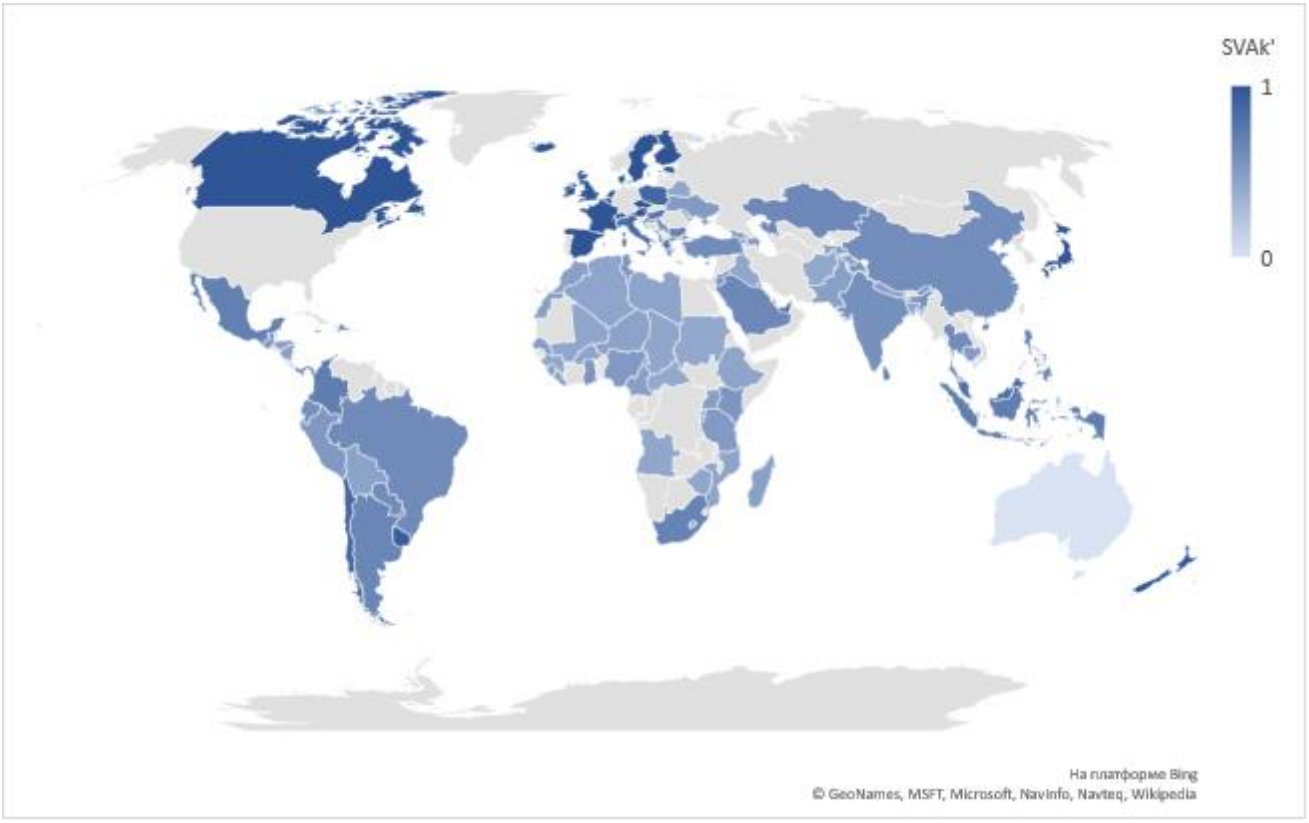


Рисунок 4.14 – Карта привабливості легалізації доходів для Германії в різних країнах світу

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 4.9 та на рисунку 4.14, 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.

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 банку для відображення транзакцій, котрі система визначила шахрайськими.

Взаємодію компонентів як єдиної системи, що пропонується, продемонстровано на діаграмі послідовності на рисунку 4.15.

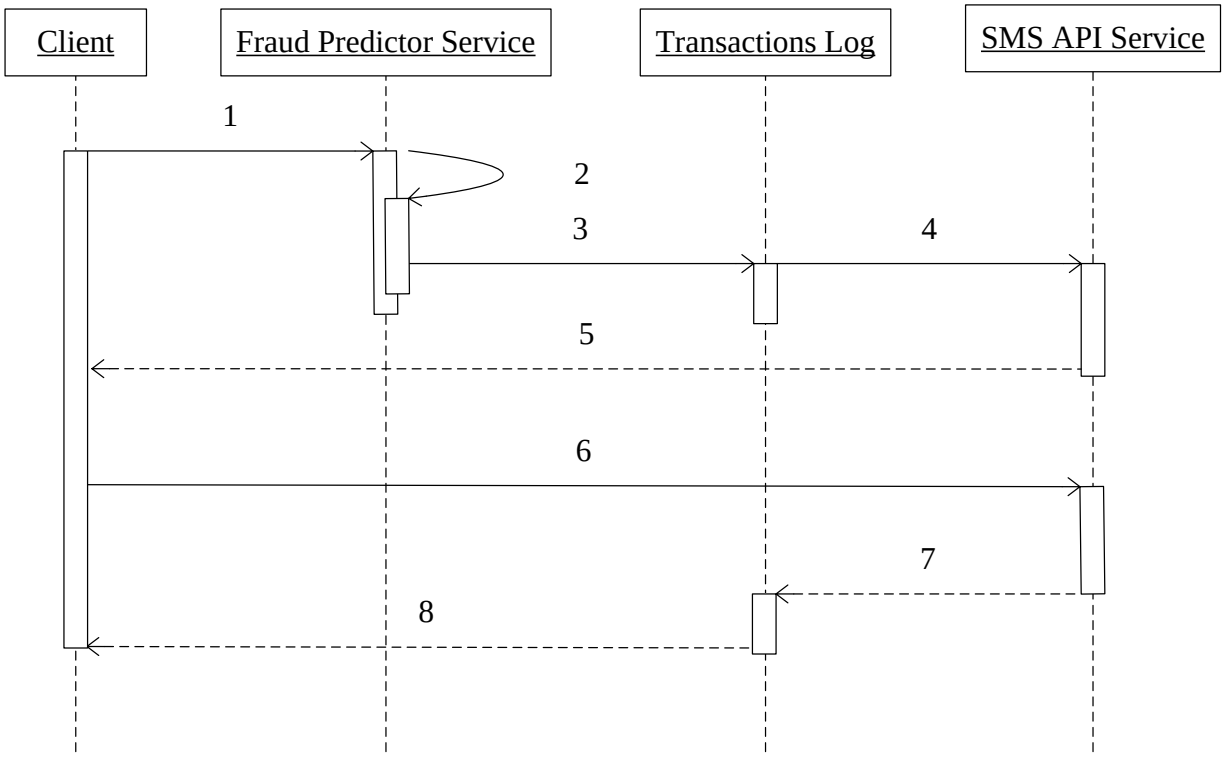


Рисунок 4.15 – Діаграма послідовності системи

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 [41].

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 [42].

Для опису бізнес-моделі нашої системи будемо використовувати нотації IDEF0 та IDEF3.

На рисунку 4.16 зображено контекстну діаграму процесу виявлення шахрайських операцій. Після неї наведемо пояснення до кожного елементу, що присутній на діаграмі (таблиця 4.10).

