Міністерство освіти і науки України
Сумський державний університет
Навчально-науковий інститут бізнес-технологій «УАБС»

СУЧАСНІ ІНСТРУМЕНТИ БОРОТЬБИ З КІБЕРШАХРАЙСТВАМИ У БАНКАХ

Монографія

За загальною редакцією О. В. Кузьменко, Г. М. Яровенко

Рекомендовано вченою радою Сумського державного університету

Суми
Видавництво "Ярославна"
2018

УДК 303.09:336.717.1

Авторський колектив:
О. В. Кузьменко, доктор економічних наук;
Г. М. Яровенко, кандидат економічних наук;
С. В. Лєонов, доктор економічних наук;
О. А. Криклій, кандидат економічних наук;
К. Г. Гриценко, кандидат технічних наук;
О.О. Пушко, кандидат економічних наук;
Я. В. Самусевич, кандидат економічних наук;
Т. В. Доценко, аспірант кафедри економічної кібернетики;
М. М. Бояджян, магістр економічної кібернетики;
В. О. Ковач, магістр економічної кібернетики;
С.В. Клімов, магістр економічної кібернетики.

Рецензенти:
І. О. Школьник – доктор економічних наук, професор, завідувач кафедри фінансів, банківської справи та страхування Науково-навчального інституту бізнес-технологій «УАБС» Сумського державного університету (м. Суми);
П. М. Григорук – доктор економічних наук, професор, завідувач кафедри автоматизованих систем і моделювання в економіці Хмельницького національного університету (м. Хмельницький);
О. В. Лебідь – кандидат економічних наук, доцент, професор кафедри банківської справи і фінансових послуг Харківського національного економічного університету ім. С. Кузнеця (м. Харків).

Рекомендовано до видання вченою радою
Сумського державного університету як
монографія (протокол № 6 від 15.11. 2018 року)

Сучасні інструменти боротьби з кібершахрайствами у банках : Монографія / О. В. Кузьменко, Г.М. Яровенко, С. В. Лєонов та ін. ; за заг. ред. О. В. Кузьменко, Г. М. Яровенко. – Суми: видавництво "Ярославна", 2018. – 144 с.
ISBN 978-966-7538-52-1

Монографія складається із чотирьох частин. У першій частині «Концептуальні основи мінімізації операційних банківських ризиків в сфері інформаційної безпеки» викладено науково-методичний підхід до операційних ризиків, як складової інформаційної безпеки, з боку його моделювання та стандартизації. У другій частині «Аналіз та оцінка наслідків кібершахрайств у банках» зосереджено увагу на оцінці впливу макроекономічних факторів на формування схильності до шахрайства, моделювання збитків банків від їх залучення до шахрайських операцій. Третя частина «Математичне моделювання як інструмент попередження кібершахрайств у банках» базується на застосуванні інтелектуального аналізу, нечітких множин та динамічного моделювання для попередження кібершахрайств. У четвертій частині «Розробка комплексу автоматизованих превентивних заходів попередження шахрайств» наведено інформаційну модель та прототип автоматизованого модулю процесу виявлення шахрайських операцій з банківськими картками.

Монографія призначена для студентів і викладачів вищих навчальних закладів, аналітиків, фахівців кібербезпеки банків.

УДК 303.09:336.717.1

ISBN 978-966-7538-52-1

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.

Монографія складається із чотирьох частин. У першій частині «Концептуальні основи мінімізації операційних банківських ризиків в сфері інформаційної безпеки» викладено науково-методичний підхід до операційних ризиків, як складової інформаційної безпеки, з боку його моделювання та стандартизації. У другій частині «Аналіз та оцінка наслідків кібершахрайств у банках» зосереджено увагу на оцінці впливу макроекономічних факторів на формування схильності до шахрайства, моделювання збитків банків від їх залучення до шахрайських операцій. Третя частина «Математичне моделювання як інструмент попередження кібершахрайств у банках» базується на застосуванні інтелектуального аналізу, нечітких множин та динамічного моделювання для попередження кібершахрайств. У четвертій частині «Розробка комплексу автоматизованих превентивних заходів попередження шахрайств» наведено інформаційну модель та прототип автоматизованого модулю процесу виявлення шахрайських операцій з банківськими картками.

Окремі підрозділи монографії підготували: підрозділи 1.3, 2.3 - доктор економічних наук, професор Кузьменко О.В.; підрозділи 2.1, 2.2, 3.1, 3.2, 4.1, 4.2, вступ та висновки - кандидат економічних наук, доцент Яровенко Г.М.; підрозділ 1.4 - доктор економічних наук, професор Лєонов С.В.; підрозділи 1.1, 1.2 - кандидат економічних наук, доцент Криклій О. А.; підрозділ 3.3 – кандидат технічних наук, доцент Гриценко К.Г.; підрозділ 3.4 – кандидат економічних наук Пушко О.О., підрозділ 1.4 - кандидат економічних наук Самусевич Я.В.; підрозділи 1.3, 2.3 - аспірант кафедри економічної кібернетики Доценко Т.В.; підрозділи 2.1, 2.2, 3.2 - магістр економічної кібернетики Бояджян М.М.; підрозділ 3.1 - магістр економічної кібернетики Ковач В.О.; підрозділ 4.2 - магістр економічної кібернетики Клімов С.В.

Монографія виконана в рамках держбюджетної науково-дослідної роботи № 0118U003574 «Кібербезпека в боротьбі з банківськими шахрайствами: захист споживачів фінансових послуг та зростання фінансово-економічної безпеки України».

1. КОНЦЕПТУАЛЬНІ ОСНОВИ МІНІМІЗАЦІЇ ОПЕРАЦІЙНИХ БАНКІВСЬКИХ РИЗИКІВ В СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1 Сутність операційного ризику банку та класифікації, що використовуються в системі управління ним в сфері інформаційної безпеки

Основною причиною, що зумовила підвищення уваги органів банківського нагляду та вітчизняних банків до управління інформаційною безпекою (ІБ), є постійне зростання рівня зовнішніх та внутрішніх загроз у цій сфері та значні масштаби прямих збитків та опосередкованих втрат у разі їх реалізації.

Банківські інформаційні системи чутливі до значної кількості загроз, що генеруються зовнішніми шкідливими та злочинними діями або помилками користувачів банківських послуг, внутрішнім середовищем банку (помилками чи шахрайством персоналу), а також обумовлених природними та техногенними катастрофами. Це обумовлено тим, що банки:

- зберігають та обробляють надвелику кількість даних про фінансовий стан та діяльність фізичних та юридичних осіб, клієнтів та контрагентів, інших банківських та фінансових установ;
- мають інструменти здійснення транзакцій, щопризводять до фінансових наслідків;
- не можуть бути повністю закритими, оскільки мають відповідати сучасним вимогам до рівня обслуговування клієнтів в частині дистанційного обслуговування.

На зростання значущості забезпечення інформаційної безпеки та зростання рівня ризиків ІБ банку впливатимуть наступні ключові довгострокові тенденції банківського бізнесу:

1) розвиток систем зв'язку, що є фундаментальним драйвером змін у сфері доставки фінансових послуг та взаємодії з клієнтами;

2) інтеграція – збільшення інтеграції інформаційних потоків та додатків, що трансформуватиме потік фінансової інформації та архітектуру фінансових додатків;

3) модуляризація – інтеграційні технології призводять до розвитку «модульної економіки», в якій бізнес-процеси розбиваються на дрібні елементи, що можуть об'єднуватись в організаційних та національних межах.

Порушення принципів цілісності, доступності, правдивості інформації, відсутність контролю над зміною інформації або можливість несанкціонованого доступу до неї можуть стати не тільки причиною значних збитків окремого банку, а й призвести до повної зупинки банківських бізнес-процесів.

Оскільки банківська система – це частина критичної інфраструктури країни, перебої в її роботі можуть привести до дестабілізації фінансової та економічної систем. Прикладом цього може слугувати масштабна кібератака 2017 року, проведена за допомогою вірусу Petya.A, спрямована на об'єкти критичної інформаційної інфраструктури України, зокрема банків. При цьому, за даними НБУ, від кібератаки різною мірою постраждали близько 30 українських банків.

Зважаючи на зазначене, питання забезпечення інформаційної безпеки банків України набуває особливо актуального значення.

Для досягнення мети дослідження необхідно дослідити сутність поняття «інформаційна безпека банку». За результатами вивчення наукових робіт з цієї тематики нами визначено наступні підходи авторів до визначення цього поняття. ІБ банку розглядається:

1. як стан захищеності, при цьому в різних джерелах визначаються різні об'єкти, на яких поширюються необхідність забезпечення інформаційної безпеки:
   - всіх інформаційних активів банку від внутрішніх та зовнішніх загроз. При цьому під інформаційними активами розуміють будь-яку інформацію, що має цінність для банку, систему її обробки або місце зберігання [1];
   - систем оброблення та зберігання даних, при якому забезпечено конфіденційність, доступність та цілісність інформації, або комплекс заходів, спрямованих на забезпечення

захищеності інформації від несанкціонованого доступу, використання, оприлюднення, руйнування, внесення змін, ознайомлення, перевірки, запису чи знищення [2, 3];

- інформації та інфраструктури, що її підтримує, від випадкових або навмисних дій природного або штучного характеру, що можуть завдати неприйнятного збитку суб'єктам інформаційних відносин, зокрема, власникам та користувачам інформації та інфраструктури, що її підтримує [4];

- інформаційних ресурсів банку від внутрішніх та зовнішніх посягань [5];

2. як сукупність засобів (організаційних, методичних, технічних) та способів, спрямованих на захист інформації від:

- загроз з метою забезпечення безперервності бізнес-процесів, зниження ризиків та оптимізації витрат банку [4];

- випадкових та навмисних загроз, у результаті реалізації яких можливе порушення сервісів (властивість) безпеки: доступності, цілісності, конфіденційності та спостережності [6];

- широкого діапазону загроз з метою забезпечення безперервності бізнесу, мінімізації ризику бізнес-процесів та отримання максимальної рентабельності інвестицій і бізнес-можливостей [7];

3. як безпеку, пов'язану з загрозами в інформаційній сфері, тобто це забезпечення захищеності сукупності властивостей інформаційної безпеки (доступності, цілісності, конфіденційності інформаційних активів) [8].

За результатами дослідження ІБ банку пропонуємо визначити як стан захищеності інформаційних активів та інформаційної інфраструктури, забезпечення збереження властивостей інформаційних активів банку (доступності, цілісності чи конфіденційності) на встановленому прийнятному рівні в умовах впливу зовнішніх та або / внутрішніх загроз.

Об'єктом системи забезпечення ІБ банку є інформаційні активи – матеріальні або нематеріальні об'єкти, що є інформацією або містять інформацію, слугують для обробки, зберігання або передачі інформації та мають цінність для банку. У межах внутрішніх політик та стратегій управління ІБ кожен банк самостійно визначає склад інформаційних активів, що розглядаються як об'єкти інформаційної безпеки. Основним критерієм для цього є значущість та цінність інформаційного активу для діяльності банку.

Основними типами інформаційних активів банку, чутливих до загроз інформаційній безпеці, є комерційна та банківська таємниця, конфіденційна інформація та персональні дані. На інформаційну безпеку банку вливає значна кількість загроз, що генерується як зовнішнім, так і внутрішнім середовищем. Зважаючи на це, необхідним є визначення та складу можливих негативних впливів (загроз) на інформаційні активи, способів реалізації та ступеня ймовірності реалізації цих загроз (уразливості ІБ банку).

Адаптуючи загальне розуміння поняття «загроза» до завдань дослідження, визначимо, що загроза ІБ банку – це потенційно можлива випадкова або навмисна подія, дія (вплив), процес або явище, що можуть призвести до втрати інформаційних активів та інформаційної інфраструктури, або порушення властивостей інформаційних активів (конфіденційності (при зберіганні та розповсюдженні інформації), цілісності (при зміні або знищення інформації), доступності інформації (в разі неотримання або несвоєчасного отримання інформації легальним користувачем)).

Ми погоджуємось з В. А. Матвеєвим, що реалізація загроз ІБ полягає в частковому або повному порушенні працездатності інформаційної системи, а також втраті цінності або частковому знеціненні інформації, що може призвести до прямих та непрямих втрат банку [9]. Узагальнивши розробки вчених, що займалися загальною класифікацією загроз, та поєднавши їх з розумінням поняття «інформаційна безпека банку», вважаємо за доцільне запропонувати наступні основні види загроз (табл. 1.1).

Таблиця 1.1 – Класифікація загроз ІБ банку [авторське узагальнення на основі 10, 11]

Ознака	Вид загрози
1	2
За джерелом	- внутрішні (втрата, знищення, викрадення, викривлення або розголошення інформації, витік інформації); - зовнішні (модифікація змісту, порушення конфіденційності, порушення логічної цілісності, порушення прав власності на інформацію, порушення фізичної цілісності, природні та техногенні катастрофи, що порушують нормальний режим роботи інформаційних систем тощо)
За походженням	- об'єктивні (природні), що характеризуються впливом на об'єкт захисту фізичних процесів або стихійних природних явищ, що не залежать відлюдини; - суб'єктивні, що характеризуються впливом на об'єкт захисту діяльністю людини; - результати соціальної інженерії (фішинг, фармінг, претекстинг, скрімінг та ін.)
За ступенем впливу на інформаційну систему	- пасивні без впливу на стан інформаційної системи; - активні з порушенням нормального процесу функціонування інформаційної системи банку
За цілеспрямованістю	- ненавмисні (помилкові, випадкові, необдумані, без злого наміру та корисливих цілей) дії персоналу та користувачів банківських послуг; - навмисні (в корисливих цілях, з примусу третіми особами, зі злим умислом тощо) персоналу, користувачів банківських послуг, злочинних груп та формувань, політичних і економічних структур, а також окремих осіб
За способом реалізації	- розголошення; - витік; - несанкціонований доступ.
За ступенем сформованості	- реальні; - потенційні.
За можливістю прогнозування	- прогнозовані; - не прогнозовані;
За ймовірністю виникнення	- реальна; - ймовірна; - малоймовірна; неймовірна.
За характером впливу	- явна, пряма (загрози, реалізація яких порушує безпеку інформаційних активів); - неявна, опосередкована (загрози, що створюють умови для появи прямих загроз);
За масштабами наслідків	- катастрофічні; - критичні; - середні; - незначні.
За можливістю нейтралізації	можливо нейтралізувати; можливо частково нейтралізувати; нейтралізувати неможливо.

Перелік способів реалізації загроз ІБ банку наведено в таблиці 1.2.

Таблица 1.2 – Перелік способів реалізації загроз ІБ банку [узагальнено автором]

Рівні ІБ	Об'єкти забезпечення ІБ банку	Способи реалізації загроз
Фізичний рівень	Фізичні носії інформації в складі систем зберігання даних; резервного копіювання; автоматизованих робочих місць. Знімні носії інформації Канали зв'язку. Монітори. Приміщення, будівлі, споруди. Технічні засоби ІС.	Розкрадання / крадіжка
		Знищення / руйнування / диверсії
		Несанкціонований фізичний доступ
		Витік інформації
Мережевий рівень	Комунікаційне обладнання.	Атаки «відмова в обслуговуванні»
		Підміна довіреного об'єкта мережі та передача за каналами зв'язку повідомлень від його імені з присвоєнням його прав доступу
		Порушення штатних режимів роботи мережевого обладнання
		Впровадження апаратних закладок
Рівень мережевих додатків і сервісів	Мережеві додатки та сервіси.	Впровадження шкідливого ПЗ
		Аналіз трафіку
		Атаки «відмова в обслуговуванні»
		Використання спеціалізованих програм
		Порушення штатних режимів роботи мережевих

Рівні ІБ	Об’єкти забезпечення ІБ банку	Способи реалізації загроз
		додатків
		Сканування мережі, спрямоване на виявлення відкритих портів та служб, відкритих з’єднань
Рівень операційних систем	Файли даних з персональними даними, банківською та комерційною таємницями. Загальносистемні програмні засоби Інформація, необхідна для ідентифікації, автентифікації та (або) авторизації. Файли даних з відкритою інформацією.	Крадіжка / втрата паролів
		Копіювання
		Модифікація / видалення
		Порушення штатних режимів роботи операційних систем
		Поширення шкідливих програм
		Неправильна (неповна) конфігурація систем захисту інформації
		Несанкціонований логічний доступ до операційних систем з використанням спеціалізованого ПЗ
Рівень систем управління базами даних	Бази даних інформаційних систем. Інформація, необхідна для ідентифікації, автентифікації і (або) авторизації.	Копіювання
		Модифікація
		Неправильна (неповна) конфігурація систем захисту інформації
		Модифікація / видалення
		Порушення штатних режимів роботи систем управління базами даних
		Підміна ідентифікаторів користувача
		Несанкціонований логічний доступ до систем управління базами даних
		Поширення шкідливих програм
		Крадіжка паролів
Рівень банківських технологічних процесів та програм	ПЗ для обробки персональних даних, банківської та комерційної таємниці. ПЗ для обробки відкритої інформації. Пластикові картки. Інформація, необхідна для ідентифікації, автентифікації та (або) авторизації. Паперові документи	Модифікація / видалення
		Розповсюдження / передача
		Друк документів
		Крадіжка документів та карток
		Крадіжка паролів
Рівень бізнес-процесів	Дані обмеженого доступу Персонал	Саботаж
		Халатність та помилки
		Шкідництво

Банк, формуючи ефективну систему забезпечення інформаційної безпеки, може протистояти значній кількості загроз, мінімізуючи таким чином їх негативний вплив (рис. 1.1).

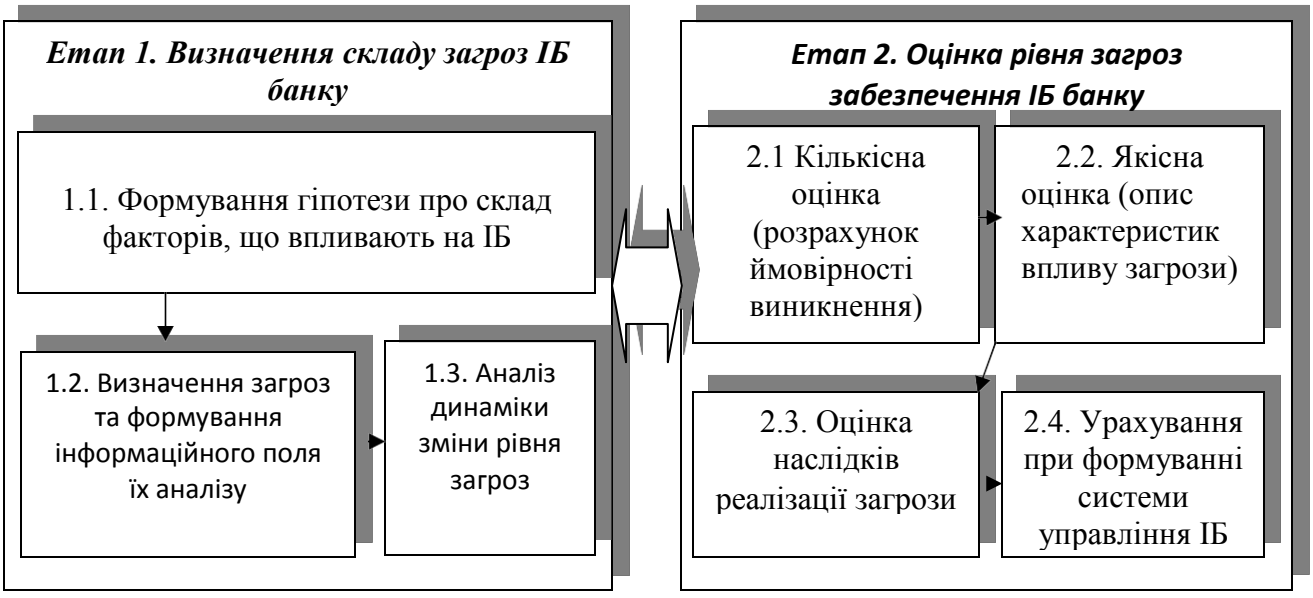


Рисунок 1.1 – Комплексна модель оцінки та аналізу загроз ІБ банку [узагальнено автором]

Модель оцінки та аналізу загроз ІБ банку є основою для формування комплексу внутрішньобанківських заходів, що забезпечать нейтралізацію загроз з використанням методів та способів захисту інформації, запобігання несанкціонованому доступу до інформаційних систем та інформаційних активів, включаючи запобігання несанкціонованого впливу на технічні та програмні засоби.

Для забезпечення ІБ банку доцільно сформувати модель порушника (суб'єкта, зацікавленого в отриманні вигоди шляхом порушення безпеки інформаційних активів), що розділяє їх за типом доступу до інформаційних активів, і дозволяє визначити, які загрози можуть бути спрямовані на них.

Узагальнивши розробки з цієї тематики, пропонуємо наступну структуризацію порушників інформаційної безпеки банку (табл. 1.3).

У разі наявності внутрішніх слабких місць в системі забезпечення ІБ банку формуються передумови до реалізації загрози, наслідком чого є:

- збитки, пов'язані зі втратою, витоком або недоступністю інформації, зі знищенням та подальшим відновленням інформації;
- збитки від дезорганізації діяльності банку та втрат, пов'язаних із невиконанням ним зобов'язань;
- репутаційні втрати;
- втрати від реалізації юридичного ризику через санкції з боку клієнтів, контрагентів та регулятора.

Ризики інформаційної безпеки є невіддільною частиною операційних ризиків банку.

Загальноприйнятим є визначення операційного ризику за Базельською угодою: «...ризик збитків, що виникає в результаті неадекватних або помилкових внутрішніх процесів, дій співробітників і систем або в результаті зовнішніх подій. Поняття включає юридичний ризик, але виключає стратегічний ризик та ризик втрати ділової репутації».

Юридичний ризик включає, але не обмежується, ризиком нарахування штрафів, пені або штрафних збитків у результаті здійснення нагляду, а також приватних судових позовів [12].

Згідно з Методичними рекомендаціями щодо управління ризиками, банки наражаються на операційно-технологічний ризик, тобто на «…загрозу фінансовому стану внаслідок неадекватності чи неспроможності внутрішніх процесів, персоналу та систем або зовнішніх подій, що виявляється у зміні чистого прибутку та / або власного капіталу» [13].

Деякі визначення використовують опосередкований (визначення Європейської комісії) або поєднання прямого та опосередкованого підходу до визначення операційного ризику, тобто під ними розуміються ризики, що не підпадають під інші категорії ризиків банківської діяльності (кредитний, ринковий, процентний ризик) та розраховується як залишкова величина. Однак практичне застосування опосередкованого підходу об'єднує в одну групу стільки різноманітних ризиків, що унеможливлює якісне управління ними.

Зважаючи на недостатнє вивчення в науковій літературі, а також відсутності уніфікації поняття операційного ризику в українській та закордонній практиці, слід чітко розмежовувати операційний, стратегічний та юридичний ризик з метою покращення ефективності управління саме ризиками інформаційної безпеки як частини операційних ризиків.

Отже, узагальнивши вище наведене, можна сформувати перелік ризиків інформаційної безпеки:

- ризики людського фактора (помилки, зовнішнє та внутрішнє шахрайство та ін.);
- ризики технології (несправності устаткування, його невідповідність, системні збої в роботі та ін.);
- ризики зовнішніх подій (стихійні лиха, катастрофи тощо).

Таблиця 1.3 – Склад можливих порушників ІБ банку [узагальнено автором]

<table>
<tr><th>Ознака</th><th colspan="2">Види порушників</th><th>Склад порушників</th><th>Приклади порушень</th></tr>
<tr><td rowspan="5">Відношення до банку</td><td rowspan="3">зовнішні, які здійснюють атаки поза межами контрольованої зони банку</td><td>комп’ютерні зловмисники, які здійснюють цілеспрямовані деструктивні дії, в тому числі використання комп’ютерних вірусів та інших типів шкідливих кодів і атак</td><td>- хакери;
- комп’ютерні хулігани;
- терористи, кримінальні елементи</td><td>- впровадження в систему та виконання шкідливих програм: програмних закладок, програмних «вірусів» та «черв’яків»;
- соціальний інжиніринг (умисні дії сторонніх осіб, які переслідують шахрайські цілі, що реалізуються за допомогою обману, введення в оману працівників банку);
- диверсії (зловмисне фізичне знищення апаратних засобів та комп'ютерних систем)</td></tr>
<tr><td>провайдери</td><td>провайдери каналів зв’язку, інтернет-провайдери</td><td>- помилки, допущені при укладанні контрактів з провайдерами, що можуть створювати проблеми в роботі ІС банку.</td></tr>
<tr><td>підрядники, що здійснюють монтаж, пусконалагоджувальні роботи та його ремонт обладнання</td><td>- співробітники технічної підтримки;
- сервісні інженери.</td><td>невиконання з боку третіх осіб взятих на себе зобов’язань перед банком за якістю, складом, змістом та / або порядком надання послуг, постачання продукції та т.і н., наприклад, невиконання вимог банку розробниками або постачальниками програмно-технічних засобів та послуг</td></tr>
<tr><td colspan="2">клієнти / контрагенти банку</td><td>залежність від клієнтів / контрагентів, що змушує банк покладатися на їх інформаційну безпеку, банк повинен бути впевнений, що вони зможуть забезпечити належний рівень безпеки.</td></tr>
<tr><td>внутрішні, які здійснюють атаки, перебуваючи в межах контрольованої зони банку</td><td>співробітники банку, які є легальними учасниками процесів в ІС та діють в межах наданих повноважень

співробітники банку, які є легальними учасниками процесів в ІС та порушують межі наданих повноважень</td><td>- користувачі ІС;
- адміністратори ІС;
- технічний персонал, який має доступ до апаратного забезпечення;
- адміністратори систем захисту інформації.</td><td>- саботаж (свідоме невиконання працівниками певних обов’язків або недбале їх виконання);
- халатність (невиконання або неналежне виконання обов’язків без злого умислу);
- шкідництво (зловмисне нанесення шкоди інформаційним активам);
- помилка (невідповідні встановленим регламентом або сформованим практикам дії персоналу, що здійснюються без злого умислу) через недостатньо чітко визначені обов’язки, недбалість, недостатнє навчання або кваліфікацію персоналу. Виникненню помилок сприяють відсутність дисциплінарного процесу і документування процесів, надання надлишкових повноважень, використання зловмисником методів соціального інжинірингу до персоналу.</td></tr>
<tr><td rowspan="2">Можливість доступу до банку</td><td colspan="4">особи, які не мають права доступу до приміщень, де розташовані технічні та програмні засоби</td></tr>
<tr><td colspan="4">особи, які мають право постійного або разового доступу в приміщення, де розташовані технічні та програмні засоби</td></tr>
</table>

Системи управління операційними ризиками в банках повинні класифікувати події, що несуть операційний ризик в контексті ІБ, наступним чином:

- внутрішнє шахрайство: умисне невідображення у звітності окремих операцій, умисне здійснення недозволених операцій, умисна крадіжка або знищення інформаційних активів, підробка документів, використання конфіденційної інформації з власною метою;
- зовнішнє шахрайство: всі випадки внутрішнього шахрайства, але за участю третьої сторони;
- нанесення пошкоджень інформаційним активам: пошкодження внаслідок стихійних лих (катастроф, пожеж тощо) або умисних дій працівників банку чи третіх осіб;
- порушення в інформаційній системі банку: збої в роботі телекомунікацій, програмного та апаратного забезпечення;
- помилки в управлінні процесами: при вводі, завантаженні або передачі даних, у веденні обліку та звітності, при наданні зовнішніх та внутрішніх звітів;
- інші події, що можуть призвести до виникнення операційних ризиків.

Операційними ризиками в контексті ІБ банку, що призводять до отримання збитків або недоотримання прибутків, є також технологічні ризики, а основними індикаторами, що свідчать про їх наявність, є:

- збої та помилки в роботі автоматизованих банківських систем (АБС) за відсутності або недостатності контролю;
- внутрішнє та зовнішнє шахрайство, пов'язане з наданням послуг, що реалізуються через віддалений доступ до грошових коштів або інформації;
- тимчасові розриви в діяльності банків у зв'язку з виходом з ладу комп'ютерних, телекомунікаційних та інших систем банківського життєзабезпечення;

У цілому можна визначити наступні елементи операційного ризику в контексті ІБ банку, на яких базується більшість визначень:

1) внутрішні процеси: ризик втрат через недоліки або відсутність чітко задокументованих та затверджених процесів з проведення операцій;

2) людський фактор: ризик втрат, що виникає внаслідок впливу персоналу, клієнтів, постачальників / зовнішніх партнерів, третіх сторін. Ця група включає:

- ненавмисні (помилкові, випадкові, необдумані, без злого наміру та корисливих цілей) порушення встановлених регламентів збору, обробки та передачі інформації, а також інші дії персоналу при експлуатації інформаційних систем, що призводять до непродуктивних витрат часу та ресурсів, розголошення конфіденційних даних, втрати інформації або порушення працездатності окремих робочих станцій, підсистем або в цілому всієї системи;
- навмисні (у корисливих цілях, з примусу третіми особами, зі злим умислом тощо) дії співробітників, допущених до роботи з інформаційними системами, а також співробітників, відповідальних за обслуговування, адміністрування програмного та апаратного забезпечення, засобів захисту та забезпечення інформаційної безпеки;
- діяльність злочинних груп та формувань, політичних й економічних структур, а також окремих осіб з добування інформації, нав'язування неправдивої інформації, порушення працездатності системи в цілому та її окремих компонентів;
- помилки, допущені при проектуванні інформаційних систем та їх систем захисту, помилки в програмному забезпеченні, відмови та збої технічних засобів (у тому числі, засобів захисту інформації та контролю ефективності захисту).

Це джерело ризику є основним та найбільш розповсюдженим. Ризик втрат, обумовлений людським фактором, ймовірніше, є навмисним.

3) системи: стосується ризику збитків у результаті відсутності та / або збоїв у роботі систем та технологічної інфраструктури банку в цілому.

Отже, ризики інформаційної безпеки як об'єкти управління 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, що призводять до зростання операційного ризику банку.

1.2 Система управління операційними банківськими ризиками в 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 [14].

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 [15].

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 [16]:

- 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 та / або забезпечення відповідальності за певні дії.

Узагальнивши розробки з цієї тематики та нормативну базу [14], 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 загальної 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).

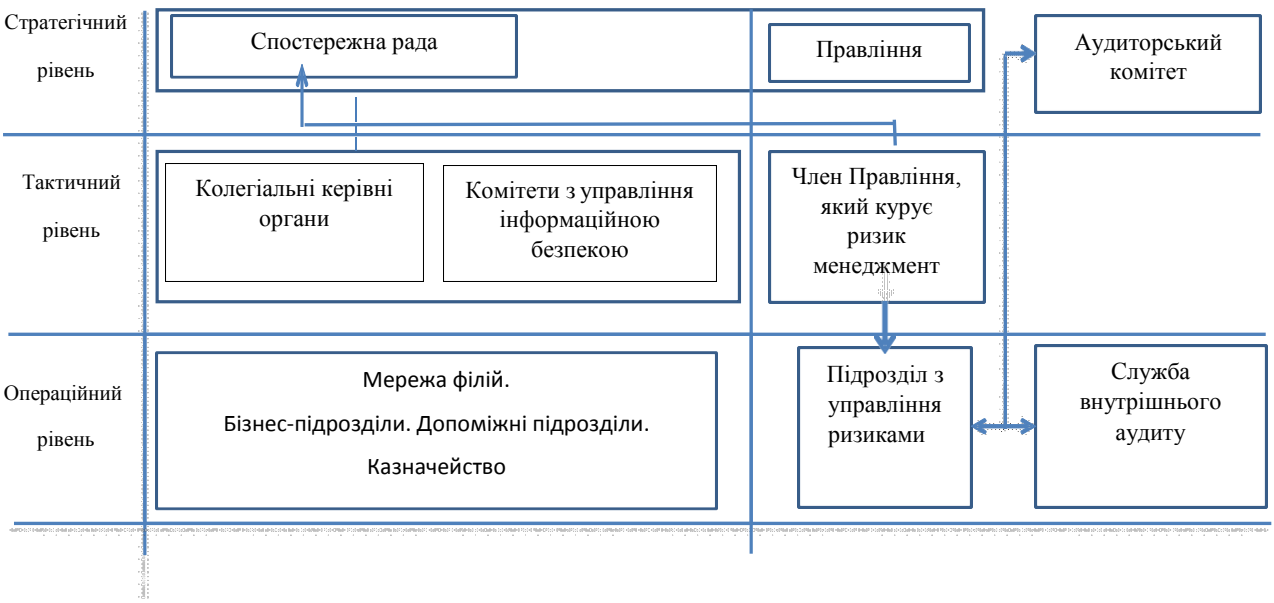


Рисунок 1.2 – Організаційно-управлінська підсистема управління ризиками ІБ банку [узагальнено автором]

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 [13, 14].

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 [13].

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 [14]. 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 [13]. 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 [13].

Функціональна підсистема визначається як сукупність інструментарію та дій суб'єктів управління по формуванню політики та стратегії управління ІБ банку, а також ідентифікації, оцінці, моніторингу та контролю величини ризиків ІБ як складової операційних ризиків банку (рис. 1.3).

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 [14].

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 [14].

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 [14].

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

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

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

Базовою методикою ідентифікації ризиків ІБ є аналіз причинно-наслідкових зв'язків зовнішніх та внутрішніх загроз, реалізація яких може привести до певних відхилень від цільових параметрів ІБ банку та цільового перебігу бізнес-процесу. Наслідком цього стають фінансові втрати, погіршення репутації, втрати транзакцій та клієнтів, санкції наглядових органів та юридична відповідальність (табл. 1.4).

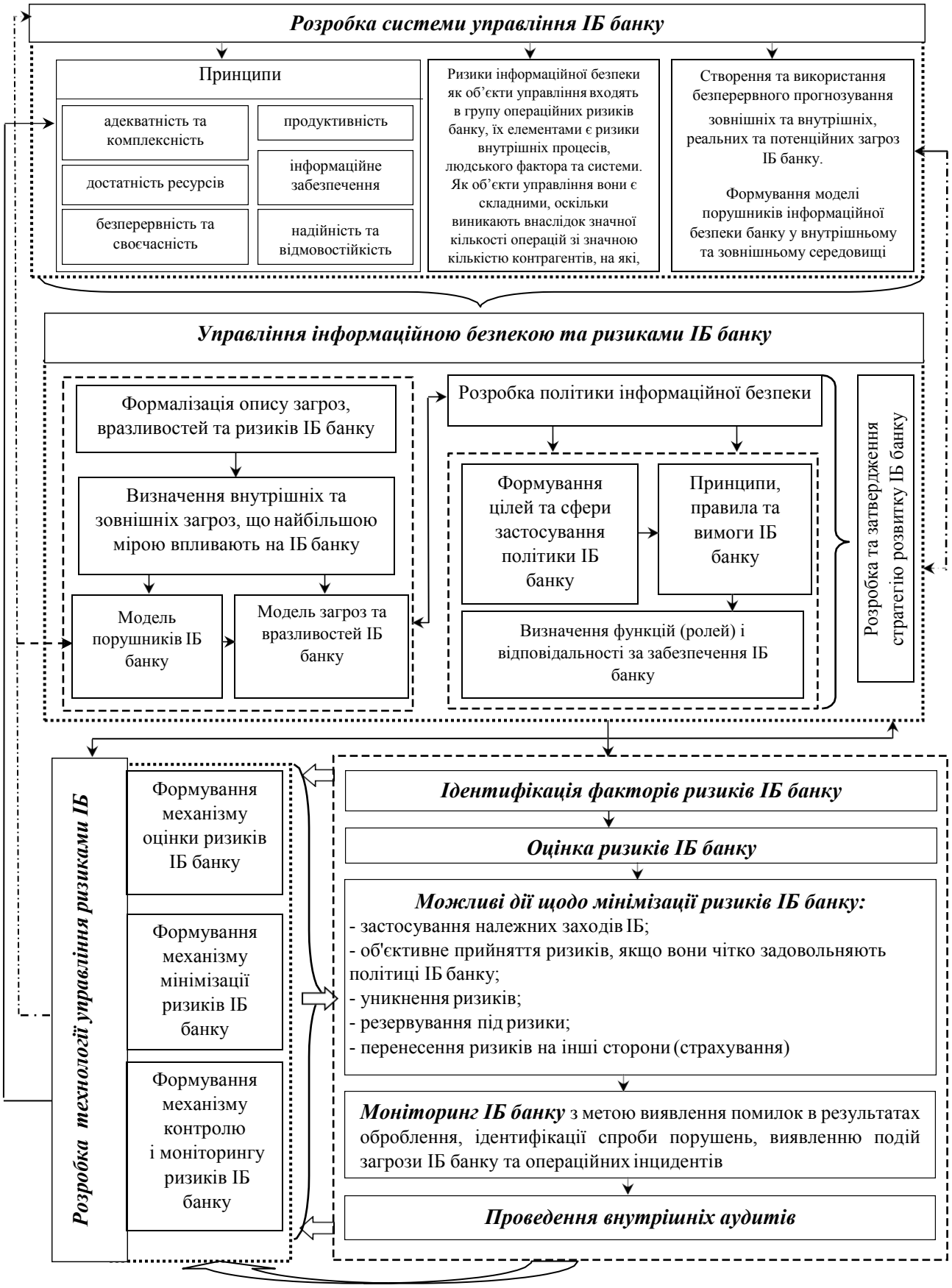


Рисунок 1.3 – Основні функції управління ІБ та ризиками ІБ банку [розроблено автором]

Таблиця 1.4 – Наслідки реалізації ризиків ІБ банку [узагальнено автором]

	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 ВВВ (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.

1.3 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 різною мірою впливаючи на них.

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

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

І для цього використовується така формула (формула 1.1) [17]:

$$NK_i = \frac{K_i}{\overline{K_i}} \qquad (1.1)$$

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

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

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

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

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

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

Отже, виникає потреба встановити ступінь впливу кожного окремого інциденту на операційний ризик банку в сфері інформаційної безпеки. Таким чином, з ціллю обчислення числових значень характеристик ступеня впливу відповідного інциденту на рівень показника операційного ризику інформаційної безпеки проведено даний аналіз (формула 1.2) [17]. Слід зауважити, що показники операційного ризику інформаційної безпеки відтворюють кожний інцидент ризику у відповідних співставеннях. Для проведення наступного аналізу представимо групи інцидентів операційного ризику інформаційної безпеки в якості фіктивних змінних, а саме змінних, що набувають значення «1» за можливості їх опису певним показником, або «0» в іншому випадку.

$$K_i = \beta_0 + \beta_1 F_{1i} + \beta_2 F_{2i} + \beta_3 F_{3i} + \beta_4 F_{4i} + \varepsilon \qquad (1.2)$$

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 (1.2) є неможливим. Так, щоб визначити на скільки відсотків кожен з інцидентів пояснює виникнення операційного ризику інформаційної безпеки за певним показником (формула 1.3) [17]:

$$K_i = \alpha_1 F_{1i} + \alpha_2 F_{2i} + \alpha_3 F_{3i} + \alpha_4 F_{4i} + \varepsilon \qquad (1.3)$$

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

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

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

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

Коефіцієнти $\alpha_m, m = 1 \div 4$ рівняння (1.3) визначаються за наступною формулою (1.4) [17]:

$$\alpha_m = \beta_m \frac{\sigma_{F_j}}{\sigma_{K_i}} \qquad (1.4)$$

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

σ_{F_j}, σ_{K_i} - середні квадратичні відхилення факторних і результативної ознак відповідно, які визначаються за формулами (1.5) і (1.6) [17]:

$$\sigma_{F_j} = \sqrt{F_j^2 - \overline{F}_j^2}, \quad (1.5)$$

$$\sigma_{K_i} = \sqrt{K_i^2 - \overline{K}_i^2}. \quad (1.6)$$

Так як метою аналізу є встановлення абсолютного значення ступеня впливу інцидентів на показники операційного ризику інформаційної безпеки, то отримані показники, в разі невідповідності знаків, беруться по модулю. Базуючись на скорегованих числових характеристиках (α_m^*) знаходиться відносний показник структури (формула 1.7) [17], що характеризує питому вагу впливу інцидентів на рівень операційного ризику інформаційної безпеки.

$$\alpha_m^* = \frac{\alpha_m}{\sum_{m=1}^{4} \alpha_m}, \quad (1.7)$$

Визначені числові значення характеристик ступеня впливу окремого інциденту на рівень певного показника кількісної оцінки ступеня операційного ризику інформаційної безпеки відповідним пояснюючим ознакам, а також абсолютні значення самих показників наведемо у таблиці 1.5.