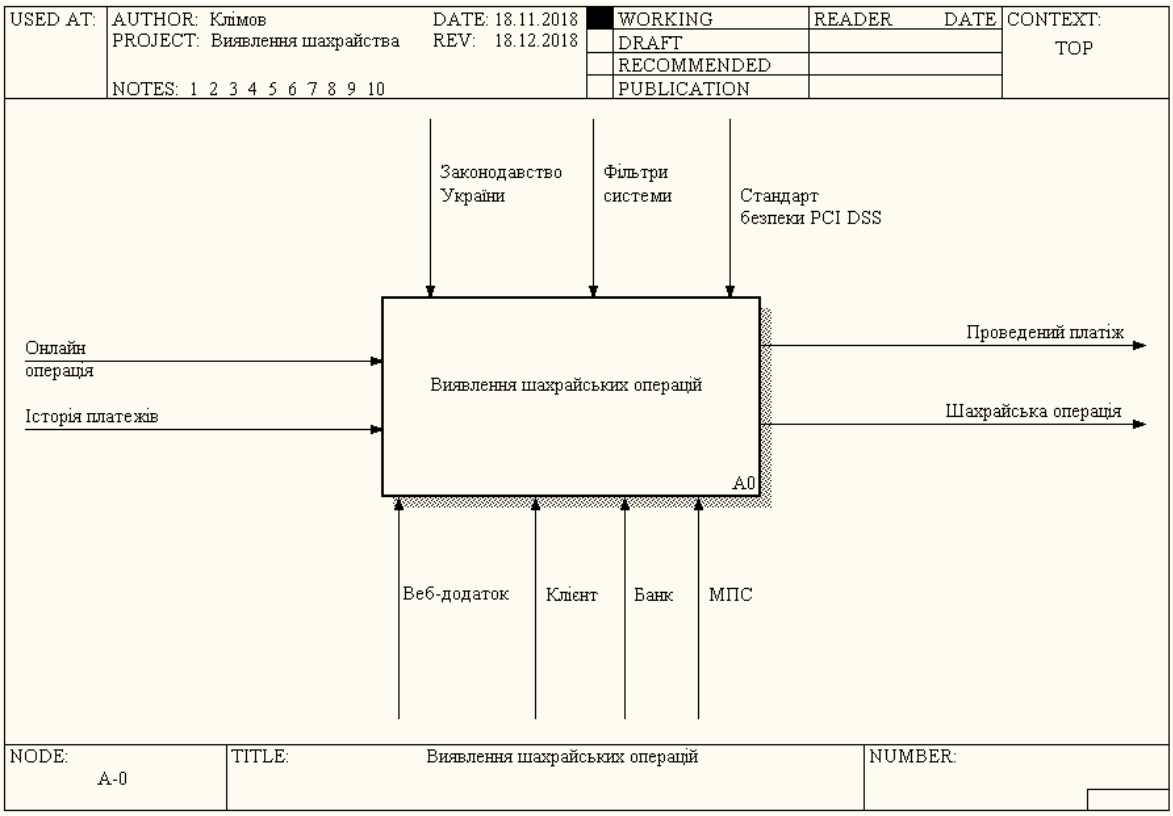


Рисунок 4.17 – Контекстна діаграма «Виявлення шахрайських операцій»

Таблиця 4.10 – 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 4.18).

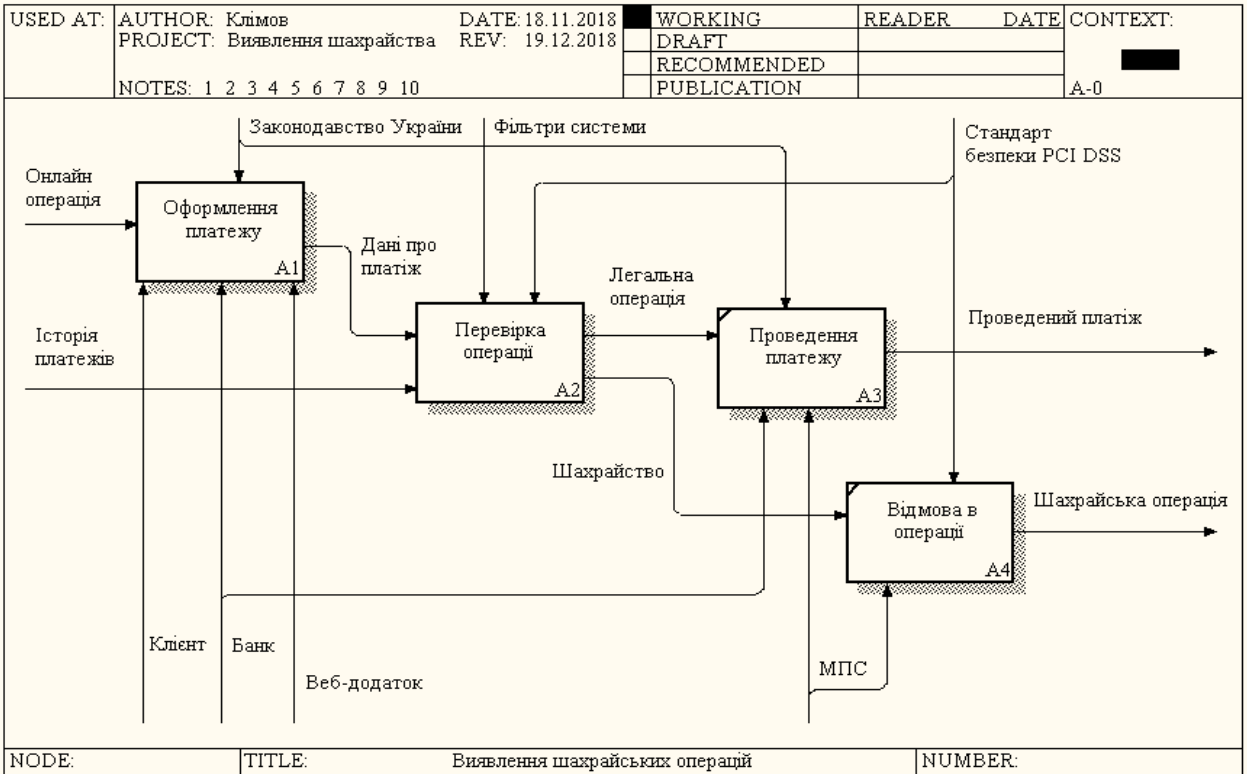


Рисунок 4.18 – Декомпозиція контекстної діаграми

Для поданого рисунка необхідно навести опис робіт (таблиця 4.11).

Таблиця 4.11 – 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 детальний опис зв’язків між роботами діаграми-декомпозиції контекстної діаграми, де буде вказано назва стрілки, її джерело, призначення та один із чотирьох можливих типів (таблиця 4.12).

Таблиця 4.12 – 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 4.19), де зображено 3 роботи, які складають процес оформлення платежу. Необхідно навести їх опис у вигляді таблиці 4.13. Також потрібно продемонструвати зв’язків між ними, описавши їх в таблиці 4.14. Зв’язки об’єднують не тільки роботи в цій діаграмі-декомпозиції, а й в батьківській.