Таблиця 1.5 - 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 $j = 4$
	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 1.5 та формули (1.1) обчислимо значення нормалізованих показників кількісної оцінки ступеня операційного ризику інформаційної безпеки зважених на характеристики впливу конкретного інциденту на рівень показника операційного ризику інформаційної безпеки.

Таблиця 1.6 – 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 (1.8) [17]:

$$NKbin_i \begin{cases} = 1; \alpha_m^* \overline{NK_m} \ge \alpha_m^* NK_i, \\ = 0; \alpha_m^* NK_i < \alpha_m^* \overline{NK_m} \end{cases}, \tag{1.8}$$

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 1.7.

Під час *четвертого етапу* визначається сума бінарних показників для певного j-го фактору ризику, що отримали значення «1», тобто експрес-оцінка операційного ризику інформаційної безпеки за j-м фактором ризику (формула 1.9) [17]:

$$EO_j = \sum_{i=1}^{n} NKbin_{ij}, \tag{1.9}$$

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

Таблиця 1.7 – 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	$NKbin_{n1}$	$NKbin_{n2}$	$NKbin_{n3}$	$NKbin_{n4}$

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

На базі знайденої суми бінарних показників для певного j-го інциденту ризику розраховується загальна сума бінарних показників, що виступає у якості експрес-оцінки операційного ризику банку в сфері інформаційної безпеки (формула 1.10) [17]:

$$EO = \sum_{j=1}^{4} \sum_{i=1}^{n} NKbin_{ij}, \qquad (1.10)$$

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 настання даного виду ризику, тобто імовірність ($p_{OR}(H1)$) виникнення операційного ризику інформаційної безпеки (подія $H1$) за умови існування інформації $OR=(OR_1,OR_2,OR_3,OR_4)$ в розрізі 4-х інцидентів, де $OR_k, k=1\div 4$ набувають значення 0, якщо відповідний норматив виконується (імовірність виникнення відповідного фактору ризику знаходиться у граничних значеннях), і 1 – у протилежному випадку. Підґрунтям для визначення складових $OR=(OR_1,OR_2,OR_3,OR_4)$ є імовірності ($p_K(H1\,j)$) 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 $H1\,j$) за умови наявності інформації $K=(K_1,K_2,...,K_n)$ наступним чином (формули 1.11-1.12) [17]:

$$p_K(H1j)=\frac{1}{1+e^{\{\lambda_0+L\}}} \tag{1.11}$$

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

$$\lambda_{ij}=\ln\left\{\frac{b_{ij}(1-g_{ij})}{g_{ij}(1-b_{ij})}\right\}, i=1,...,n \tag{1.12}$$

$$\lambda_{0j} = \ln\left(\frac{p(H2\,j)}{p(H1\,j)}\right) + \sum_{i=1}^{n} \ln\left(\frac{1-b_{ij}}{1-g_{ij}}\right)$$

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);

$P(H1\,j)$ – імовірність гіпотези $H1\,j$;

$H1\,j$ – висунута гіпотеза, що виникне j-й інциденту операційного ризику інформаційної безпеки;

$P(H\,2\,j)$ – імовірність протилежної гіпотези;

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

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

g_{ij} – імовірність супротивної події.

Щоб отримати кількісну оцінку ступеня операційного ризику інформаційної безпеки за j-м інцидентом спочатку визначимо значення b_{ij} - імовірність події $NKбін_{ij} = 0$, та g_{ij} - імовірність події $NKbin_{ij} = 1$ за всіма n показниками за формулами 1.13 [17]:

$$g_{ij} = \frac{\sum_i NKbin_{ij}}{n}, \qquad b_{ij} = 1 - g_{ij} \tag{1.13}$$

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

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

Так, використовуючи вище здійснені розрахунки, отримаємо алгоритм знаходження кількісної оцінки ступеня операційного ризику банку в сфері інформаційної безпеки як імовірності виникнення операційного ризику інформаційної безпеки при наявності інформації $B=(p_K(H11),\ p_K(H12),\ p_K(H13),\ p_K(H14))$, що обчислюється на грунті аналітичних показників характеристики діяльності відповідної банківської установи $K=(K_1,K_2,...,K_n)$ (див. таблицю 1.8):

Таблиця 1.8 – 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)	$0 \le p_K(H1j) < fsr\left\{\min_s\{p_B(H1)_s\} \div fsr\{p_B(H1)_s\}\right\}$			
Бінарні показники за j інцидентами операційного ризику інформаційної безпеки	$NKbin_1$	$NKbin_2$	$NKbin_3$	$NKbin_4$
Імовірність виникнення операційного ризику інформаційної безпеки (кількісна оцінку ступеня операційного ризику)	$p_B(H1)$			

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 - $0 \le p_K(H1\,j) < 0{,}3$, що передбачає нормальний рівень ризику.

4. Перехід від імовірнісних показників $p_K(H1\,j)$ до бінарних показників $NKбін_j$ за j інцидентами операційного ризику інформаційної безпеки: $NKбін_j$ набуває величини «1» у випадку попадання показника $p_K(H1\,j)$ у гранично допустимі межі або «0» у протилежному випадку.

5. Обчислення g_j - імовірності події $NKбін_j = 1$ ($g_{ij} = \dfrac{\sum_i NKbin_{ij}}{n}$) 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 1.14-1.15) [17]:

$$p_B(H1) = \frac{1}{1 + e^{\{\lambda_0 + L\}}} \tag{1.14}$$

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

$$\lambda_j = \ln\left(\frac{b_j(1-g_j)}{g_j(1-b_j)}\right), \quad j = 1,\ldots,4$$

$$\lambda_{0j} = \ln\left(\frac{p(H2)}{p(H1)}\right) + \sum_{j=1}^{4} \ln\left(\frac{1-b_j}{1-g_j}\right) \tag{1.15}$$

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 $fsr\{p_{B\ s}(H1)\} \le p_{B\ s}(H1) < fsr\left\{fsr\{p_{B\ s}(H1)\} \div \max_s\{p_{B\ s}(H1)\}\right\}$, високий рівень ризику;

- якщо $fsr\left\{fsr\{p_{B\ s}(H1)\} \div \max_s\{p_{B\ s}(H1)\}\right\} \le p_{B\ s}(H1) \le 1$, 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.

1.4 Стандартизація менеджменту якості банківських послуг як інструмент підвищення інформаційної безпеки банку

На сучасному етапі зростання актуальності управління інформаційною безпекою банку пов’язано, передусім, з розвитком онлайн-банкінгу та зростанням потреб клієнтів у забезпеченні конфіденційності інформації. Управління інформаційною безпекою у фінансовому секторі включає цілий ряд елементів, що стосуються виявлення інформаційних ризиків, формування стратегії управління ними, впровадження заходів з підвищення інформаційної безпеки та контроль їх ефективності. Основними наслідками реалізації організаційних ризиків у сфері інформаційної безпеки банку є:

– втрата довіри клієнтів та зниження обсягів надання послуг;

– санкції з боку регулятора за порушення вимог інформаційної безпеки;

– зростання вимог клієнтів для перевірки безпеки транзакцій;

– репутаційні збитки [23].

Виходячи з вище зазначеного, можна констатувати, що інформаційна безпека виступає важливим елементом якості банківських послуг та ефективності банку в цілому. Відмітимо, що управління якістю банківських послуг, орієнтоване на забезпечення відповідності пропозиції банків очікуванням клієнтів, передбачає формування стратегії та тактики управління якістю, а також розробку та впровадження конкретних заходів щодо її підвищення. У той же час, управління якістю має узгоджуватись з загальною стратегією розвитку банку та відповідати ринковим тенденціям розвитку банківського бізнесу, що передбачає необхідність формування комплексу принципів, покладених в основу менеджерських дій. На міжнародному рівні основні принципи та вимоги щодо системи управління якістю викладені у вигляді стандарту ISO 9001, який на сучасному етапі активно впроваджується банками різних країн світу. Міжнародна організація зі стандартизації відзначає, що саме впровадження стандартів групи ISO 9001

характерно для систем управління якістю, орієнтованих на формування здатності організації задовольняти потреби та очікування клієнтів [25].

Дана група стандартів реалізується впровадженням заходів у наступні сфери діяльності організації:

– загальні вимоги щодо системи управління якістю та документації;

– управління відповідальністю, політика, планування та цілі;

– управління ресурсами;

– реалізація продукту та процесний менеджмент;

– вимірювання, моніторинг, аналіз та удосконалення.

При цьому вимоги клієнтів виступають вхідним фактором розвитку системи управління якістю, а задоволення клієнтів розглядається як результативний показник функціонування даної системи.

Н. Греньюк інтерпретує застосування стандартів ISO 9001:2008 на рівні банку через наступні параметри, на яких має бути сфокусована система менеджменту:

– удосконалення механізмів підтримки та стійкості в умовах глобальної кризи у відповідності до державної політики та національної стратегії;

– орієнтація на поточні тренди і майбутні потреби та очікування клієнтів;

– просування іміджу банку;

– розвиток структури банку у відповідності до сучасних вимог динаміки функціонування банківських та фінансових інституцій;

– розвиток кадрових ресурсів банку у відповідності до вимог інноваційних змін у банківській діяльності;

– перманентне удосконалення системи управління якістю на рівні банку [21].

Таким чином, можемо констатувати, що стандартизація систем менеджменту якості банківських послуг включає також зростання інформаційної безпеки банку з точки зору покращення інфраструктурної компоненти та здатності протистояти викликам зовнішнього середовища.

Відповідно до дослідження групи італійських науковців, активне поширення стандартів групи ISO 9001 у світі спостерігається з перших років прийняття стандартівISO 9001:2000. Так, якщо у 2001 році з переліку 161 країни, які адаптували стандарти ISO 9001, 98 країн впровадили такожISO 9001:2000, частка яких у загальній кількості організацій, що пройшли сертифікацію, становила 8,7%, то протягом 2002 року стандарт ISO 9001:2000 було впроваджено організаціями 134 країн, а загальна частка таких стандартів становила 29,8%. Незважаючи на той факт, що сфера фінансового посередництва за досліджений період не характеризується випереджаючими показниками порівняно з різними секторами промисловості та інфраструктури, станом на 2002 рік частка впроваджених стандартів ISO9001:2000 становила 32,2% відносно загальної кількості сертифікованих організацій даного сектору [20].

Результати наукових досліджень свідчать, що ефект від проходження та дотримання вимог стандартів якості для компанії проявляються як на рівні внутрішніх бізнес-процесів, так і у відносинах з клієнтами, що призводить до покращення результатів діяльності сертифікованих організацій. Так, у табл. 1.9 представлено результати опитування 40 менеджерів алжирських компаній, яким було запропоновано оцінити фактори, на які вплинуло отримання сертифікату відповідності стандарту ISO 9001, за шкалою Лайкерта від 1 до 5, де 1 – дуже низький вплив та 5 – дуже високий вплив.

Як можна відмітити, три основні наслідки отримання сертифікату якості характеризують операційний та фінансовий результат діяльності компанії. Дещо нижчим рівнем характеризуються параметри, що відображають відносини з клієнтами та імідж компанії на ринку. При цьому показники внутрішніх відносин у компанії, на думку менеджерів, не зазнають наскільки суттєвих змін під впливом сертифікації як попередні групи індикаторів. У даному контексті відмітимо також позитивний вплив сертифікації на внутрішні організаційні процеси

банку, що веде до скорочення операційних ризиків та підвищення інформаційної безпеки в цілому.

Таблиця 1.9 – Результати ранжування вигід компанії від проходження ISO 9001 сертифікації [29]

Вигоди компанії від отримання сертифікату ISO 9001	Середнє значення	Відхилення
Зростання продажів	3,85	0,80
Зростання частки на ринку	3,75	0,78
Приріст прибутковості	3,62	0,98
Зростання продуктивності	3,57	0,78
Покращення іміджу компанії на ринку	3,57	0,93
Покращення задоволення клієнтів	3,40	0,81
Покращення якості продуктів/послуг	3,40	0,87
Скорочення скарг на компанію	3,25	0,84
Модернізація внутрішніх організаційних процесів компанії	3,20	0,65
Зростання конкурентних переваг	2,87	0,91
Скорочення невідповідностей	2,82	0,87
Покращення навичок персоналу	2,60	0,87
Удосконалення внутрішньої комунікації	2,47	0,90
Покращення відносин між менеджментом та працівниками	2,27	0,85

Огляд емпіричних досліджень щодо виявлення впливу ISO сертифікації на фінансові показники діяльності компаній реального сектору засвідчує наявність певних залежностей, що позитивно характеризує результат проходження сертифікації для функціонування організації. Так, на прикладі 146 великих компаній Сінгапуру було доведено, що сертифікація позитивно впливає на загальні показники їх фінансового стану [19]. У свою чергу А. Терлаак і А. Кінг [27] виявили, що обсяги виробництва та продажів американських компаній зростають більш швидкими темпами після отримання сертифікату. У той же час, Д. Шарма за результатами дослідження діяльності 70 компаній протягом 6 років приходить до висновку, що сертифікація більшою мірою призводить до позитивних результатів ефективності операційної діяльності (маржинального прибутку), ніж до зростання обсягів продаж та рентабельності капіталу, що пов’язано з удосконаленням внутрішніх бізнес-процесів [26].

Наявність позитивного впливу ISO 9001сертифікації на результати діяльності організації підтверджують результати дослідження,проведено групою грецьких науковців на прикладі 600 компаній, що належать до сфери послуг. Для розрахунків було обрано такі змінні як ISO 9001 ефективність – незалежна змінна розрахована як сумоване значення цілей стандарту ISO 9001, операційна результативність, фінансова результативність та якість продуктів/послуг – залежні змінні, агреговані за методом головних компонент на основі ключових індикаторів діяльності компанії. У результаті побудови множинних регресійних рівнянь авторами було виявлено, що ISO 9001 ефективність має статистично значимий позитивний вплив на якість продуктів/послуг та операційну результативність. У свою чергу, на другому етапі розрахунків підтверджено позитивний вплив операційної результативності на фінансову результативність, що, на думку авторів, є свідченням опосередкованого зв’язку стандартизації та зростання фінансової результативності компанії [24].

У той же час, результати дослідження Б. Мандерса підтверджують наявність прямого позитивного впливу ISO 9001 сертифікації на фінансову результативність підприємств. Так, для 40% компаній спостерігається зростання фінансових результатів у період після отримання сертифікату, у той час як частка компаній, що демонструють скорочення витрат та/або зростання доходів після сертифікації становить 60% загальної вибірки [22].

Однак, незважаючи на активне впровадження стандартів ISO 9001 банками та іншими фінансовими установами, на сучасному етапі спостерігається брак наукових досліджень, спрямованих на виявлення результатів, у тому числі фінансових вигід, від отримання таких сертифікатів якості.

В Україні впровадження стандартів ISO 9001 банківськими установами бере початок з отримання ПАТ «КРЕДИТПРОМБАНК» сертифікату відповідності системи менеджменту якості банку вимогам стандартуISO 9001:2000 у 2005 році. Сертифікація поширювалась на сферу надання банківських послуг, охоплюючи управлінські процеси, обслуговування клієнтів, технології та нормативні документи. У 2008 році банк отримав другий випуск сертифікату дійсний до 2011 року [36].

У 2009 році сертифікати відповідності системи менеджменту стандарту якості ISO 9001:2008 отримали два українських банки. ПАТ «Укрексімбанк» в подальшому п'ять разів поспіль успішно проходив наглядовий аудит на підтвердження відповідності системи менеджменту якості вимогам стандарту до 2013 року включно [35]. АТ «ПЕРШИЙ ІНВЕСТИЦІЙНИЙ БАНК» перші кроки щодо початку процесу сертифікації бізнес-процесів за програмою оцінки якості ISO 9001:2000 здійснив у 2008 році, однак лише у 2009 році банком було отримано сертифікат якості ISO 9001:2008, відповідність системи менеджменту якості вимогам якого було підтверджено результатами наглядового аудиту у 2010-2011 роках. У 2012 році АТ «ПЕРШИЙ ІНВЕСТИЦІЙНИЙ БАНК» отримав сертифікат ISO 9001:2008 на наступні три роки його функціонування за результатами ресертифікаційного аудиту системи менеджменту якості [32].

ПАТ «КРЕДІ АГРІКОЛЬ БАНК» приєднався до переліку банків, система менеджменту яких відповідає міжнародним вимогам, у 2011 році, отримавши сертифікат відповідності стандарту ISO 9001: 2008 за напрямком автомобільне кредитування. У період до 2017 року банк підтверджував відповідність системи менеджменту якості вимогам стандарту за результатами річного аудиту, а за підсумками ре-сертифікаційного аудиту, проведеному у липні 2017 року банком було отримано підтвердження відповідності системи менеджменту якості версії стандарту ISO 9001:2015 та отримано відповідний сертифікат [34].

У 2018 році ПАТ «БАНК АВАНГАРД» успішно пройшов перевірку системи менеджменту якості на відповідність міжнародним вимогам та отримав сертифікат ISO 9001:2015 за напрямком діяльності «Послуги в сфері транзакційного бізнесу, грошового ринку, валютного ринку, ринку боргових цінних паперів, цифрового банкінгу»[30]. Таким чином, можна відмітити, що в банківській системі України спостерігається поступовий перехід банків до побудови систем менеджменту якості відповідно до вимог міжнародних стандартів.

Варто позитивно відзначити наявність диференціації напрямків банківської діяльності, за якими було отримано міжнародні сертифікати якості банками України. Відмітимо також відносну популярність сертифікації технологічного забезпечення якості банківських послуг, що мала місце в банках України. З іншого боку, неоднозначним є той факт, що з п'яти банків, якими у різний період було отримано сертифікати відповідності стандартам якості ISO 9001, на поточний момент лише два мають чинні підтвердження продовження дії сертифікатів. Все це актуалізує необхідність дослідження ролі наявності сертифікату якості для результатів функціонування банку, що дозволить зрозуміти причини, які обумовлюють тенденції сертифікації банківських установ.

Саме тому, враховуючи результати зарубіжних досліджень щодо формування додаткової ефективності компаній реального сектору, отриманої у результаті наявності сертифікату відповідності міжнародним стандартам якості ISO 9001, можемо висунути гіпотезу про наявність позитивного впливу сертифікації системи менеджменту якості банку на його ефективність.

Для проведення дослідження було сформовано вибірку з 10 українських банків, чотири з яких мали підтверджений сертифікат відповідності стандарту якості ISO 9001, а шість банків було обрано з різних груп, які є маркетмейкерами на ринку банківських послуг. Період

дослідження охоплює 2008-2017 роки, що дозволяє охопити роки наявності стандарту якості як мінімум в одному з обраних банків.