Таблиця 4.13 – 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 міста, куди відправляти товар	WORKING
Визначення місцезнаходження	Пошук міста, в якому знаходиться клієнт, за допомогою IP-адреси	WORKING

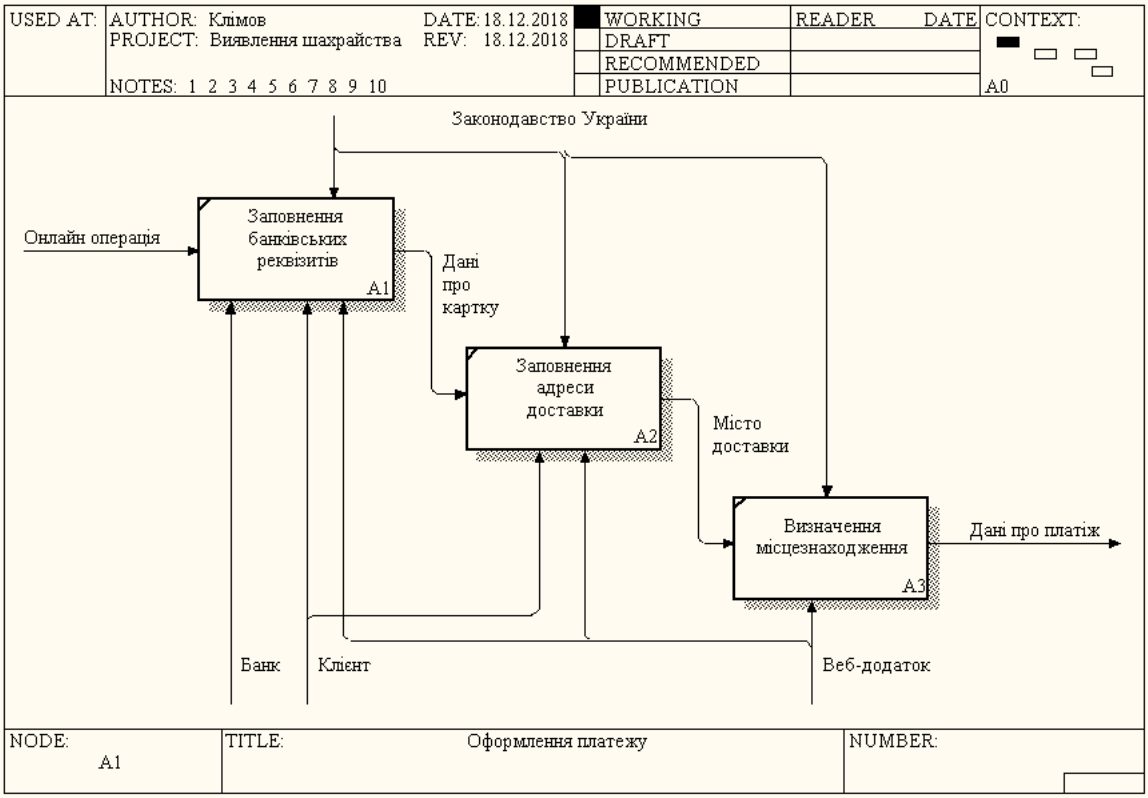


Рисунок 4.19 – Діаграма-декомпозиція процесу «оформлення платежу»

Таблиця 4.14 – 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 4.20. Детальний опис поданої діаграми наведемо в наступній таблиці 4.15.

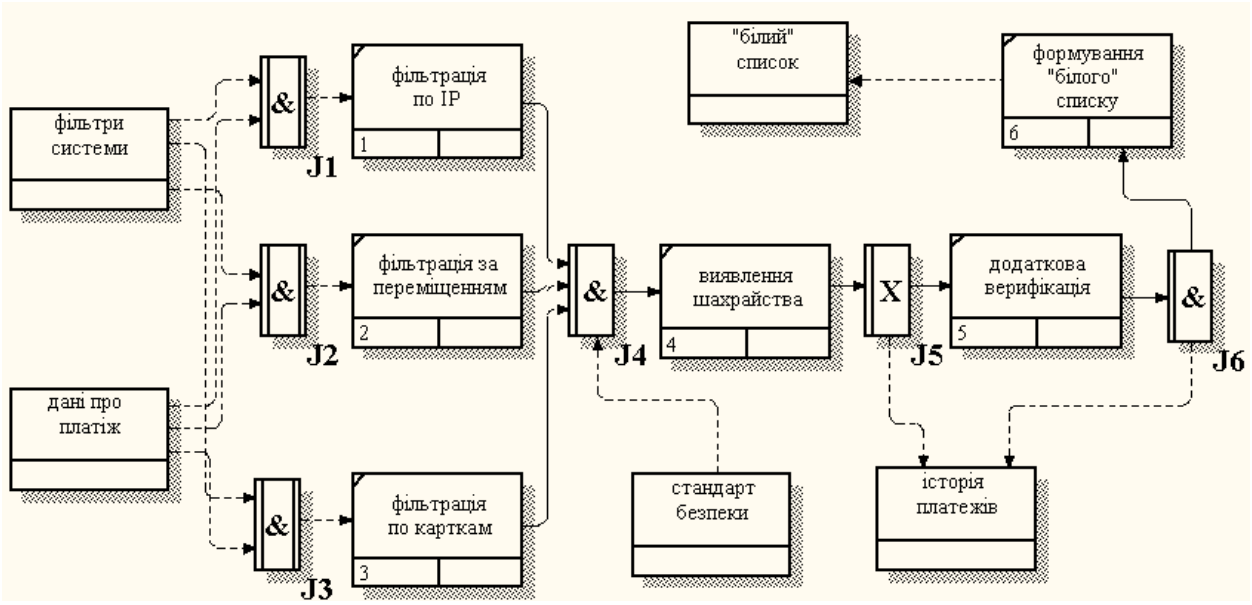


Рисунок 4.20 – IDEF3 діаграма системи виявлення шахрайства

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 4.15 – 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, які використовуються 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 4.16 – 4.21).

Таблиця 4.16 – 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 4.17 – 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 4.18 – 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 4.19 – 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 4.20 – 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 4.21 – 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 4.21).

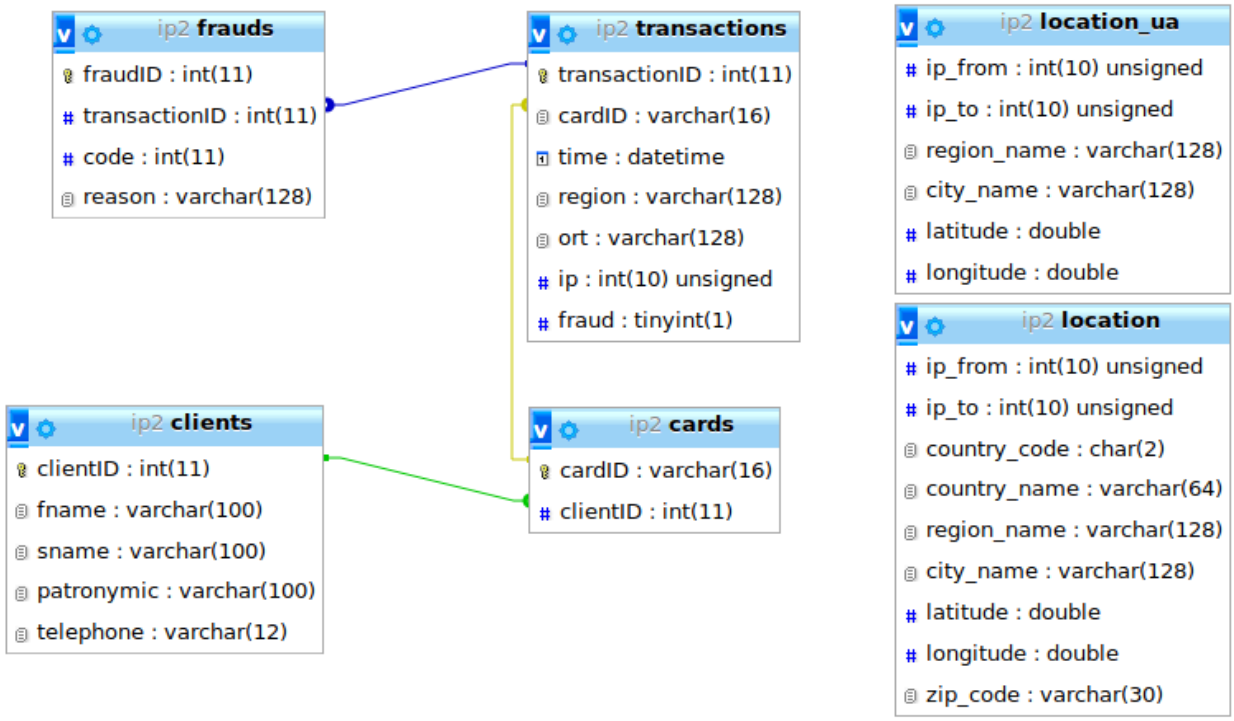


Рисунок 4.21 – Схема бази даних автоматизованого модуля виявлення шахрайських операцій з картками

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.

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 4.22-4.25).

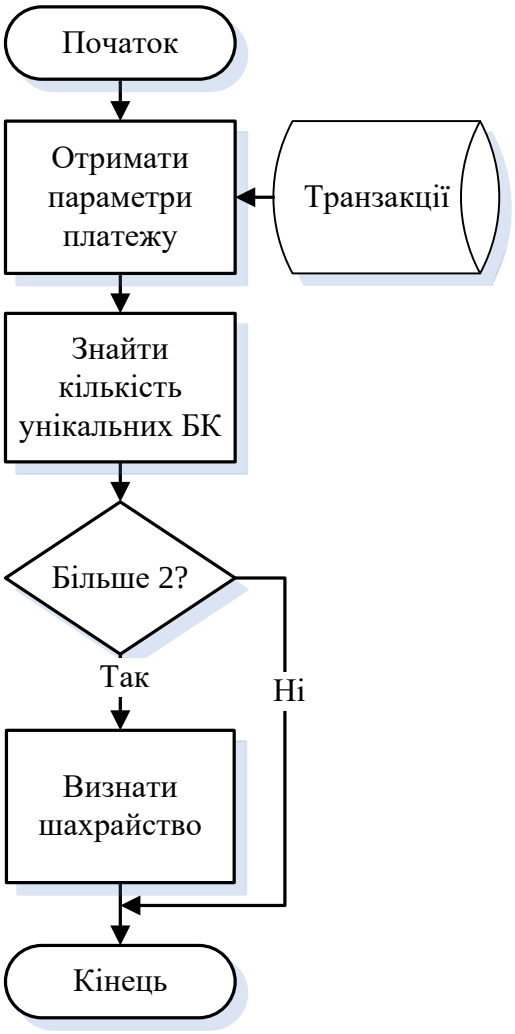


Рисунок 4.22 – Блок-схема алгоритму фільтрування за кількістю карт

Логіка алгоритму, продемонстрованого на рисунку 4.22, 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.

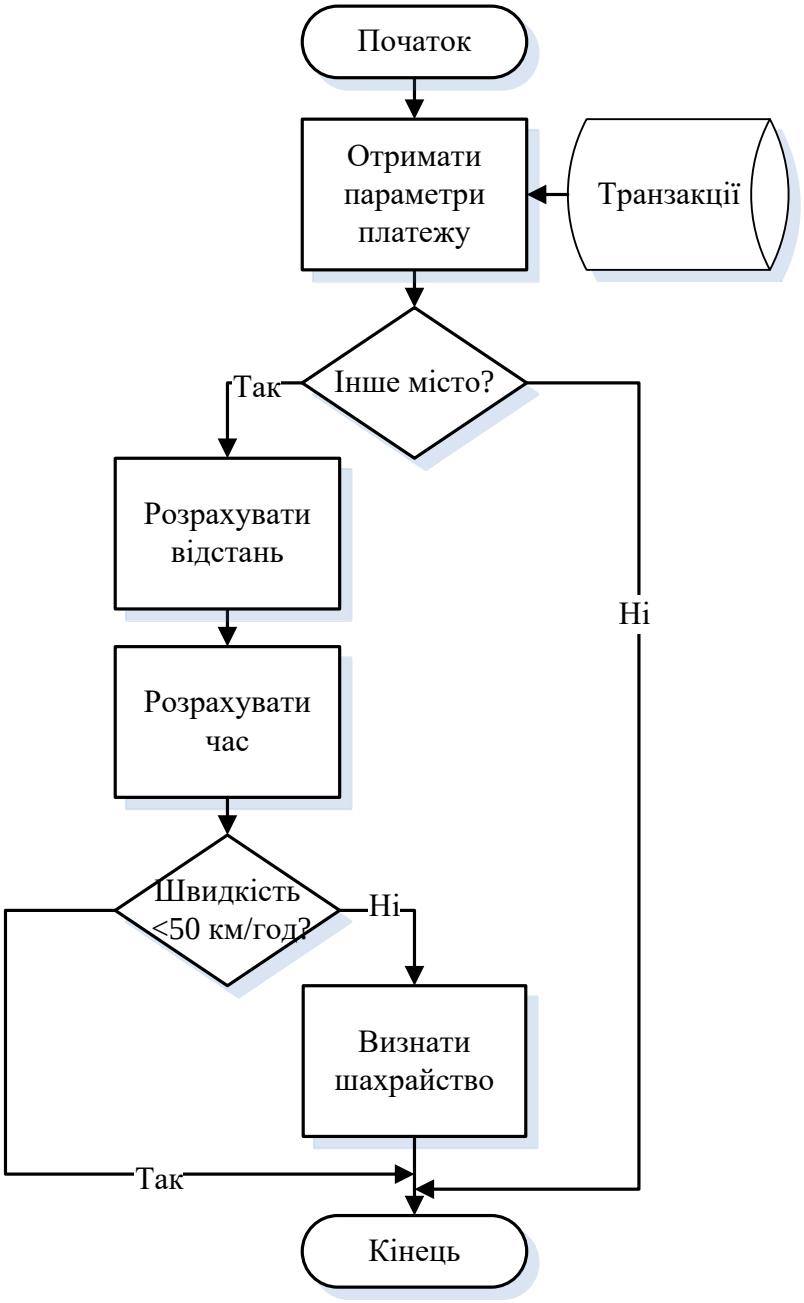


Рисунок 4.23 – Блок-схема алгоритму фільтрування за швидкістю переміщення клієнта

Рисунок 4.23 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.