Результативною змінною дослідження було обрано ефективність функціонування банку. Для розрахунку даного показника використаємо підхід до визначення ефективності банківського бізнесу, який було запропоновано та успішно апробовано у дослідженні А. В. Буряк [31]. Відповідно до даного підходу, ефективність банківського бізнесу можна оцінити на основі наступного переліку вхідних факторів:

– параметри, що характеризують витрати банку – величина загальноадміністративних витрат на одиницю згенерованих доходів, величина витрат на персонал на одиницю згенерованих доходів;

– параметри, що характеризують доходи банку – чиста процентна маржа, чиста непроцентна маржа;

– додаткові параметри – чистий спред, частка негативно класифікованих кредитів у структурі кредитного портфелю банку, частка активів банку в банківській системі.

Аналіз наявних статистичних даних за окремими параметрами, що характеризують складові ефективності банківської діяльності засвідчив, що в середньому спостерігаються відмінності показників для банків, які здійснювали заходи щодо сертифікації систем менеджменту якості, та для інших банків у вибірці. Так, рисунок 1.4 демонструє різницю параметрів витрат для двох типів банку. Відмітимо, що за показником загальноадміністративних витрат не спостерігається чіткої тенденції показника як у часі, так і у розрізі різних груп.

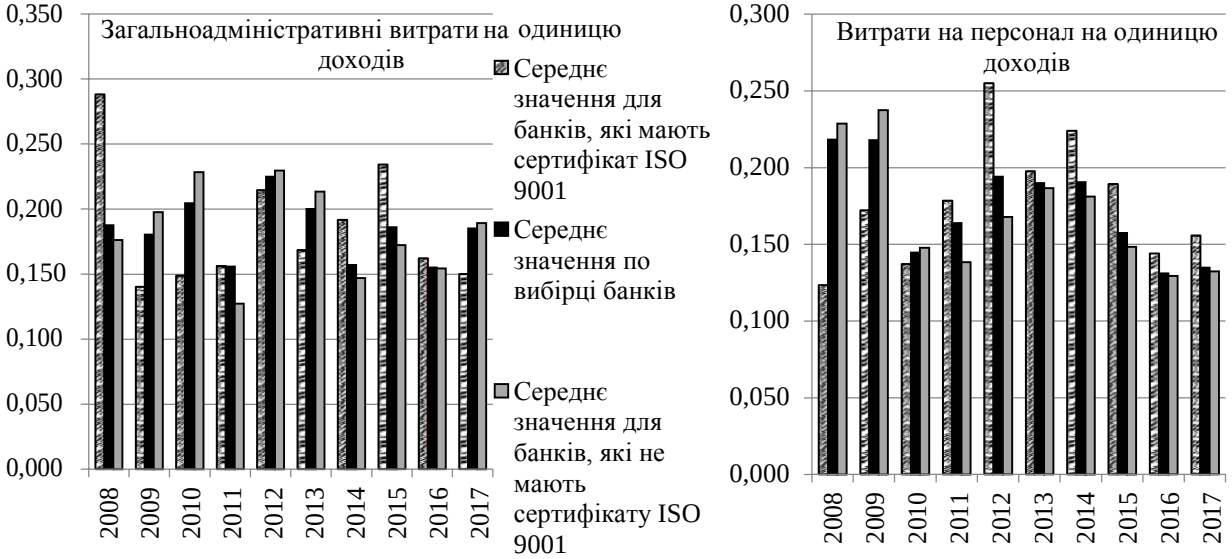


Рисунок 1.4 – Статистичний опис параметрів, що характеризують витрати банків різних типів за період 2008-2017 років, коп. на 1 грн. доходів (побудовано за даними [33])

З іншого боку, за показником відносних витрат на персонал у більшості періодів спостерігається перевищення середнього значення для банків, що мали чинні сертифікати систем менеджменту якості порівняно з іншими банками, враховуючи той факт, що заходи з удосконалення такої системи мають обов’язково передбачати підвищення кваліфікації персоналу. При цьому слід звернути увагу на той факт, що за показниками витрат не спостерігається довгострокових тенденцій зміни їх середніх значень, що свідчить про існування певного оптимального з точки зору керівництва банку рівня, достатнього для забезпечення його ефективного функціонування.

Аналізуючи індикатори, що характеризують доходи банків (рис. 1.5), відмітимо, що за показником чистої процентної маржі у переважній більшості періодів спостерігається

перевищення значення показника для банків, які не проходили процедуру сертифікації систем менеджменту якості, порівняно з сертифікованими банками, однак протягом 2016-2017 років є характерною протилежна тенденція зі значним розривом усереднених значень.

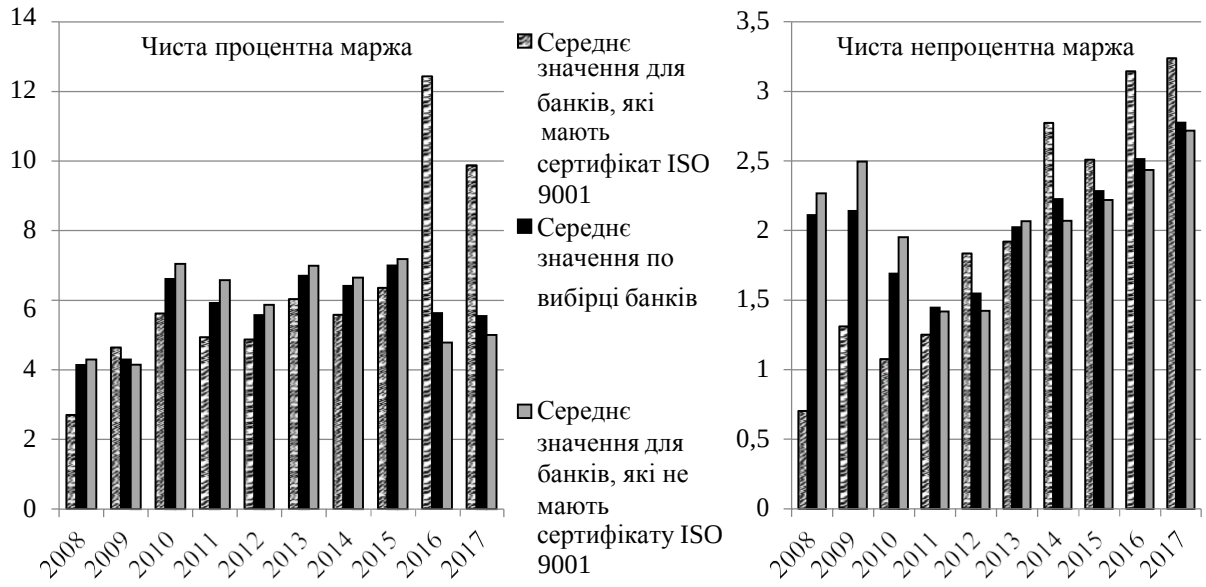


Рисунок 1.5 – Статистичний опис параметрів, що характеризують доходи банківрізних типів за період 2008-2017 років, %(побудовано за даними [33])

У свою чергу, за параметром чистої непроцентної маржі характерним є перевищення значень, отриманих для сертифікованих банків, над іншими банками вибірки починаючи з 2012 року з поступовим нарощенням розривів у наступні періоди. Таким чином, аналіз усереднених статистичних даних щодо параметрів доходів та витрат засвідчив неоднозначність виявлених тенденцій, які дозволили б охарактеризувати ефективність функціонування банків, що успішно пройшли процедуру сертифікації систем менеджменту якості. Привертає увагу також той факт, що серед додаткових параметрів ефективності банку для сертифікованих банків характерним є отримання нижчих середніх значень чистого спреду порівняно з іншими банками (рис. 1.6), у той час як середній рівень частки негативно класифікованих кредитів для банків, система менеджменту якості яких відповідає міжнародним стандартам, є суттєво нижчим за показник, розрахований для інших банків у вибірці, що позитивно характеризує вплив управлінських заходів щодо стандартизації на фінансову стійкість банків.

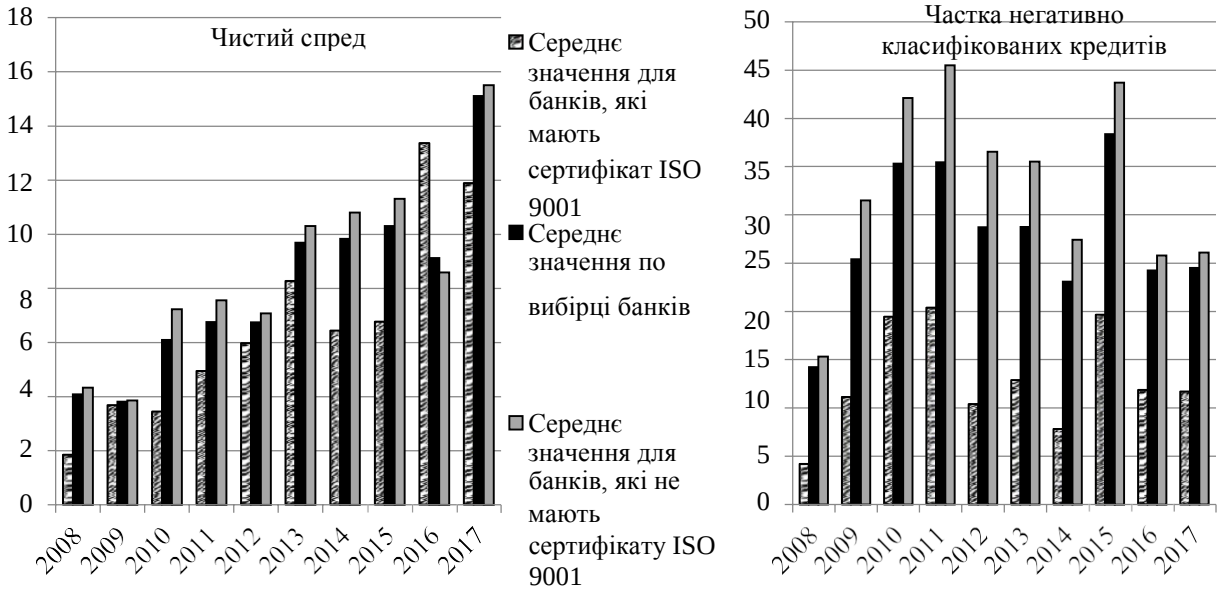


Рисунок 1.6 – Статистичний опис додаткових параметрів ефективності банків різних типів за період 2008-2017 років, %(побудовано за даними [33])

Слід звернути увагу, що за показником масштабу діяльності банку, в основу розрахунку якого покладено розмір активів, сертифіковані банки характеризуються суттєво нижчими показниками обсягів їх діяльності порівняно з іншими банками вибірки (рис. 1.7), що вказує на той факт, що тенденції щодо впровадження міжнародних стандартів характерні не лише для банків-лідерів за масштабами діяльності, а й можуть бути результатом обрання банком вектору стратегії управління якістю та орієнтації на довгострокову ефективність.

Для оцінювання ефективності банків використовується метод стохастичного фронтірного аналізу, який передбачає визначення також вихідної змінної, на яку впливають вхідні параметри.

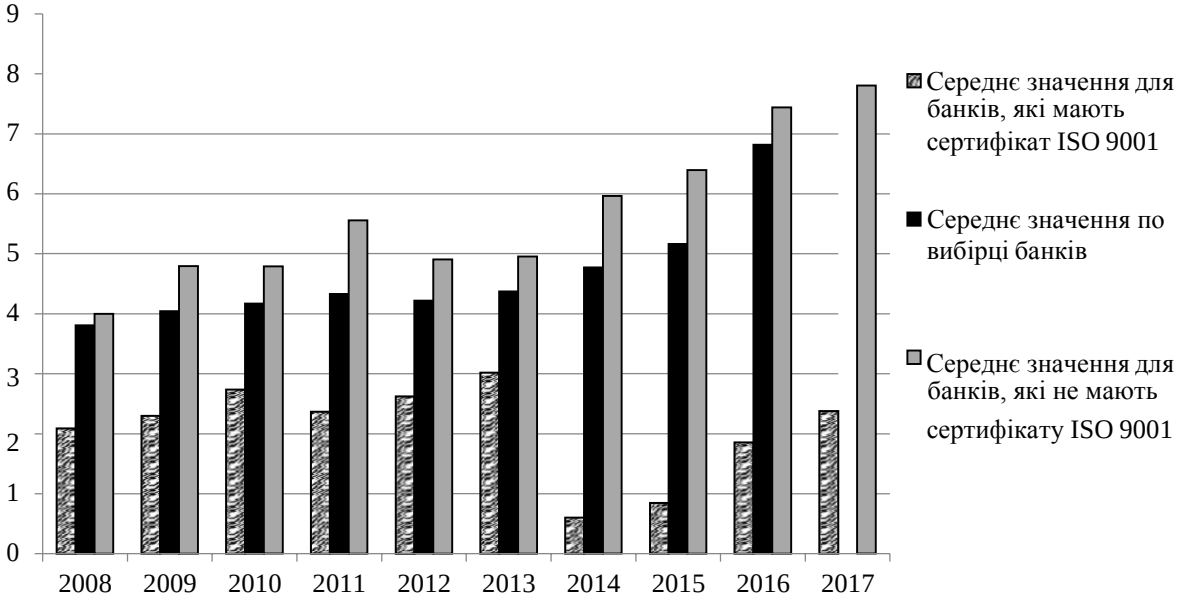


Рисунок 1.7 – Статистичні дані, що описують частку активів вибраних банків різних типів у банківській системі України за період 2008-2017 років, % (побудовано за даними [33])

Результативною змінною, що використовується для визначення ефективності банків, є рентабельність активів банків, розрахована як відношення прибутку до оподаткування до

сукупних активів банку, визначене у відсотках. Як бачимо з рисунку 1.8 середня прибутковість активів сертифікованих банків була суттєво вищою, ніж показник інших банків вибірки протягом всіх досліджених періодів (у збиткові для всіх банків роки, рівень збитків банків, що мали підтвердження відповідності систем менеджменту якості вимогам стандарту, був нижчим порівняно з іншими банками).

Таким чином, попередній аналіз засвідчив, що в цілому зусилля банків, спрямовані на забезпечення відповідності систем менеджменту якості вимогам міжнародних стандартів, не дають значного ефекту у забезпеченні додаткових доходів, однак відіграють значну роль у підтриманні фінансової стійкості та прибутковості їх діяльності.

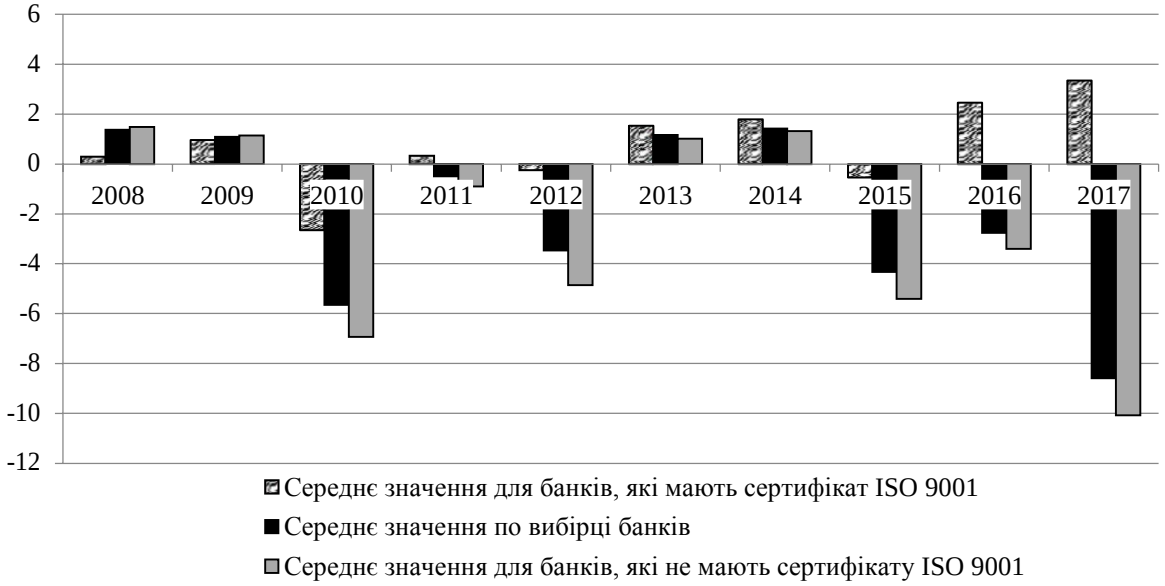


Рисунок 1.8 – Статистичні дані, що описують рентабельність активів вибірки банків різних типів за період 2008-2017 років, %(побудовано за даними [33])

Обраний метод економетричного аналізу передбачає логарифмування даних. Враховуючи той факт, що розрахункові показники рентабельності активів банків у вибірці приймали також від'ємні значення, перед проведенням логарифмування змінних моделі було здійснено нормалізацію рентабельності активів шляхом додавання абсолютного рівня найменшого від'ємного значення індикатора до всіх спостережень індикатора у вибірці.

У той же час, остаточні висновки щодо підтвердження чи спростування висунутої гіпотези можна сформулювати лише за результатами економетричного моделювання. Отже, на першому етапі оцінимо ефективність сформованої вибірки банків на основі проведення стохастичного фронтірного аналізу засобами програмного забезпечення Stata 12 SE. Відмітимо, що даний інструментарій передбачає чотири специфікації моделі фронтірного стохастичного аналізу. Для вибору специфікації порівняємо параметри адекватності побудованих моделей (табл. 1.10).

Таблиця 1.10 – Критерії адекватності різних специфікацій моделі оцінювання ефективності комерційних банків

Функція моделі / Фактор часу	Виробнича функція (Production function)	Функція витрат (Cost function)
Незмінна у часі (Time-invariant model)	Wald chi2(7) = 50,03 Prob > chi2 = 0,0000 Log likelihood = -128.81166	Wald chi2(7) = 50,03 Prob > chi2 = 0,0000 Log likelihood = -128,81166
Модель зі зміною часу (Time-varying decay model)	Wald chi2(7) = 20,01 Prob > chi2 = 0,0055	Wald chi2(7) = 124,24 Prob > chi2 = 0,0000

	Log likelihood = 74,083698	Log likelihood = -116,0735

Приймаючи до уваги критерії адекватності доцільно обрати для оцінювання модель зі зміною часу, засновану на функції витрат. Особливістю даної специфікації є, з одного боку, припущення про наявність інваріантних незмінних факторів, які не включені до вибірки, але впливають на результат, та, з іншого боку, врахування необмеженої кількості вхідних факторів [188]. урахуванням переліку вхідних та вихідних параметрів побудована економетрична модель для оцінювання панельних даних має наступний вигляд:

$$\ln ROA_{it} = \beta_0 + \sum_{j=1}^{7} \beta_j \ln x_{jit} + \upsilon_{it} + u_{it} \quad (1.16)$$

де ROA_{it} – рентабельність активів *i*-го банку в періоді *t*;

x_{jit} – j-та факторна змінна для *i*-го банку в періоді *t*;

υ_{it} – похибка вимірювання та специфікації;

u_{it} – значення неефективності *i*-го банку в періоді *t*.

Результати оцінювання факторів, що визначають ефективність українських комерційних банків представлено в табл. 1.11. Аналізуючи результати проведених розрахунків, відмітимо, що з семи факторних ознак статистично значимі коефіцієнти впливу було отримано для п’яти параметрів.