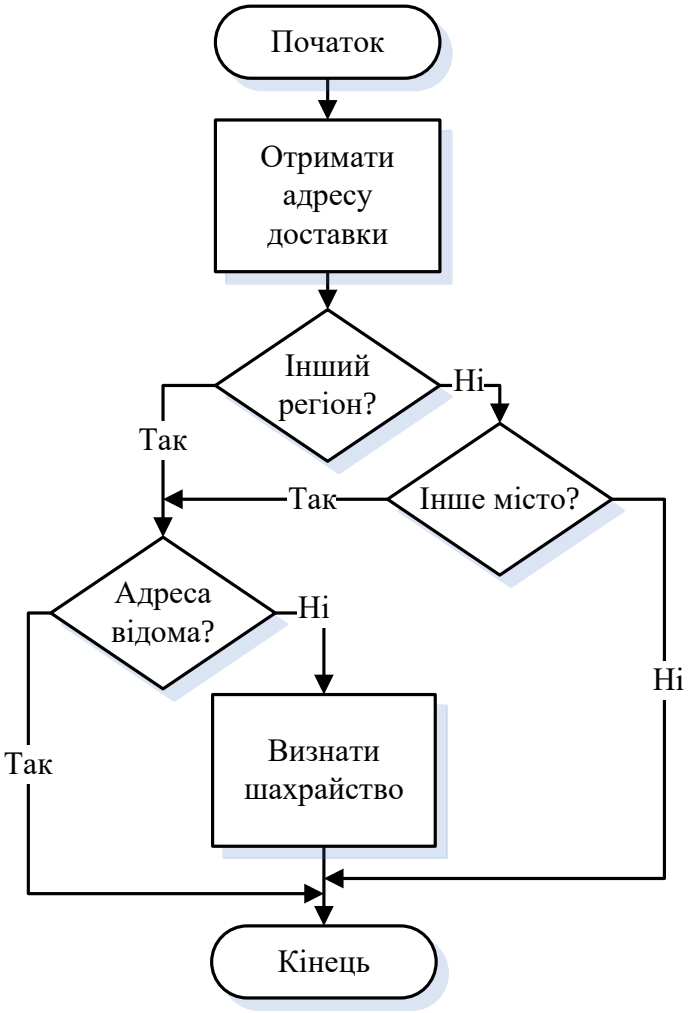


Рисунок 4.24 – Блок-схема алгоритму фільтрування за місцем знаходження та доставки

Робота даного фільтру 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.

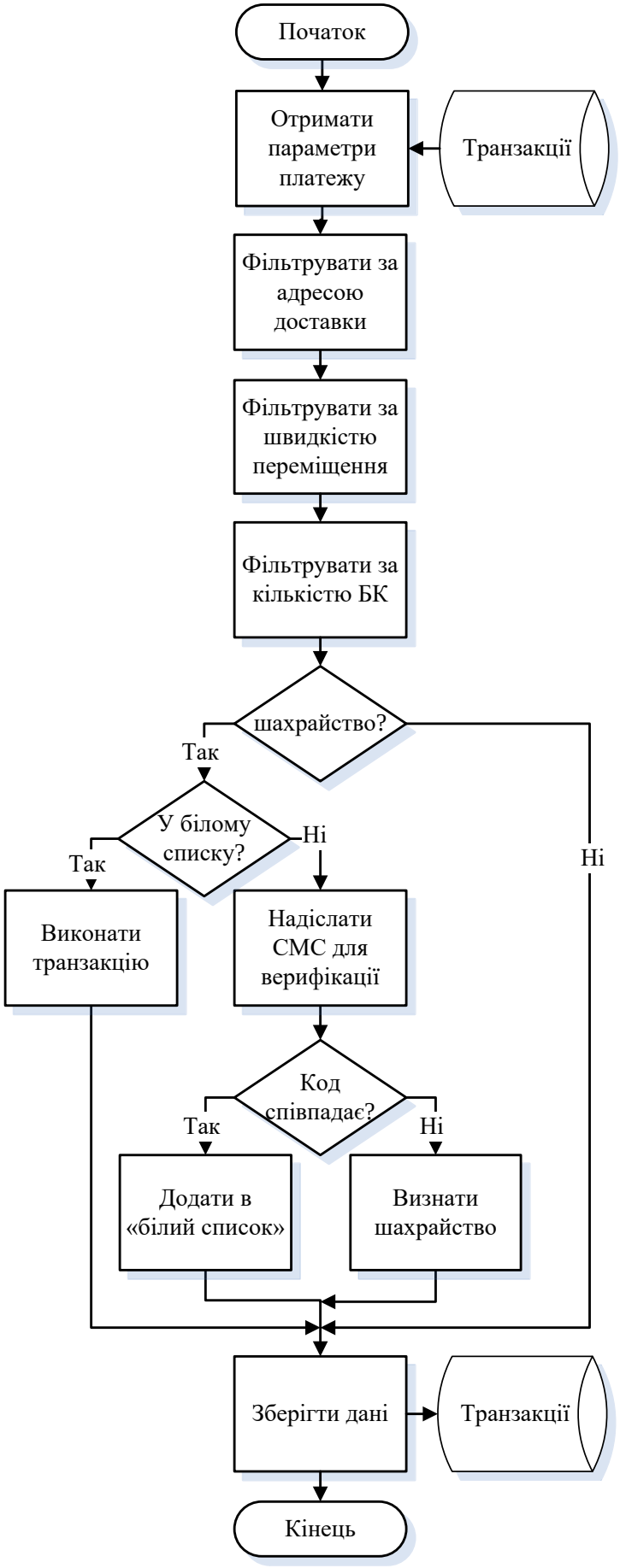


Рисунок 4.25 – Загальний вигляд алгоритму модулю виявлення шахрайства

На рисунку 4.25 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 4.1), який відповідає за аналіз часу та місцем знаходження клієнта між платежами:

Лістинг 4.1 – 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 4.25, 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 4.26). 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.

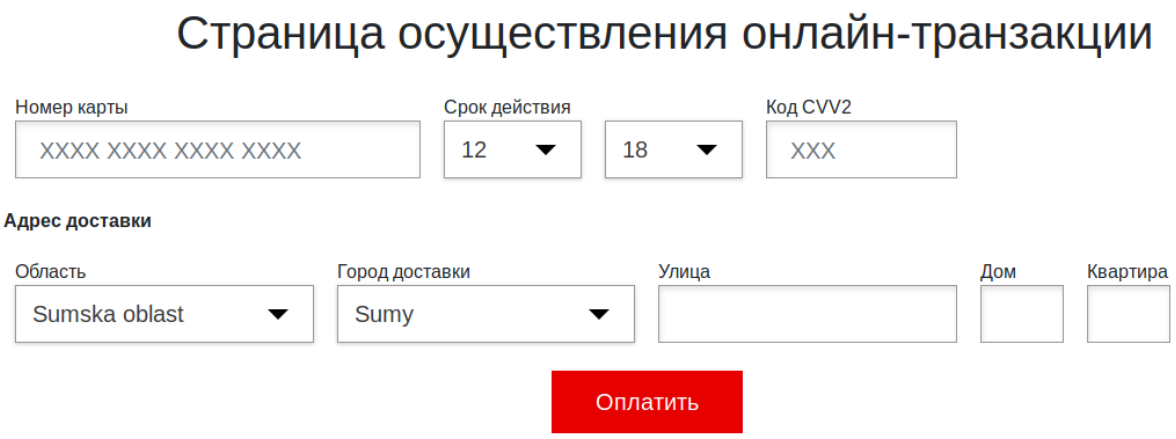


Рисунок 4.26 – Вікно здійснення онлайн-платежу

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.

У випадку виявлення шахрайства виконання транзакції призупиняється і виконується запит до SMS API Service. На мобільний телефон клієнта приходить повідомлення із кодом (рисунок 4.27), який необхідно ввести у форму (рисунок 4.28). 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.

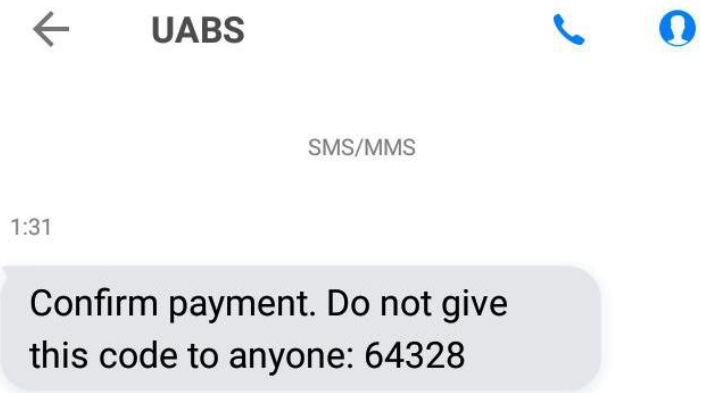


Рисунок 4.27 – СМС з кодом підтвердження

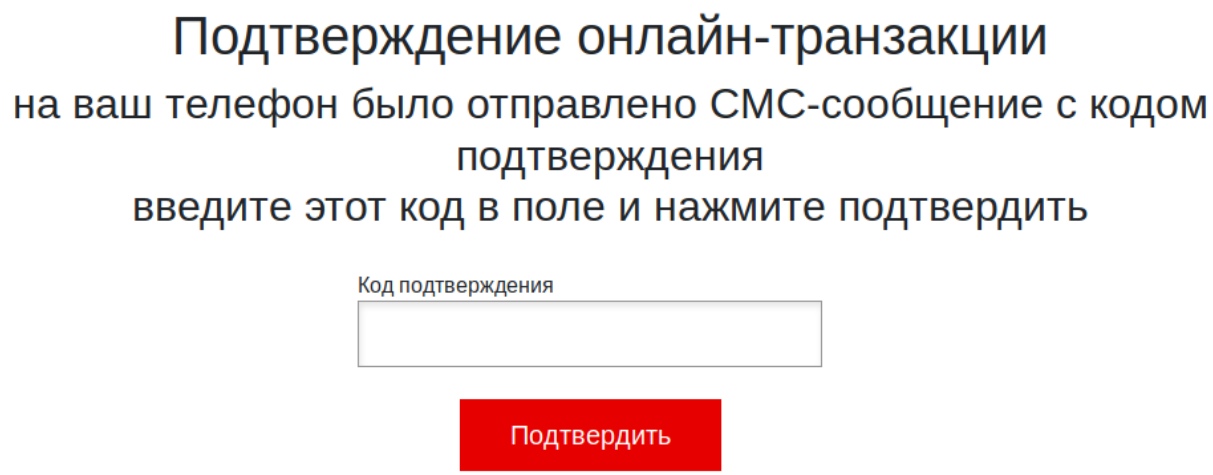


Рисунок 4.28 – Вікно підтвердження платежу

Лістинг 4.2 – 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 4.29). 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.

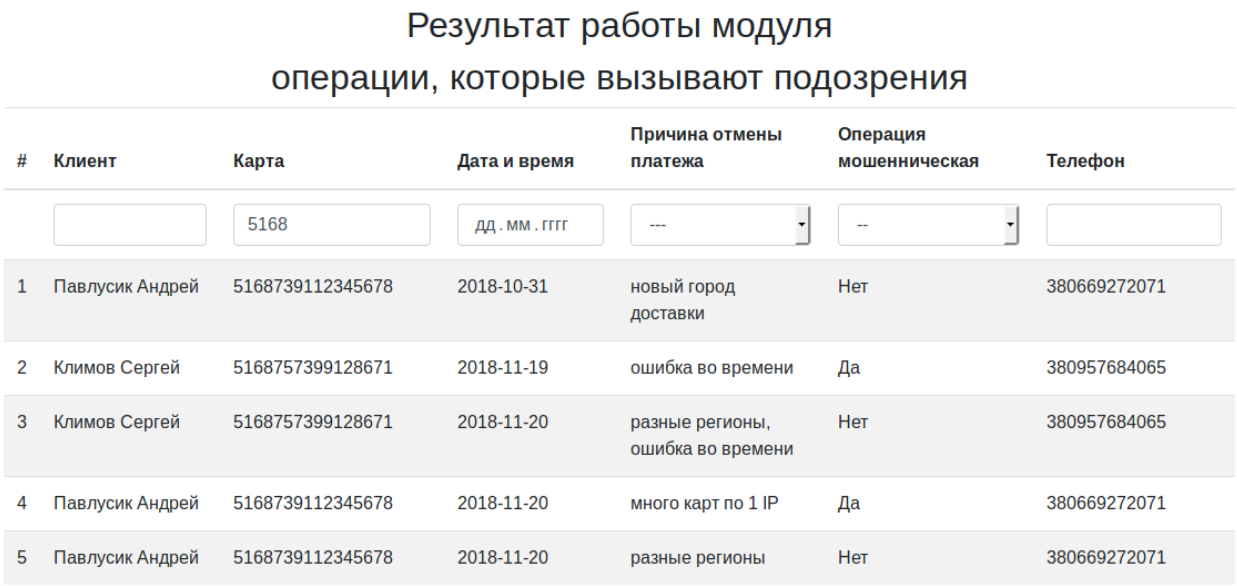


Рисунок 4.29 – Вікно виведення шахрайських операцій

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

Автоматизоаний 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.

ВИСНОВКИ

Отримані 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, щляхом 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.

Подальші дослідження повинні бути спрямовані на: розробку методичних рекомендацій щодо організації системи незалежного аудиту для попередження шахрайств персоналом банку, які дозволять комерційним банкам сформувати комплекс превентивних заходів у даній сфері; розробку алгоритмів інтелектуального програмного забезпечення для виявлення та попередження шахрайств в банках.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Данилов В. Кибербезопасность в банковской сфере [Електронний ресурс] / В. Данилов. – Режим доступу : https://icf.ua/blog/view/kiberbezopasnost-v-bankovskoy-sfere

2. Проект Стратегії забезпечення кібернетичної безпеки України [Електронний ресурс]. – Режим доступу : http://www.niss.gov.ua/public/File/2013_nauk_an_rozrobku/kiberstrateg.pdf

3. The Top Five Security Threats to Your Banking Institution [Електронний ресурс]. – Режим доступу : http://www.level3.com/-/media/files/infographics/en_infg_financialserv_topnetworksecuritythreats_regionalbanks.pdf

4. DoS-атака [Електронний ресурс] – Режим доступу: https://ru.wikipedia.org/wiki/DoS-атака

5. Qijun Gu, Peng Liu Denial of Service Attacks [Електронний ресурс] / Qijun Gu, Peng Liu. – Режим доступу: https://s2.ist.psu.edu/paper/DDoS-Chap-Gu-June-07.pdf

6. K. Munivara Prasad, A. Rama Mohan Reddy, K. Venugopal Rao. DoS and DDoS Attacks: Defense, Detection and Traceback Mechanisms – A Survey [Електронний ресурс] – Режим доступу: https://globaljournals.org/GJCST_Volume14/3-DoS-and-DDoS-Attacks-Defense-Detection.pdf

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 [Електронний ресурс]. – Режим доступу : http://www.level3.com//media/files/infographics/en_infg_financialserv_topnetworksecuritythreats_regionalbanks.pdf

9. IT threat evolution Q3 2017. Statistics [Електронний ресурс]. – Режим доступу : https://securelist.com/it-threat-evolution-q3-2017-statistics/83131/

10. Головна мобільна кіберзагроза [Електронний ресурс]. – Режим доступу : http://www.ohrana-ua.com/articles/837-golovna-moblna-kberzagroza.html

11. The official site of the company “SAS” (2016), “SAS Enterprice Miner. Solution Overview”, available at: https://www.sas.com/content/dam/SAS/ru_ru/doc/factsheet/sas-enterprise-miner-04-04-2016.pdf

12. Чернышова Г.Ю. Интеллектуальный анализ данных: учебное пособие для студентов / Г.Ю.Чернышова. – Саратов: Саратовский государственный социально-экономический университет, 2012. – 92 с.