Таблиця 1.11 – Результати оцінювання ефективності банків та впливу факторів, що її визначають

Факторна ознака	Коефіцієнт	Стандартна похибка	z	P>|z|	Нижні 95%	Верхні 95%
Загально-адміністративні витрати	-0,070	0,195	-0,36	0,719	-0,452	0,312
Витрати на персонал	1,396	0,297	4,70	0,000	0,814	1,979
Чиста процентна маржа	2,609	0,290	8,99	0,000	2,040	3,178
Чиста непроцентна маржа	-0,381	-0,209	1,82	0,068	-0,792	0,028
Чистий спред	-1,676	0,216	-7,76	0,000	-2,099	-1,252
Негативно класифіковані кредити	-0,114	0,113	-1,01	0,312	-0,337	0,107
Частка активів банку	0,303	0,113	2,67	0,008	0,080	0,526
Константа	5,091	0,679	7,49	0,000	3,759	6,423
Параметри моделі						
mu	-188,286	2809,628	-0,07	0,947	-5695,055	5318,483
eta	-0,324	0,076	-4,22	0,000	-0,474	-0,173
$\ln sigma^2$	5,778	14,637	0,39	0,693	-22,911	34,468
ilgtgamma	6,449	14,663	0,44	0,660	-22,291	35,190
$sigma^2$	323,362	4733,36			1,12e-10	9,32e+14
gamma	0,998	0,023			2,08e-10	1
$sigma\_u^2$	322,852	4733,361			-8954,365	9600,069
$sigma\_v^2$	0,510	0,078			0,356	0,664

Так, факторами-стимуляторами ефективності функціонування банку можна вважати такі показники як витрати на персонал, чиста процентна маржа та частка активів банку, що цілком закономірно, враховуючи інвестиційний характер людського капіталу як статті витрат організації, наявність безпосереднього зв’язку між формуванням процентних доходів та прибутку банку, а також значну роль ефекту масштабу в забезпеченні прибутковості банківської діяльності. З іншого боку, неочікуваними виявилися результати, щодо наявності оберненого зв’язку між такими параметрами як чиста непроцентна маржа та чистий спред на

ефективність банку, що може бути результатом недостатньої дохідності окремих груп активів та пасивів банку та, в результаті, формуванням низьких значень отриманих показників зі зворотними відносно інших параметрів тенденціями їх динаміки. У той же час відмітимо, що параметри загальноадміністративних витрат та негативно класифікованих кредитів мають від'ємний знак при розрахованих коефіцієнтах, що, попри статистичну незначимість, свідчить про наявний потенціал дестимулюючого впливу даних факторів у формуванні банківської ефективності.

Оцінені значення ефективності діяльності для досліджуваної вибірки банків представлено у таблиці 1.12.

Таблиця 1.12 – Результати оцінювання ефективності банків України за період 2008-2017 років

Назва банку	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017
АТ «Укрексімбанк»	1,27	1,39	1,58	1,88	2,40	3,37	5,40	10,41	26,02	93,85
АТ «ОЩАДБАНК»	1,15	1,21	1,31	1,45	1,68	2,05	2,71	4,02	6,96	15,16
ПАТ КБ «ПРИВАТБАНК»	1,01	1,02	1,02	1,03	1,04	1,06	1,09	1,13	1,18	1,27
ПАТ «КРЕДІ АГРІКОЛЬ БАНК»	1,03	1,04	1,06	1,08	1,11	1,16	1,22	1,33	1,50	1,78
АТ «ПЕРШИЙ ІНВЕСТИЦІЙНИЙ БАНК»	1,12	1,17	1,24	1,35	1,52	1,78	2,23	3,07	4,80	9,04
АТ «Райффайзен Банк Аваль»	1,03	1,04	1,06	1,08	1,12	1,17	1,24	1,36	1,54	1,86
АБ «УКРГАЗБАНК»	1,29	1,42	1,63	1,96	2,54	3,64	6,00	12,02	31,73	123,4
АТ «УкрСиббанк»	1,02	1,03	1,05	1,07	1,09	1,13	1,19	1,28	1,42	1,66
ПАТ «АЛЬФА-БАНК»	1,06	1,09	1,12	1,17	1,25	1,37	1,55	1,84	2,37	3,40
ПАТ «КРЕДИТПРОМБАНК»	1,04	1,06	1,09	1,12	1,18	1,26	-	-	-	-

З даних таблиці можна відмітити тенденцію щодо перманентного зростання ефективності протягом дослідженого періоду для всієї вибірки банків. У той же час, метою дослідження є перевірка наявності впливу сертифікації банків на ефективність їх діяльності. Для оцінювання було обрано модель «різниці різниць» (Difference-in-Differences model), яка базується на формуванні вибірки з двох груп об'єктів дослідження. Перша група (дослідна) протягом періоду дослідження підпадає під дію певних факторів (у нашому випадку проходить процедуру сертифікації). Друга група (контрольна) не підпадає під вплив даного фактору протягом періоду дослідження. Порівняння оцінок середньої зміни результативної ознаки у період дії фактору та до його виникнення для двох груп факторів дозволяє оцінити вплив даного фактору на результативну ознаку [28]. Таким чином, модель дозволяє усунути вплив постійних відмінностей у параметрах об'єктів, що належать до різних досліджуваних груп, а також нівелювати вплив фактору часу на зміну результативної ознаки. Економетрична модель має наступний вигляд:

$$Eff = \beta_0 + \beta_1 dB + \delta_0 d2 + \delta_1 d2 \cdot dB + u \qquad (1.17)$$

де Eff – результативна змінна, що позначає ефективність банківської діяльності;

$d2$ – фіктивна змінна, що позначає період наявності впливу факторної ознаки – сертифікації менеджменту якості банківських послуг;

δ_0 – коефіцієнт, що враховує вплив параметрів, які спричинили б зміну результативної ознаки при відсутності фактору впливу сертифікації;

dB – фіктивна змінна, що позначає дослідну групу – банки, які отримали сертифікати відповідності стандартам якості;

β_1 – коефіцієнт, що враховує відмінності між дослідною та контрольною групами до початку процедур сертифікації;

$d2 \cdot dB$ – фіктивна змінна взаємодії дослідної групи та періоду впливу фактору;

δ_1 – коефіцієнт впливу сертифікації систем менеджменту якості на ефективність банківської діяльності;

u – похибка вимірювання та специфікації.

Результати розрахунків щодо ідентифікації ролі наявності сертифікату про відповідність системи менеджменту якості банків вимогам міжнародних стандартів групи ISO 9001 у забезпеченні ефективності банківської діяльності демонструє табл. 1.13.

Таблиця 1.13 – Результати оцінювання впливу сертифікації банківських послуг на ефективність діяльності банку

Параметр	Значення ефективності	Стандартна похибка	|t|	P>|t|
До проходження процедури сертифікації				
Контрольна група	1,095			
Дослідна група	1,102			
β_1	0,008	0,005	1,58	0,099
Після проходження процедури сертифікації				
Контрольна група	4,970			
Дослідна група	6,079			
δ_0	1,110	0,352	1,87	0,076
δ_1	1,102	0,171	2,61	0,009

Аналізуючи результати оцінювання відмітимо, що відмінності у значеннях ефективності банківської діяльності для дослідної та контрольної груп банків спостерігались на всіх етапах дослідження. У той же час розрив значень суттєво зростає при аналізі параметрів ефективності сертифікованих банків у період після проходження ними процедури підтвердження системи менеджменту якості вимогам міжнародних стандартів. Таким чином, можна зробити висновок про підтвердження раніше висунутої гіпотези про наявність позитивного впливу сертифікації банківського бізнесу на фінансові параметри його діяльності. Враховуючи комплексний характер показника ефективності банку, можна припустити, що позитивний вплив сертифікації менеджменту якості банківських послуг буде проявлятися також і на рівні управління ризиками банку, що, в тому числі, обумовить зростання рівня інформаційної безпеки у банківському секторі.

Результати дослідження можна узагальнити у вигляді науково-методичного підходу, який представлено на рисунку 1.9.

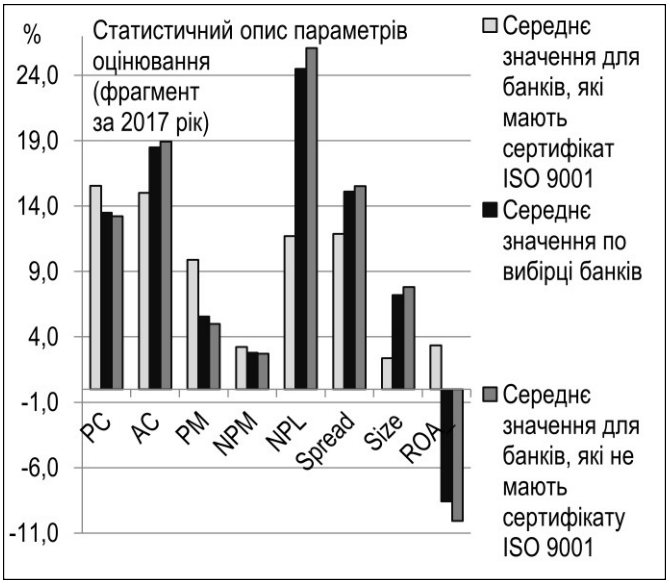
Інформаційна база дослідження

Об'єкт дослідження – 10 банків, 4 з яких мали підтверджений сертифікат відповідності системи УЯ БП стандарту якості ISO 9001 (дослідна група), 6 обрано з різних груп, які є маркетмейкерами БП (контрольна

Період дослідження – 2008-2017 рр. (обумовлено наявністю стандарту якості принаймні в одному з 4 банків).

Вхідні параметри для оцінювання ефективності банківської діяльності– витрати на персонал на одиницю доходів (PC); загальноадміністративні витрати на одиницю доходів (AC); чиста процентна маржа (PM); чиста непроцентна маржа (NPM); чистий спред (Spread); частка негативно класифікованих кредитів у структурі кредитного портфелю банку (NPL); частка активів банку в банківській системі (Size).

Результативний параметр ефективності – рентабельність активів банку (ROA).



Формалізований параметр наявності стандартів якості в банку – фіктивна змінна, яка приймає значення [1;0].

Оцінювання ефективності банків

Вибір для оцінювання специфікації моделі зі зміною часу, заснованої на функції витрат. Критерієм вибору є максимізація параметрів адекватності (Waldchi2; Prob>chi2;

$$\ln ROA_{it} = \beta_0 + \sum_{j=1}^{\tilde{} } \beta_j \ln x_{jit} + \upsilon_{it} + u_{it}$$

де ROA_{it} – рентабельність активів *i*-го банку в періоді *t*; x_{jit} – *j*-та факторна змінна для *i*-го банку в періоді *t*; υ_{it} – похибка вимірювання та специфікації; u_{it} – значення неефективності *i*-го банку в періоді *t*.

Коефіцієнти впливу факторних параметрів на ефективність банку:
PC→1,396***; AC→-0,070; PM→2,609***;
NPM→-0,381*; Spread→ -1,676***;
NPL→ -0,114; Size→0,303**

*** – значимість 99%; ** – значимість 95%;
* – значимість 90%

Оцінювання впливу стандартів якості БП на ефективність банку

Difference-in-**Differences модель оцінювання впливу стандартів якості БП на ефективність банку:**

$$Eff = \beta_0 + \beta_1 dB + \delta_0 d2 + \delta_1 d2 \cdot dB + u$$

де Eff – ефективність банківської діяльності; $d2$ – фіктивна змінна періоду впливу стандартів якості; δ_0 – коефіцієнт впливу параметрів, які спричинили б зміну ефективності привідсутності сертифікації; dB – фіктивна змінна дослідної групи; β_1 – коефіцієнт відмінностей дослідної та контрольної груп до початку сертифікації; $d2 \cdot dB$ – фіктивна змінна взаємодії дослідної групи та періоду впливу фактору; δ_1 – коефіцієнт впливу стандартів якості на ефективність банку; u – похибка вимірювання та специфікації.

Параметр	*Eff*	Станд. похибка	|t|	P>|t|
До проходження процедури сертифікації				
Контрольна група	1,095			
Дослідна група	1,102			
β_1	0,008	0,005	1,58	0,099
Після проходження процедури сертифікації				
Контрольна група	4,970			
Дослідна група	6,079			
δ_0	1,110	0,352	1,87	0,076
δ_1	1,102	0,171	2,61	0,009

Рисунок 1.9 – Науково-методичний підхід до оцінювання впливу сертифікації систем менеджменту якості банківських послуг на ефективність діяльності банку

2. АНАЛІЗ ТА ОЦІНКА НАСЛІДКІВ КІБЕРШАХРАЙСТВ У БАНКАХ

2.1 Аналіз наслідків кібершахрайств в банківській системі України

Впровадження банківських карт і використання комп'ютерних технологій в сфері платежів є характерною рисою повсякденного життя. Швидкими темпами розвиваються безготівкові форми розрахунків. Платежі, що здійснюються без участі готівки, сприяють прискоренню оборотності, скороченню кількості грошових коштів, необхідних в обігу, що, як наслідок, призводить до зниження витрат обігу, збільшенню прозорості розрахунків [37]. Завдяки своєї простоти, масовості, доступності технологій, операції з банківськими картками найбільш приваблюють шахраїв.

З 01.01.2017 по 26.08.2017 платіжні сервіси системи Exchange-Online зафіксували 12416 підозрілих операцій на загальну суму 3409000 гривень. В операціях прийняло участь 7390 банківських карт 135 банків з 53 країн, в тому числі з 67 українських банків. Дані кошти шахраї намагалися вивести за допомогою мобільних пристроїв. [38]

На рисунку 2.1 представлено країни, за картками яких проводились спроби операцій, ідентифікованих системою, як шахрайська, та відсоток операцій, які дійсно виявилися шахрайськими.

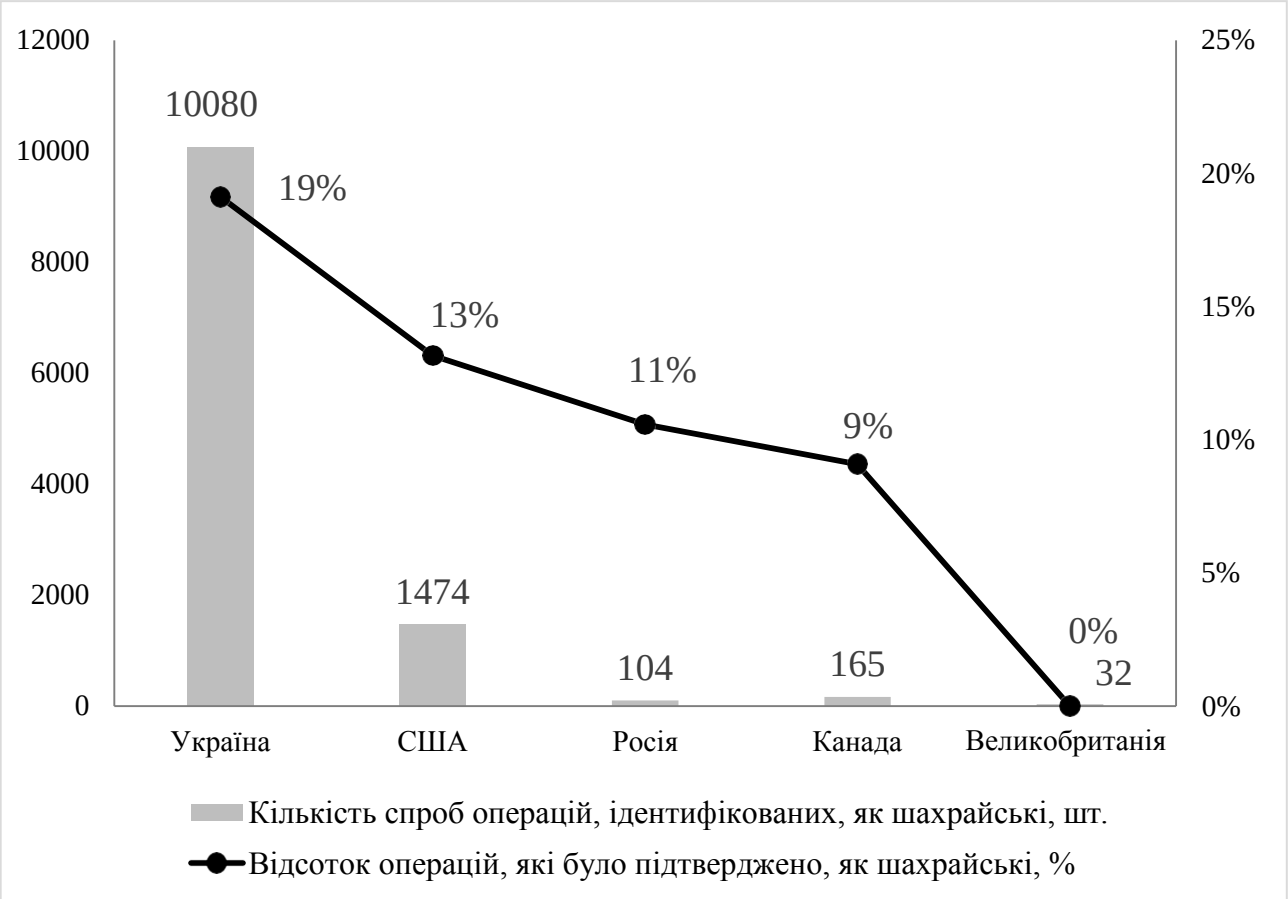


Рисунок 2.1 – Аналіз шахрайських операцій, здійснених у 2017 році (графік побудовано на основі статистичних даних Української міжбанківської Асоціації членів платіжних систем [38])

Дані рисунку 2.1 свідчать про те, що Україна займає лідуюче місце та втрапила в п’ятірку країн, в яких банківські платіжні операції є не досить захищеними. Виявилося, що 19% операцій є дійсно шахрайськими і це перевищує обсяги шахрайств в інших країнах. За допомогою кібершахрайств з карток українців було знято 238955 гривень. Тобто, банківські платіжні системи через слабкий захист потенційно можуть втрачати клієнтів через той факт, що вони

можуть стати об'єктами шахрайства. Тому це не тільки проблема банків, але й соціальна проблема, яку треба вирішувати комплексно та із залученням різних структур – держави, населення, банків, інвесторів.

На сьогоднішній день найбільш поширеними видами шахрайських операцій з банківським картками є:

– скімінг – викрадення інформації з магнітної стрічки картки або ПІН-коду за допомогою спеціальних пристроїв;

– трапінг – встановлення пасток на шатер банкомату;

– фізичне пошкодження банкоматів;

– фішинг – шахрайство за допомогою Інтернету;

– вішинг – шахрайство за допомогою мобільного звязку;

– вірусні та хакерські атаки, тощо.

На рисунку 2.2 наведені групи шахрайських операцій, здійснених за 1 півріччя 2017 року та об'єднаних за однаковим способом здійснення, які представлені у відсотках.

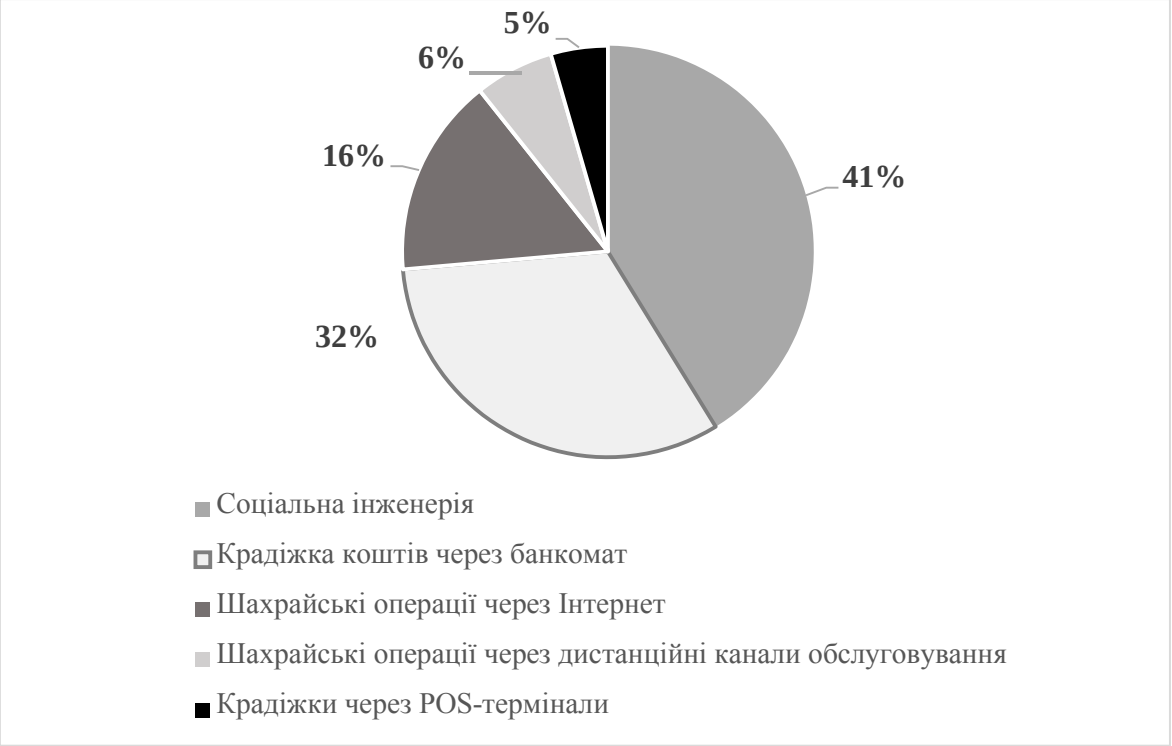


Рисунок 2.2 – Групи шахрайських операцій, об'єднаних за однаковим способом здійснення (графік побудовано на основі статистичних даних Української міжбанківської Асоціації членів платіжних систем [39])

Найбільша доля шахрайських операцій, які було здійснено за допомогою методів соціальної інженерії (41%), включають в себе здійснення вішингу та фішингу, тобто шахраї виманюють дані платіжних карток у клієнтів, отримують доступ до рахунків та знімають кошти. Зазвичай жертвами соціальної інженерії стають літні люди (від 55 і старші) – 15%, і середнього віку (35-44) – 13%.

Досить популярними у шахраїв є способи крадіжок коштів через банкомат (32%) та через Інтернет (16%) (див. рис. 2.2). Тобто, банківська система кібербезпеки повинна розробити додаткові способи захисту операцій від цих видів шахрайств.

Шахрайство шляхом соціальної інженерії – це глобальна проблема. Станом на кінець першого кварталу 2017 року найбільшої шкоди від фішингових атак зазнали 51,70% банків світу. До країн з найвищим відсотком нападу на користувачів відносяться: Китай (20,87%), Бразилія (19,16%), Макао (11,94%), Російська Федерація (11,29%) , Австралія (10,73%),

Аргентина (10,42%), Нова Зеландія (10,18%), Катар (9,87%), Казахстан (9,61%), Тайвань (9,27%). За часткою атакованих користувачів від вішингу до найбільш атакованих країн відносяться: Росія (1,2%), Узбекистан (0,40%), Казахстан (0,36%), Таджикистан (0,35%), Туреччина (0,34%), Молдова (0,31%), Україна (0,29%), Киргизстан (0,27%), Білорусь (0,26%) та Латвія (0,23%) [40].

В Україні у 2017 року збитки клієнтів банків від соціальної інженерії склали 509,72 млн грн., що практично вдвічі перевищило збитки за 2016 рік та у 9 разів за 2015 рік. Також збільшилася середня сума шахрайської операції, здійсненої за допомогою методів соціальної інженерії, до 2543 грн. у 2017 році, що в 1,8 разів перевищує даний показник у 2016 році (див. табл. 2.1).

Таблиця 2.1 - Збитки від шахрайських операцій, здійснених за допомогою соціальної інженерії та засобів Інтернет*

Вид збитку	2015		2016		2017	
	Соціальна інженерія	Інтернет	Соціальна інженерія	Інтернет	Соціальна інженерія	Інтернет
Середня сума збитку від однієї шахрайської операції, грн.	834	206	1403	345	2543	145
Загальні збитки від шахрайських операцій, млн. грн.	51,74	32,62	275,45	63,68	509,72	159,91

* Таблицю побудовано на основі даних Української міжбанківської Асоціації членів платіжних систем [41, 42]

В Україні найбільша кількість випадків платіжного шахрайства з використанням методів соціальної інженерії здійснюється в середовищі Card-Not-Present (операції здійснюються без наявності картки та фізичної присутності користувача), у порівнянні із обслуговуванням через банкомати, POS-термінали та дистанційне банківське обслуговування (див. рис. 2.3).

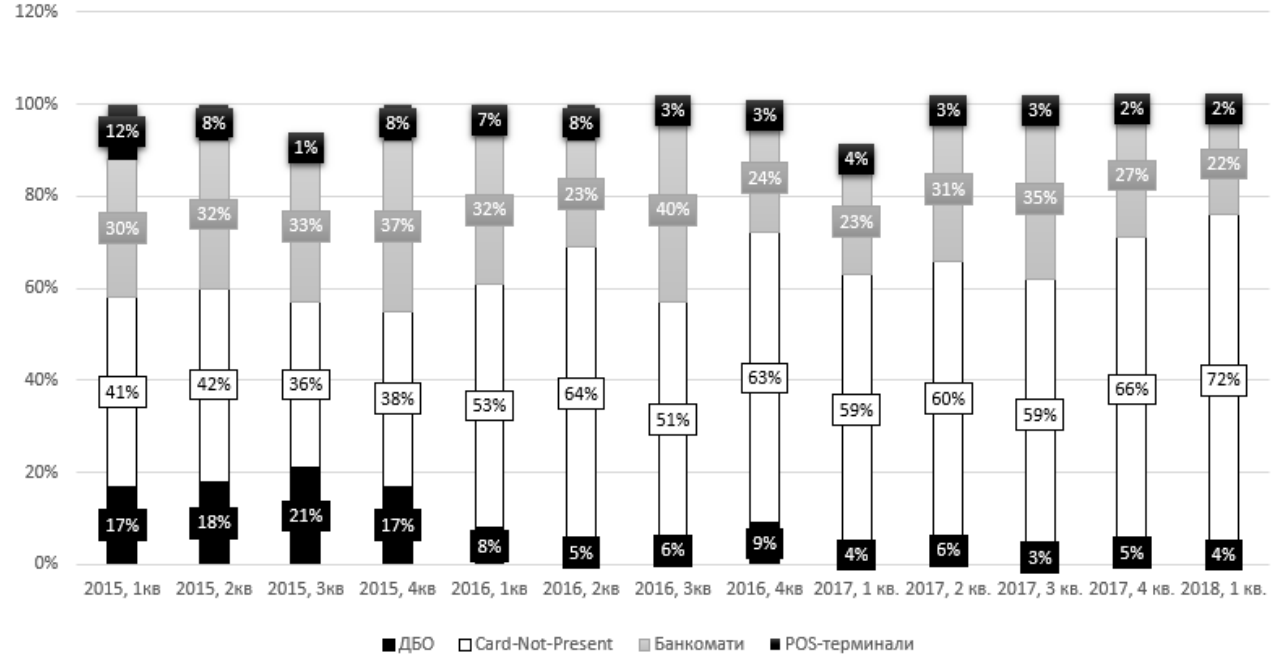


Рисунок 2.3 – Шахрайські операції за різними видами банківського обслуговування (графік побудовано на основі статистичних даних Української міжбанківської Асоціації членів платіжних систем [43])

Методи соціальної інженерії набирають популярності у шахраїв, оскільки зловмисники не тільки отримують дані платіжної картки, але й ідентифікаційні дані клієнта. Також даний спосіб шахрайства є досить простим у здійсненні. Хоча банківські співробітники й попереджають своїх клієнтів не розголошувати платіжну інформацію через телефон, але шахраї мають досить багато способів психологічного впливу на жертву.

На основі проведеного аналізу наслідків кібершахрайств, які відбуваються в сфері використання клієнтами банків платіжних засобів, найбільш вразливим місцем є сам клієнт, який під дією різних методів соціальної інженерії становиться об'єктом шахрайства. Для боротьби з даним способом шахрайства українські банки не мають досить дієвих інструментів. На нашу думку, для даного випадку шахрайства доцільно застосовувати сукупність засобів, що базуються на методах інтелектуального аналізу та інформаційних технологій.

Автори статті вбачають організацію наступних заходів для боротьби із кібершахрайствами, особливо соціальною інженерією:

1) доцільно побудувати алгоритми із використанням інструментів Data Mining, за допомогою яких відбуватиметься відслідковування операцій та перевірка їх на предмет шахрайства у відповідності з певними ознаками. Дана проблематика розкрита авторами даної статті у роботі [44]. Особливо дієвим є застосування нейронних мереж, що дозволить постійно налаштовувати систему на нові ознаки шахрайства. Тобто у випадку, коли шахрай знімає всю суму коштів з рахунку, то система здійснює перевірку даної операції. У випадку шахрайства операція блокується;

2) розробка автоматизованого модулю моніторингу, вбудованого в банківську систему та різні платіжні системи, функція якого – автоматична перевірка операцій на предмет шахрайства, блокування операцій та подвійна (потрійна) ідентифікація клієнта. Частково це реалізовано в існуючих платіжних системах, але у випадках соціальної інженерії системи не працюють. Коли система блокує операцію з ознаками шахрайства, то вона повинна надіслати клієнту повідомлення, в якому вказується тип операції з вказівкою місця її здійснення та суми. Наприклад, якщо шахрай знаходиться в іншій країні, то клієнту надходить повідомлення, що є спроба зняття з його рахунку коштів на вказану суму із вказаної країни. Якщо клієнт не ініціював операцію, то він повинен надіслати банку код з відміною або з блокуванням;

3) створення інтегрованого банку даних, який буде містити інформацію щодо: способу, методу, виду шахрайства, характерних ознак, характеристик шахрая та його жертви, мобільні телефони, IP-адреси шахраїв, тощо. Дана інформація дозволить формувати нові правила перевірки та контролю банківських операцій на предмет відповідності ознакам шахрайства. Подібні бази повинні створюватися не для окремих банків, а для всієї банківської системи, оскільки дана інформація є типовою;

4) жорстке обмеження прав доступу працівників банків до бази даних клієнтів для зменшення шахрайств з боку працівників. Це можливе за рахунок чіткого розмежування прав доступу до інформації, налаштованого на програмному рівні. Даний підхід потребує створення та модифікацію посадових інструкцій працівників банків та розробку інструкцій та рекомендацій головних банків та Національного банку України;

5) збільшити кількість інструментів соціальної роботи із населенням через засоби масової інформації та Інтернет для зменшення випадків соціального шахрайства. Це сприятиме формуванню ефективної системи взаємодії між банками та клієнтами.

Таким чином, здійснення кібершахрайських операцій з банківськими картками та різними платіжними операціями має негативні наслідки для стабільності фінансової системи держави. Це проявляється у гальмуванні поширення безготівкової форми оплати, зниженні довіри населення до банків у частині зберігання коштів та кредитування. Недостатні знання про механізми кіберзлочинів ускладнюють процес визначення шахрайства. Вивчення ознак шахрайства, в першу чергу, необхідно для розробки більш дієвих засобів і методів захисту від даного виду злочину. Аналіз наслідків кібершахрайств дозволяє виявити слабкі місця в

банківській системі та сприяє накопиченню інформації щодо способів, методів шахрайства, портретів шахраїв та їх жертв, формування ознак шахрайства.

В результаті проведеного в статті аналізу виявлено, що збитки банків в результаті кібершахрайств зростають, не дивлячись на заходи служб безпеки. Клієнти та банки втрачають кошти завдяки різним шахрайським способам, серед яких найбільшої шкоди завдають методи соціальної інженерії. Для боротьби з такого роду шахрайствами запропоновано ряд заходів, реалізація яких потребує застосування методів Data Mining та розвинутих інформаційних технологій.

2.2 Оцінка 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 2.4).

Рисунок 2.4 – 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 2.2.

Таблиця 2.2 – Опис вхідних змінних

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

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

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

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

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

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

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

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

Змінна X6 показує забезпечення країни правової середи, яка базується на принципах верховенства права.

Змінна X7 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 X8 показує зміну в часі загального рівня цін на товари та послуги в країні.

Змінна X9 відображає долю населення сімейний дохід якої нижче абсолютного рівня.

Змінна X10 показує загальну кількість людей проживаючих у даній країні.

Змінна X11 відображає знецінення грошей.

Змінна X12 відображає рівень економічного розвитку.

Змінна X14 та X13 показує кількість чоловіків і жінок проживаючих в країні.

Змінна X15 відображає кількість фіксованих телефонних абонентів.

Змінна X16 показує кількість безпечних інтернет серверів.

Змінна X17 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 X18 показує наскільки кримінальна активність в країні.

Змінна X19 відображає оцінку прогресу людського розвитку у трьох сферах, а саме довготривале та здорове життя населення, доступу до знань, гідний рівень життя суспільства.

Змінна X20 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 [45]. 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:

$$t_{y(\text{е})} = \beta_1 \cdot t_{x3} + \beta_2 \cdot t_{x12} + \beta_2 \cdot t_{x11} + \beta_2 \cdot t_{x8} + \beta_2 \cdot t_{x9} + \beta_2 \cdot t_{x1} + \\ + \beta_2 \cdot t_{x17} + \varepsilon, \quad (2.1)$$

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:

$$t_{y(\text{п})} = \beta_1 \cdot t_{x18} + \beta_2 \cdot t_{x3} + \beta_2 \cdot t_{x2} + \beta_2 \cdot t_{x4} + \beta_2 \cdot t_{x7} + \beta_2 \cdot t_{x20} + \varepsilon, \quad (2.2)$$

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:

$$t_{y(c)} = \beta_1 \cdot t_{x4} + \beta_2 \cdot t_{x5} + \beta_2 \cdot t_{x7} + \beta_2 \cdot t_{x9} + \beta_2 \cdot t_{x10} + \beta_2 \cdot t_{x13} + \\ + \beta_1 \cdot t_{x14} + \beta_2 \cdot t_{x15} + \beta_2 \cdot t_{x16} + \beta_2 \cdot t_{x17} + \beta_2 \cdot t_{x19} + \varepsilon, \quad (2.3)$$

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:

$$tj = \frac{xi - \bar{x}i}{\sigma xi} \quad (2.4)$$

де xi значення в xi спостереженні

$$t_y = \frac{y - \bar{y}}{\sigma y} \quad (2.5)$$

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 [45].

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 [46]:

– адитивної

$$F(x_i) = \sum_{j=1}^{n} \omega_j \cdot x_{ij} \quad (2.6)$$

– мультиплікативної

$$F(x_i) = \prod_{j=1}^{n} x_{ij}^{\omega_j} \tag{2.7}$$

Які вважаються найпоширенішими [47] для формування класичного виду адитивно-мультиплікативної згортки.

Недоліки методів згортки:

– на адекватність впливає розподіл альтернатив у вибірці критеріїв [47];

– недостане значення одного критерію може компенсуватися значенням іншого критерія [48];

– часткові функції корисносіт повинні бути односпрямовані [49].

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 [50]. Тому необхідно критерії поділити на:

Стимулятори:

$$f_j(x) \to max, \qquad j = \overline{1,k}, x \epsilon S \tag{2.8}$$

Дестимулятори:

$$f_j(x) \to min, \qquad j = \overline{1,k}, x \epsilon D \tag{2.9}$$

де S та D – множина критеріїв.

Нормування стимуляторів проводиться за формулою:

$$x'_{ij} = \frac{x_{ij}}{x_{maxj}} \tag{2.10}$$

Нормування дистимуляторів проводиться за наступною формулою:

$$x'_{ij} = \frac{x_{ij}}{x_{minj}} \tag{2.11}$$

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

$$\rho(y, z) \geq 0 \ , \rho(y, z) = 0, y \Leftrightarrow z; \tag{2.12}$$

$$\rho(y, z) = \rho(z, y); \tag{2.13}$$

$$\rho(y, z) \leq \rho(w, y) + \rho(y, z). \tag{2.14}$$

Метрика Мінковського має наступний вигляд:

$$\rho(y, z) = \left(\sum_{i=1}^{n} a_i^s \cdot |y_i - z_i|^r\right)^{1/r} \tag{2.15}$$

Функція корисності матиме вигляд:

$$F(x_i) = 1 - \sqrt[n]{\sum_{j=1}^{k} \omega_j \cdot \left|1 - \frac{x^{ij}}{x_{maxj}}\right|^n + \sum_{j=k+1}^{n} \omega_j \cdot \left|1 - \frac{x^{minj}}{x_{ij}}\right|^n} \quad (2.16)$$

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. [51-53]

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 2.5).

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.

$$R_t = \frac{n_{et} \cdot n_{st} \cdot}{\sqrt{(n_{et} + n_{st} + n_{pt}) \cdot (-n_{et} + n_{st} + n_{pt}) \cdot (n_{et} + n_{st} - n_{pt}) \cdot} \quad (2.17)$$
$$\frac{\cdot\, n_{pt}}{\sqrt{\cdot\, (n_{et} - n_{st} + n_{pt})}}$$

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:

$$\sin \alpha_{et} = \frac{n_{et}}{2 \cdot R_t} \quad (2.18)$$

$$\sin \alpha_{st} = \frac{n_{st}}{2 \cdot R_t} \quad (2.19)$$

$$\sin \alpha_{pt} = \frac{n_{pt}}{2 \cdot R_t} \quad (2.20)$$

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.

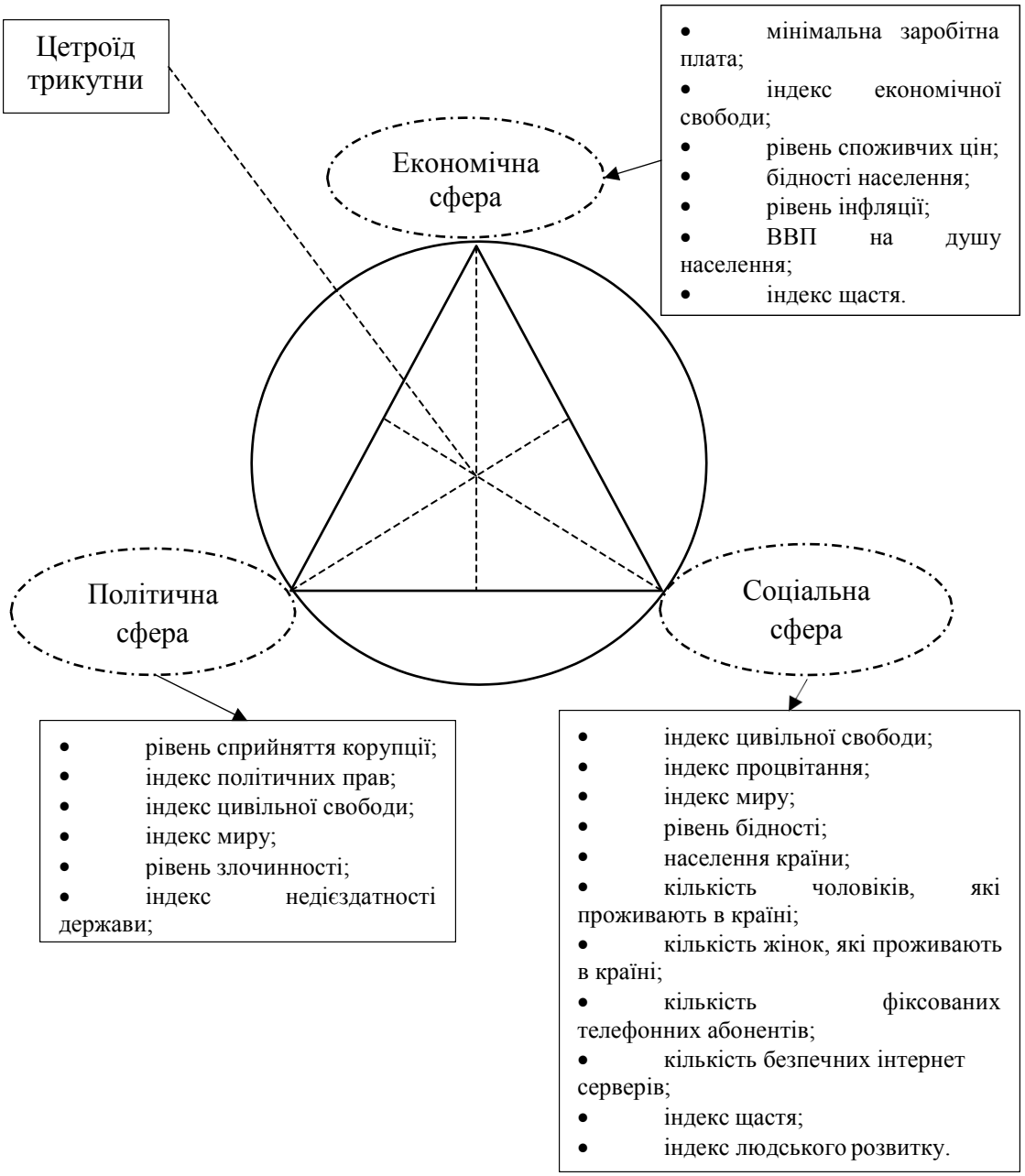


Рисунок 2.5 – Трикутник

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 [51-52].