13. Барсегян А. А., Куприянов М. С., Степаненко В. В., Холод И. И. Б26. Методы и модели анализа данных: OLAP и Data Mining. – СПб.: БХВ-Петербург, 2004. – 336 с.

14. Бахрушин В.Є. Методи аналізу даних : навчальний посібник для студентів /. В.Є. Бахрушин. – Запоріжжя : КПУ, 2011. – 268 с.

15. Кластерний аналіз [Електронний ресурс] – Режим доступу: http://uk.wikipedia.org/wiki/Кластерний_аналіз

16. Яровенко Г.М. Моделювання виявлення ознак кіберзагроз в банках із використанням інтелектуального аналізу [Електронний ресурс] / Г.М. Яровенко, А.І. Сковронська, М.М. Бояджян // Ефективна економіка. - 2018. - № 7. - Заголовок з екрану. – http://www.economy.nayka.com.ua/pdf/7_2018/39.pdf

17. Ryan C. Hybrid Risk: The truth behind first party fraud [Електронний ресурс] / Chris Ryan // The official site of the company "Experian". – 2015. – Режим доступу до ресурсу: http://www.experian.com/blogs/insights/2015/10/hybrid-risk-the-truth-behind-first-party-fraud/.

18. Third Party Fraud [Електронний ресурс] // Open Risk Manual. – 2017. – Режим доступу до ресурсу: https://www.openriskmanual.org/wiki/Third_Party_Fraud.

19. #FraudStats [Електронний ресурс] // The official site of the company "Experian". – 2018. – Режим доступу до ресурсу: https://www.experian.co.uk/identity-and-fraud/fraud-statistics/.

20. What is Mortgage Fraud? [Електронний ресурс] // MortgageLoan.com. – 2015. – Режим доступу до ресурсу: https://www.mortgageloan.com/.

21. Яровенко Г.М. Моделювання портретів потенційних шахрая та жертви банківських шахрайств [Електронний ресурс] / Г.М. Яровенко, В.О. Ковач // Ефективна економіка. - 2018. - № 10. - Заголовок з екрану. – http://www.economy.nayka.com.ua/pdf/10_2018/63.pdf

22. Яровенко Г.М. Розробка інформаційної моделі виявлення ознак шахрайств у банках / Г.М. Яровенко // Інвестиції: практика та досвід. – 2018. - № 14. – С. 23-28.

23. AllFusion® Process Modeler Data Flow Diagramming. Design Guide r7.2 [Електронний ресурс] // The official site of the company “CA”. – 2006. – Режим доступу до ресурсу: https://supportcontent.ca.com/cadocs/0/e002761e.pdf.

24. Business Process Model and Notation (BPMN) Version 2.0 [Електронний ресурс] // The official site of the company “Object Management Group”. – 2011. – Режим доступу до ресурсу: http://www.omg.org/spec/BPMN/2.0.

25. Рекомендації щодо зниження ризику шахрайських операцій НБУ 04.07.2018 № 57-0009/36366 http://zakon.rada.gov.ua/laws/show/v3636500-18. [Електронний ресурс] - Режим доступу: http://nbuv.gov.ua/UJRN/vamcudu_2015_1_23.

26. 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. С. О. Дмитрова . – Суми : ДВНЗ “УАБС НБУ”, 2010. – 264 с.

27. Кібальник Л. О. Концептуальний підхід до формування інформаційної безпеки банківських установ в системі економічної безпеки [Електронний ресурс] / Л. О. Кібальник, І. Ю. Напора // Ефективна економіка. - 2016. - № 12. Режим доступу: http://www.economy.nayka.com.ua/?op=1&z=5303.

28. ГСТУ СУІБ 1.0/ISO/IEC 27001:2010, Інформаційні технології - методи захисту – система управління інформаційною безпекою. Офіційний переклад, ст.3.

29. Щодо впровадження системи управління інформаційною безпекою та методики оцінки ризиків відповідно до стандартів Національного банку України [Електронний ресурс] : методичні рекомендації від 03.03.2011 № 24-112/365. – Режим доступу : http://document.ua/shodo-vprovadzhennja-sistemi-upravlinnja-informaciinoyu-bezp-doc49593.html.

30. Про організацію заходів із забезпечення інформаційної безпеки в банківській системі України [Електронний ресурс] : положення, затверджене Постановою Правління НБУ від 28 вересня 2017 року№ 95. – Режим доступу : https://bank.gov.ua/document/download?docId=56426049.

31. Щодо організації та функціонування систем ризик-менеджменту в банках України [Електронний ресурс] : методичні рекомендації, схвалені Постановою Правління НБУ від 02 серпня 2004 № 361. – Режим доступу : http://zakon.nau.ua/doc/?uid=1045.5945.1&nobreak=1.

32. Иванов С.В. Преимущества генетических алгоритмов и их применение в медицине / С.В. Иванов // Актуальные проблемы гуманитарных и естественных наук. – 2014. – Вып.10. – С. 44-47.

33. Нейман Дж. Теория игр и экономическое поведение / Дж. Нейман, О. Моргенштерн. – М.: Наука, 1970. – 708 с.

34. Кривошапова С. В. Оценка и способы борьбы с мошенничеством с банковскими картами / С.В. Кривошапова, Е.А. Литвин // Международный журнал прикладных и фундаментальных исследований. – 2015. – Вып. 4. – С. 116–120.

35. Буреева Н.Н. Многомерный статистический анализ с использованием ППП “STATISTICA”. Учебно-методический материал по программе повышения квалификации «Применение программных средств в научных исследованиях и преподавании математики и механики» / Н.Н. Буреева. – Нижний Новгород, 2007. – 112 с.

36. Барсегян А. А. Методы и модели анализа данных: OLAP и Data Mining. / Барсегян А. А., Куприянов М. С., Степаненко В. В. – СПб.: БХВ. Петербург, 2004. – 336 с.

37. Згуровський М.З. Основи системного аналізу / Згуровський М.З., Панкратова Н.Д. – К.: Видав. група BHV, 2007. – 544 с.

38. Кузьменко О.В. Моделювання оцінювання рівня економічного, соціального та політичного розвитку України, Італії та Франції в контексті оптимізації їх взаємодії / О.В. Кузьменко, О.В. Колотіліна // Сталий розвиток економіки. – 2018. - №2(39). - С. 111-120.