Реалізацію моделі проведемо в програмному забезпечені STATISTICA. На рисунку 2.6 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 2.6 – 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 2.7.

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 2.7 – 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 2.8.

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 2.8 – Результати регресійної моделі для соціального стану

В результаті проведення первинного аналізу були отримані найбільш вагомі змінні:

— економічні

$$F_{\text{e}} = b_{i1} \cdot X_1 + b_{i2} \cdot X_3 + b_{i3} \cdot X_{12} \quad (2.21)$$

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

$$F_i = b_{i1} \cdot X_4 + b_{i2} \cdot X_5 + b_{i2} \cdot X_7 + b_{i2} \cdot X_{10} + b_{i2} \cdot X_{17} + \\ + b_{i2} \cdot X_{19} \quad (2.22)$$

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

$$F_i = b_{i1} \cdot X_2 + b_{i2} \cdot X_4 + b_{i3} \cdot X_{18} + b_{i4} \cdot X_{20} \quad (2.23)$$

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. 2.9).

C	C	C	Д	C	Д	Д	C	C	Д	C	C	C	C
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 2.9 – Відносна нормалізація показників

Як видно з рисунку 2.9 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. 2.10).

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 2.10 – 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. 2.11).

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 2.11 – 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. 2.12)

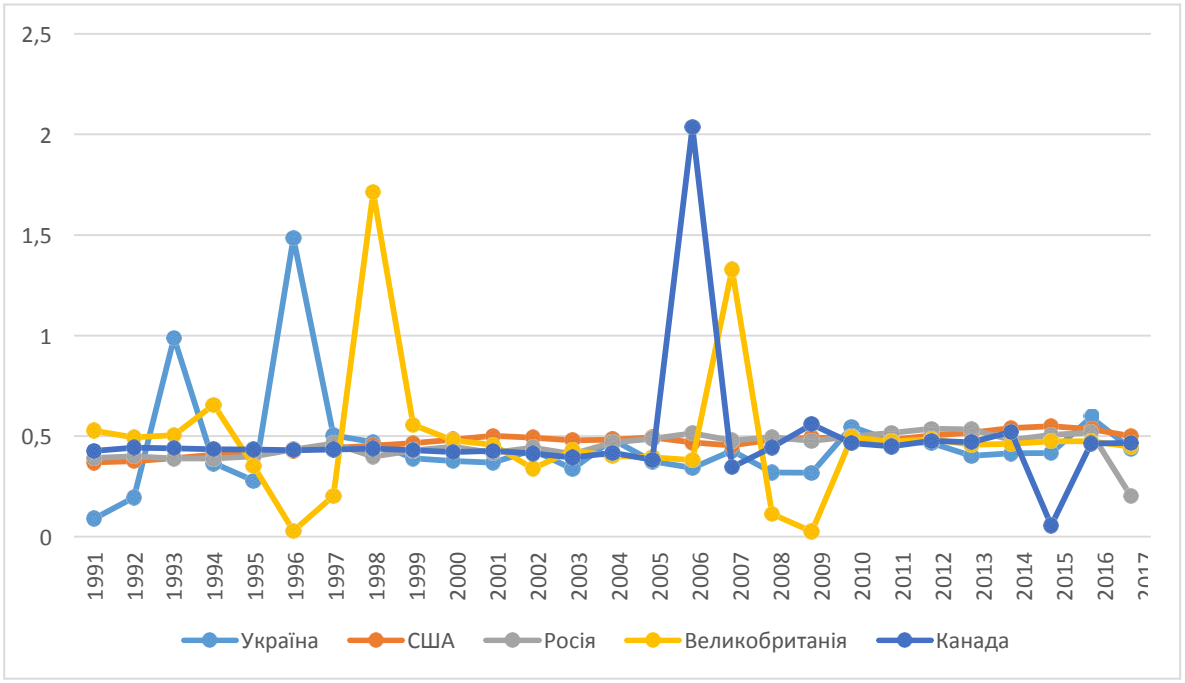


Рисунок 2.12 – Діаграма динаміки значень радіуса кола описаного навколо трикутника політичної та економічної ситуації України, США, Великобританії, Канади та Росії

На основі даних, які наведених на рисунку 2.12, 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. 2.12), 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 2.13.

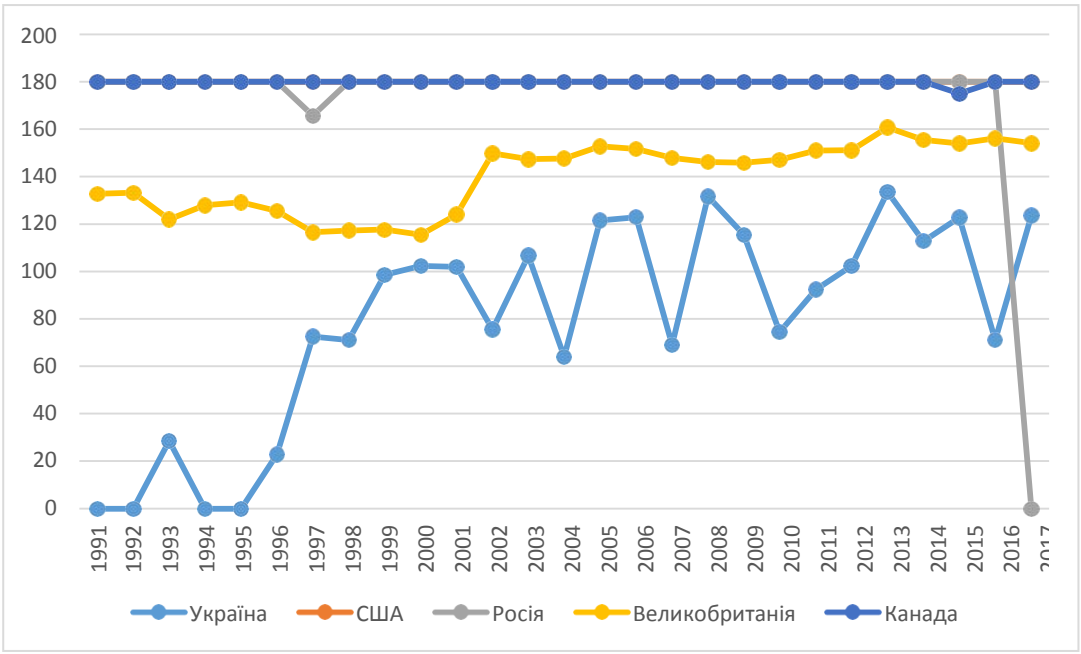


Рисунок 2.13 – Діаграма динаміки схильності до шахрайства в України, США, Великобританії, Канади та Росії

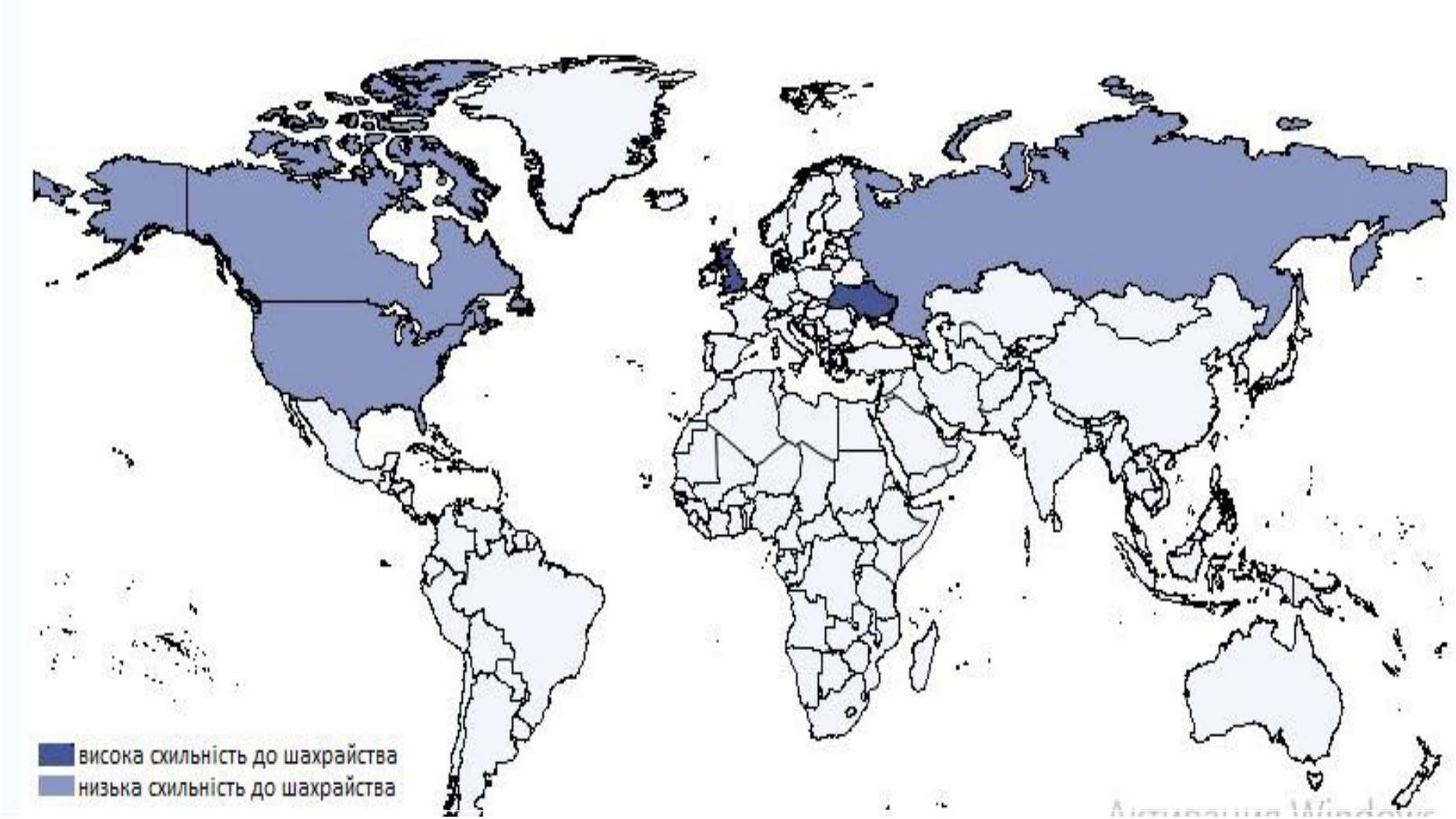


Рисунок 2.14 – Рівень впливу шахрайства по країнам

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

2.3 Оцінювання збитків банків від їх залучення до шахрайських операцій

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 [54]:

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. 2.3).

Таблиця 2.3 – 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 таблиці 2.3 необхідно зазначити, що їх визначення проводиться наступним чином (формула 2.24):

$$r_{lj} = \begin{cases} 1, \text{якщо } l-\text{й релевантний фактор ризиків надає } j-\text{ту перевагу} \\ 0, \text{якщо } l-\text{й релевантний фактор ризиків не надає } j-\text{тої переваги} \end{cases} \quad (2.24)$$

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 2.4 – 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 (табл. 2.5).

Таблиця 2.5 – 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 2.5, пропонується обраховувати наступним чином:

$$v_{lj} = \begin{bmatrix} L_{lj}|_{1-r_{lj}=1} \\ 0|_{1-r_{lj}=0} \end{bmatrix} \quad (2.25)$$

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

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

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

$v_{lj}|_{l=20\div25,\,j=1\div6}$ - 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 2.25, перейдемо послідовно до побудови витратних матриць:

$$L = \begin{matrix} min\{L_{lj}|_{1-r_{lj}=1}\} & \begin{matrix} min\{L_{lj}|_{1-r_{lj}=1}\} + \\ +min\{L_{lj}|_{1-r_{lj}=1}\} \end{matrix} & \begin{matrix} min\{L_{lj}|_{1-r_{lj}=1}\} + \\ +max\{L_{lj}|_{1-r_{lj}=1}\} \end{matrix} \\ max\{L_{lj}|_{1-r_{lj}=1}\} & \begin{matrix} max\{L_{lj}|_{1-r_{lj}=1}\} + \\ +min\{L_{lj}|_{1-r_{li}=1}\} \end{matrix} & \begin{matrix} max\{L_{lj}|_{1-r_{lj}=1}\} + \\ +max\{L_{lj}|_{1-r_{li}=1}\} \end{matrix} \end{matrix} \quad (2.26)$$

Визначення ймовірностей їх отримання в кожній конкретній ситуації:

$$P = \begin{matrix} maxP\,[min\{L_{lj}|_{1-r_{lj}=1}\}] & minP\,[max\{L_{lj}|_{1-r_{lj}=1}\}] \\ maxP\,[min\{L_{lj}|_{1-r_{lj}=1}\}] \times maxP\,[min\{L_{lj}|_{1-r_{lj}=1}\}] & maxP\,[min\{L_{lj}|_{1-r_{lj}=1}\}] \times minP\,[max\{L_{lj}|_{1-r_{lj}=1}\}] \\ minP\,[max\{L_{lj}|_{1-r_{lj}=1}\}] \times maxP\,[min\{L_{lj}|_{1-r_{lj}=1}\}] & minP\,[max\{L_{lj}|_{1-r_{lj}=1}\}] \times minP\,[max\{L_{lj}|_{1-r_{li}=1}\}] \end{matrix} \quad (2.27)$$

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:

$$R = \begin{matrix} min\{L_{lj}|_{1-r_{lj}=1}\} + min\{L_{lj}|_{1-r_{lj}=1}\} & min\{L_{lj}|_{1-r_{lj}=1}\} + max\{L_{lj}|_{1-r_{lj}=1}\} & max\{L_{lj}|_{1-r_{lj}=1}\} + max\{L_{lj}|_{1-r_{lj}=1}\} \\ maxP\,[min\{L_{lj}|_{1-r_{lj}=1}\}] \times maxP\,[min\{L_{lj}|_{1-r_{li}=1}\}] & minP\,[max\{L_{lj}|_{1-r_{lj}=1}\}] \times maxP\,[min\{L_{lj}|_{1-r_{li}=1}\}] & minP\,[max\{L_{lj}|_{1-r_{lj}=1}\}] \times minP\,[max\{L_{lj}|_{1-r_{li}=1}\}] \end{matrix} \quad (2.28)$$

$$\{P(R \le L\}^{L}$$

$$= \begin{matrix} min\{L_{lj}|_{1-r_{lj}=1}\} + min\{L_{lj}|_{1-r_{lj}=1}\} & min\{L_{lj}|_{1-r_{lj}=1}\} + max\{L_{lj}|_{1-r_{lj}=1}\} & max\{L_{lj}|_{1-r_{lj}=1}\} + min\{L_{lj}|_{1-r_{lj}=1}\} \\ maxP\,[min\{L_{lj}|_{1-r_{lj}=1}\}] \times maxP\,[min\{L_{lj}|_{1-r_{lj}=1}\}] & maxP\,[min\{L_{lj}|_{1-\eta_j=1}\}] \times maxP\,[min\{L_{lj}|_{1-r_{lj}=1}\}] + minP\,[max\{L_{lj}|_{1-r_{lj}=1}\}] \times maxP\,[min\{L_{lj}|_{1-r_{li}=1}\}] & 1 \end{matrix} \quad (2.29)$$

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. МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ ЯК ІНСТРУМЕНТ ПОПЕРЕДЖЕННЯ КІБЕРШАХРАЙСТВ У БАНКАХ

3.1 Моделювання портретів потенційної жертви та шахрая

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. [55]

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.[56]

Так, розподіл шахрайств від першої сторони за видами фінансових продуктів в Великій Британії за 2015-2018 роки представлений на рисунку 3.1. [57]

Шахрайства від першої сторони найбільш ймовірно припадають на шахрайства з поточними банківськими рахунками (Current Accounts) та іпотеку (Mortgages) (рис. 3.1). 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. [58]

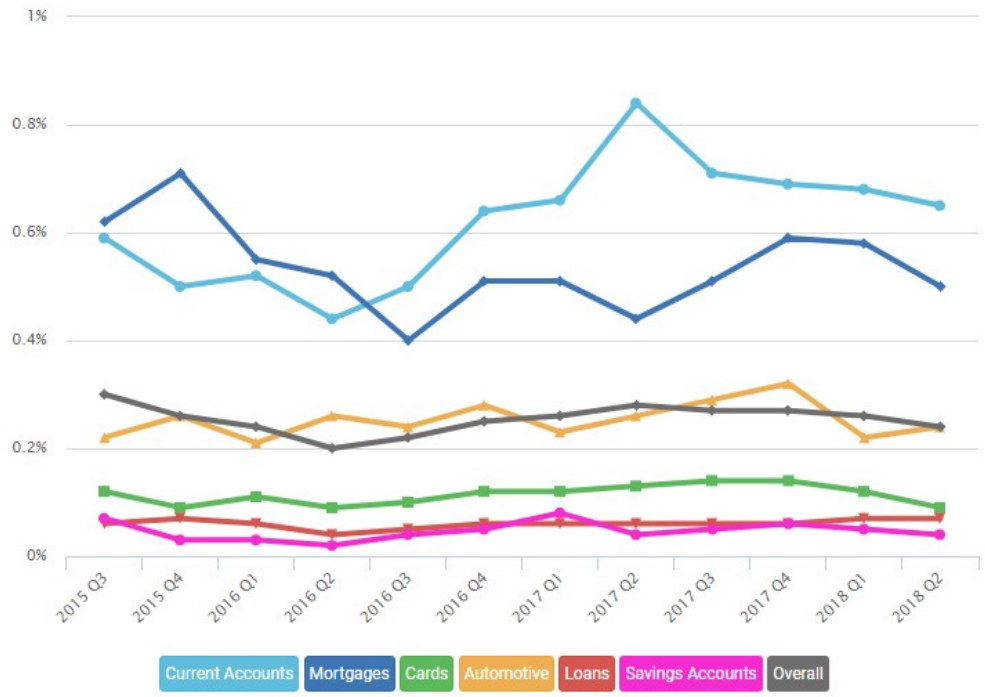


Рисунок 3.1 – Розподіл шахрайств від першої сторони за видами фінансових продуктів в Великій Британії за 2015-2018 роки

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. 3.2). 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.