39. Kuzmenko O.V. Practical aspects of modeling the stable political and economic situation in the country on the basis of multi-criteria optimization methods / O.V. Kuzmenko // Journal of Strategic and International Studies. – 2014. – № 4. – Volume IX. – P. 17-24.

40. 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.

41. Business Process Model and Notation (BPMN) version 2.0. [Електронний ресурс] // The official site of the company «Object Management Group». – 2011. – Режим доступу : http://www.omg.org/spec/BPMN/2.0

42. PHP Manual [Електронний ресурс] – Режим доступу : https://secure.php.net/manual/en/intro-whatcando.php

43. Lyeonov S.V. Macroeconomic stability evaluation in countries of lower-middle-income economies / S.V. Lyeonov, T.A. Vasylieva, O.V. Lyulyov // Вісник національного гірничого університету. – 2018. – № 1. – С. 138-146.

44. Vasylieva, T. Macroeconomic Stability and Its Impact on the Economic Growth of the Country / Vasylieva, T., Lyeonov, S., Lyulyov, O., & Kyrychenko, K. // Montenegrin Journal of Economics (Scopus). – 2018. - 14(1), 159-170.

45. Яровенко Г.М. Аналіз наслідків кібершахрайств в банківській системі України [Електронний ресурс] / Г.М. Яровенко, М.М. Бояджян // Економіка та

суспільство. – 2018. - № 18. - С. 836-843. - Заголовок з екрану. – http://www.economyandsociety.in.ua/journal/18_ukr/116.pdf

46. Кузьменко В.О., Овчаренко В.О. Оцінювання впливу інноваційних технологій на ринок банківських послуг України // Бізнес-інформ. - 2018. - № 2. - С. 121- 127

47. Левченко В.П., Бойко А. О., Доценко Т. В. Оцінювання збитків банків від їх залучення до процесу легалізації кримінальних доходів // "Причорноморські економічні студії" Випуск 35/2018. - 2018.

48. Babenko V. Analysis of the current state of development of electronic commerce market in Ukraine / Babenko V., Syniavska O. // Technology audit and production reserves. – Vol 5, NO 4(43), 2018. – С. 40-45.

49. Яровенко Г.М. Системний підхід до побудови інформаційної моделі виявлення передумов виникнення шахрайств в банках / Г.М. Яровенко // Матеріали Міжнародної науково-практичної конференції «Актуальні проблеми моделювання та управління соціально-економічними системами в умовах глобалізації». – Дрогобич, 2018. – С. 66-69

50. Яровенко Г.М. Концептуальна модель виявлення ознак кібершахрайств в банках / Г.М. Яровенко, М.М. Бояджян // Сучасні міжнародні економічні відносини: становлення та шляхи перспективного розвитку: збірник тез наукових робіт учасників Всеукраїнської науково-практичної конференції (м. Одеса, 9-10 лютого 2018 р.) / ГО «Центр економічних досліджень та розвитку». – О. : ЦЕДР, 2018. – С. 98-100.

51. Синявська О.О. Застосування моделей економічної динаміки при моделюванні процесу боротьби із шахрайськими атаками / О.О. Синявська // Моніторинг, моделювання та менеджмент емерджентної економіки : зб. наукових праць Сьомої Міжнародної наук.-практ. конференції, Одеса-Черкаси, 23-25 травня 2018 р. / Редкол. Кібальник Л.О., Соловйов В.М. (відп. за випуск) та ін. - Черкаси : в-во Вовчок О.Ю., 2018. - С. 232-234.

52. Кузьменко О.В. Структурне моделювання впливу інноваційних технологій на ринок банківських послуг України / О.В. Кузьменко, В.О.

Овчаренко // Моніторинг, моделювання та менеджмент емерджентної економіки : зб. наукових праць Сьомої Міжнародної наук.-практ. конференції, Одеса-Черкаси, 23-25 травня 2018 р. / Редкол. Кібальник Л.О., Соловйов В.М. (відп. за випуск) та ін. - Черкаси : в-во Вовчок О.Ю., 2018. - С. 165-169

53. 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

54. Бояджян М.М. Моделювання виявлення ознак кіберзагроз в банках із використанням інтелектуального аналізу // Матеріали ІІ туру Всеукраїнського конкурсу студентських наукових робіт у 2017/2018 н.р / за ред. проф. В.М, Вовка. - Львів : Видавничий центр ЛНУ ім. І.Франка, 2018. - С. 29-31.

55. Гриценко К.Г. Нечітко-множинна модель оцінки рівня захищеності банку від кібершахрайств / К.Г.Гриценко // Математичне та програмне забезпечення інтелектуальних систем: тези доповідей XVI Міжнародної науково-практичної конференції MPZIS-2018, Дніпро, 21-23 листопада 2018 р. / Під загальною редакцією О.М. Кисельової. – Дніпро: ДНУ, 2018. – С. 47-48

56. 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 : збірник матеріалів ІІІ Всеукраїнської науково-практичної on-line конференції (22-23 листопада 2018 року) / Навчально-науковий інститут бізнес-технологій «УАБС» Сумського державного університету. – Суми : ННІ БТ «УАБС» СумДУ, 2018. – С. 294-297

57. Яровенко Г. М., Клімов С. В. Система виявлення шахрайських операцій з банківськими картками // Проблеми та перспективи розвитку фінансово-кредитної системи України : збірник матеріалів ІІІ Всеукраїнської науково-практичної on-line конференції (22-23 листопада 2018 року) / Навчально-

науковий інститут бізнес-технологій «УАБС» Сумського державного університету. – Суми : ННІ БТ «УАБС» СумДУ, 2018. – С. 303-307

58. Кузьменко О. В., Попова З. В. Визначення та аналіз факторів для економетричного моделювання корупційних правопорушень та шахрайства у банківському секторі України // Проблеми та перспективи розвитку фінансово-кредитної системи України : збірник матеріалів ІІІ Всеукраїнської науково-практичної on-line конференції (22-23 листопада 2018 року) / Навчально-науковий інститут бізнес-технологій «УАБС» Сумського державного університету. – Суми : ННІ БТ «УАБС» СумДУ, 2018. – С. 311-316

59. Syniavska O. O. Investigation Of The Process Of Combating Bank Fraud By The Method Of System Dynamics / O. O. Syniavska // Цифрова економіка: зб. мат. Національної наук.-метод. конф., 4–5 жовтня 2018 р., м. Київ. — К.: КНЕУ, 2018. — С. 26-28

60. Доценко Т.В., Овчаренко В.О. Оцінювання фінансового стану позичальника в новітніх умовах господарювання // ІІ Всеукраїнська науково-практична інтернет-конференція студентів, аспірантів та молодих вчених "Сучасні інструменти управління корпоративними фінансами" (5 грудня 2018 р.). – Київ: ДВНЗ «Київський національний економічний університет імені Вадима Гетьмана». – 2018.

ДОДАТКИ

Додаток А

(довідковий)

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

(довідковий)

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

(довідковий)

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/bootst
rap.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/bootst
rap.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/bootst
rap.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/po
pper.min.js" integrity="sha384-
ZMP7rVo3mIykV+2+9J3UJ46jBk0WLaUAdn689aCwoqbBJiSnjAK/l8WvCWPIPm49"
crossorigin="anonymous"></script>
<script
src="https://stackpath.bootstrapcdn.com/bootstrap/4.1.3/js/bootstra
p.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');
          });
    });
```