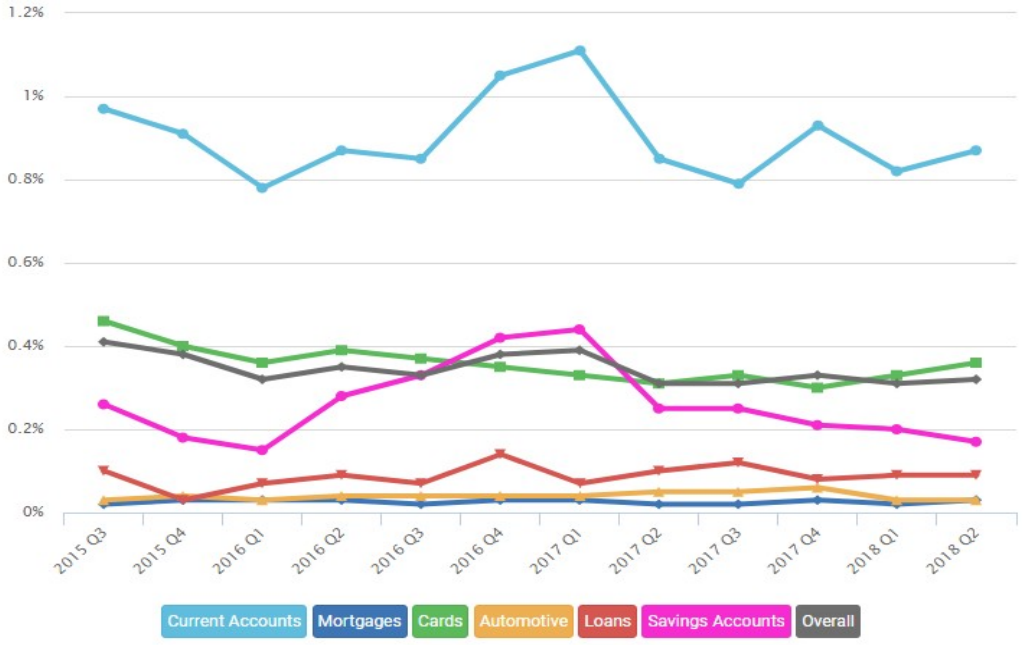


Рисунок 3.2 – Розподіл шахрайств від третьої сторони за видами фінансових продуктів у Великій Британії за 2015-2018 роки

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 3.3. 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. 3.3) 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.

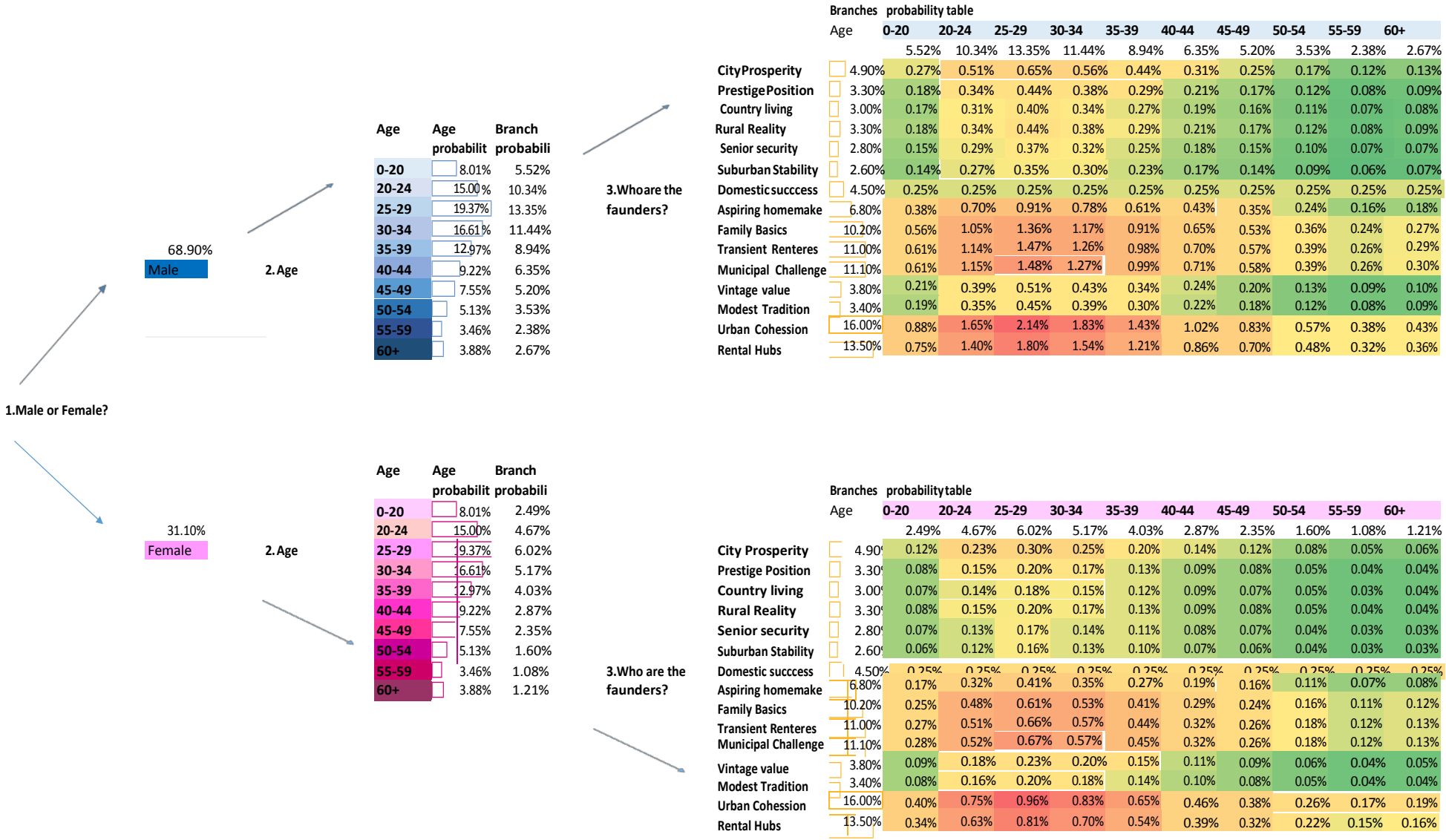


Рисунок 3.3 – Модель портрету потенційного шахрая від першої сторони за ознаками статі, віку та соціальної групи [59]

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 3.4. Отримана модель вказує на те, що найбільше від сторонніх шахраїв потерпають чоловіки в віці 25 - 44 років, які відносяться до соціальної групи «Rental Hubs» – переважно молоді, одинокі люди, та люди середнього віку, які живуть у міських поселеннях та орендують свої будинки, перебуваючи на ранній або середній стадіях своєї кар'єри або продовжують навчання.

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

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

Рисунок 3.4 – Модель портрету потенційної жертви шахрайства від третьої сторони за ознаками статі, віку та соціальної групи [59]

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.

3.2 Застосування інтелектуального аналізу даних для прогнозування 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 [60]:

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. 3.5).

Рисунок 3.5 – 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” [66].

В результаті побудови логіт-регресії отримано результати оцінки, представлені на рисунку 3.6. [71]

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 3.6 – 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 3.1):

$$P = \frac{1}{1 + E^{-(-3{,}4+5{,}11X_{3.2}-0{,}89X_5+0{,}87X_6)}} \tag{3.1}$$

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. 3.7). [71]

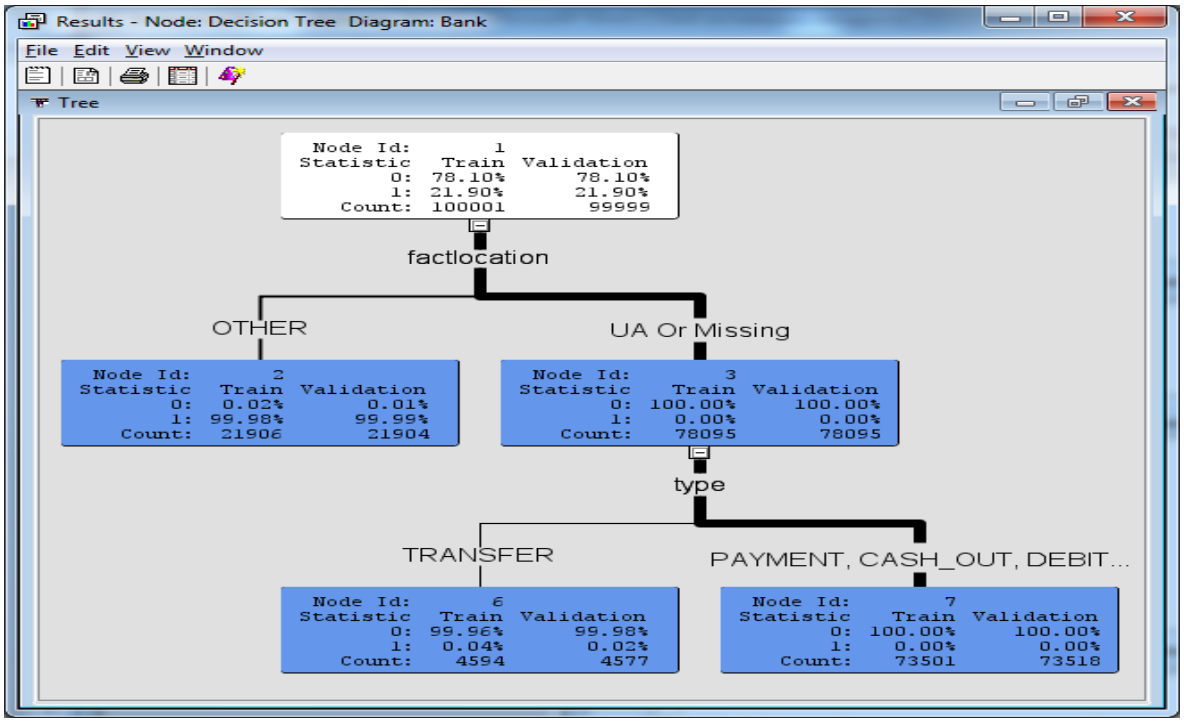


Рисунок 3.7 – Результат побудови дерева рішень

З побудованої діаграми дерева рішень (рис. 3.7) 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. 3.8). [71]

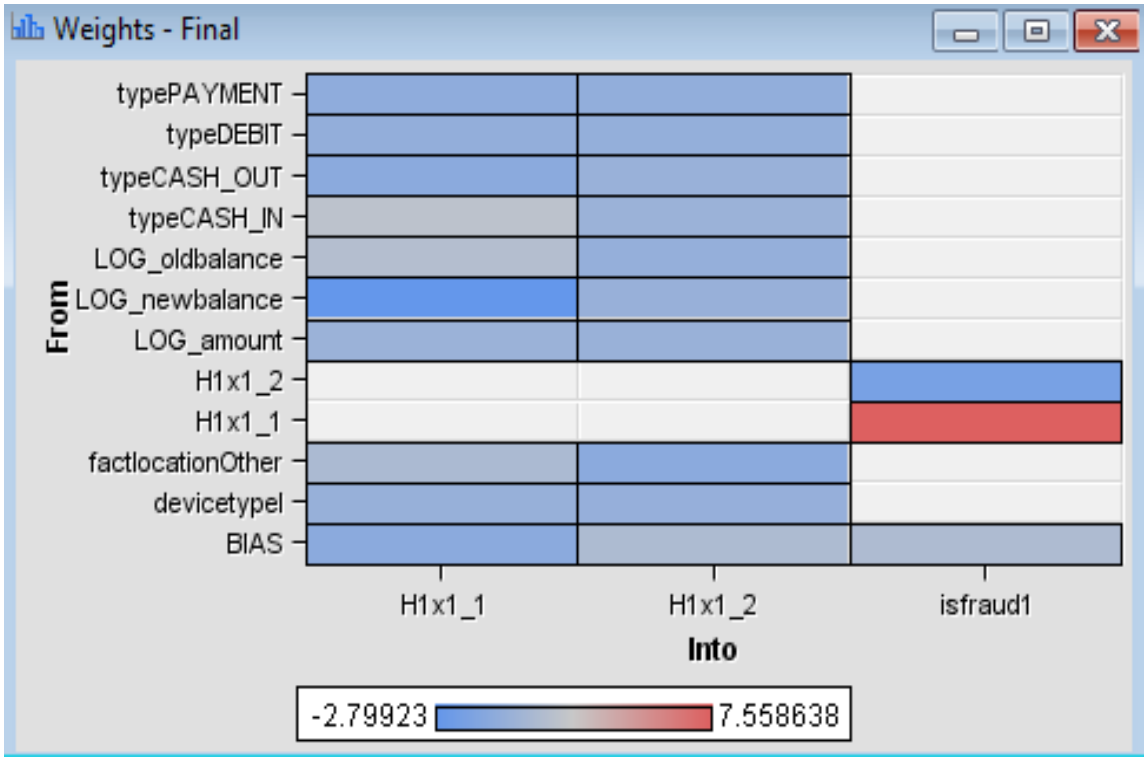


Рисунок 3.8 – Архітектура побудованої нейронної мережі

Отримані вагові коефіцієнти нейронної мережі представлено на рисунку 3.9.

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 3.9 – Вагові коефіцієнти нейронної мережі

Математичну інтерпретацію отриманої нейронної мережі наведено у формулах 3.2–3.4:

$$Y = 1{,}02 + 7{,}56 \cdot H_1 x_1 - 1{,}76 \cdot H_2 x_2; \quad (3.2)$$

$$H_1 = \tanh(-0{,}78 + 0{,}04 \cdot LOGX_1 - 0{,}13 \cdot X_{2.2} + 0{,}87 \cdot X_{3.2} - 2{,}8 \cdot LOGX_5 + 1{,}36 \cdot LOGX_6 + 1{,}78 \cdot X_{7.1} - 0{,}76 \cdot X_{7.2} - 0{,}35 \cdot X_{7.3} - 0{,}58 \cdot X_{7.4}); \quad (3.3)$$

$$H_2 = \tanh(0{,}99 - 0{,}05 \cdot LOGX_1 - 0{,}23 \cdot X_{2.2} - 0{,}78 \cdot X_{3.2} - 0{,}11 \cdot LOGX_5 - 0{,}25 \cdot LOGX_6 + 0{,}05 \cdot X_{7.1} - 0{,}07 \cdot X_{7.2} - 0{,}3 \cdot X_{7.3} - 0{,}4 \cdot X_{7.4}). \quad (3.4)$$

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. 3.1). [71]

Таблиця 3.1 – 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 3.1, 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 3.10 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.

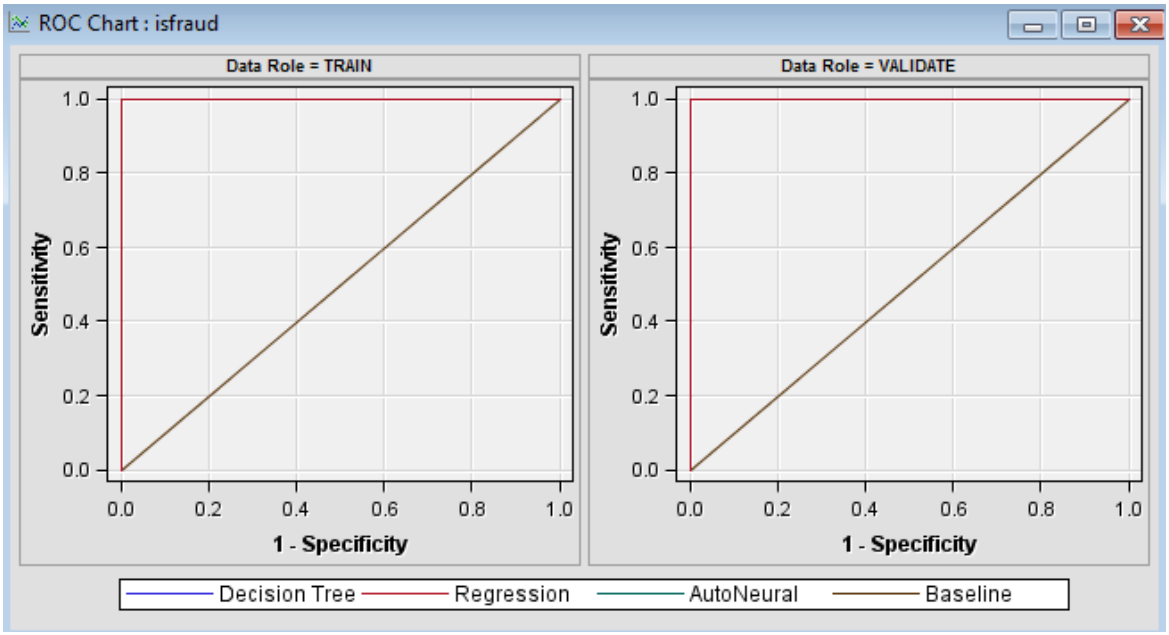


Рисунок 3.10 – ROC-криві дерева рішень, регресії та нейронної мережі

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. 3.2).

Таблиця 3.2 – 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 3.2 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.

3.3 Нечітко-множинна модель оцінки рівня захищеності банку від кібершахрайств

Кібербезпека визначається як стан захищеності окремих об'єктів держави, зокрема банківських установ, від ризику стороннього кібервпливу, за якого забезпечується їх сталий розвиток, а також своєчасне виявлення, запобігання й нейтролізація реальних і потенційних викликів, кібернетичних втручань і загроз особистим, корпоративним і/або національним інтересам [72]. Актуальною задачею, що характеризується вираженою практичною спрямованістю, є вибір банківської установи (наприклад, відділення банку) для проведення аудиту її системи кібербезпеки, в результаті якого формулюються конкретні пропозиції по покращенню існуючої системи кібербезпеки. Для вирішення цієї задачі нами розроблена нечітко-множинна модель оцінки рівня захищеності банку від кібершахрайств, яка може працювати як з кількісними показниками, так і з анкетними даними. Використання цієї моделі значно спрощує процес вибору банківської установи для проведення повноцінного аудиту системи кібербезпеки.

Модель оцінки рівня захищеності банку від кібершахрайств може бути представлена у вигляді деревоподібного зваженого графа (рис.3.11), що описує ієрархічну структуру факторів, які впливають на рівень захищеності банку.

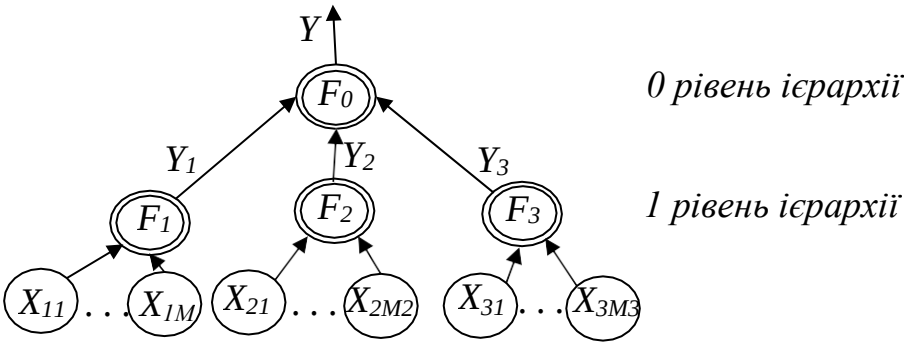


Рисунок 3.11 – Ієрархічна структура моделі

Спочатку в результаті агрегування вхідних факторів (X_{ij}) визначаються оцінки рівня захищеності банку від кібершахрайств в розрізі наступних критеріїв [73]: захищеність інформаційно-телекомунікаційної системи банку (Y_1), надійність персоналу банку (Y_2), якість інформації для прийняття рішень (Y_3). Потім визначається рівень захищеності банку в цілому. Елементи графа інтерпретуються наступним чином: Y – загальний рівень захищеності банку від кібершахрайств; дуги, що виходять із вершин F_i, – вищезазначені критерії; X_{ij} – вхідні фактори, $i = \overline{1,n};\ n = 3;\ j = \overline{1, M_i}$, де n – кількість критеріїв, M_i – кількість факторів, що пов'язані з i-тим критерієм через вершину F_i, $i = \overline{1,3}$.

На нашу думку, до факторів, що визначають захищеність інформаційно-телекомунікаційної системи банку, відносяться:

– якість систем життєзабезпечення даних департаментів банку;

– якість технологічних процесів передачі, одержання, використання, розповсюдження і зберігання інформації;

– якість засобів забезпечення технічного захисту інформації;

– якість засобів забезпечення діяльності банку, які мають вихід за межі контрольованої території;

– якість експлуатаційної документації, яка забезпечує інформаційну діяльність.

До факторів, що визначають надійність персоналу банку, відносяться:

– плинність працівників банку;

– готовність працівників банку до нововведень;

– підготовленість персоналу банку до розпізнавання шахрайств;

– досвід роботи працівників банку;

– компетентність працівників банку;

– мотивація працівників банку.

До факторів, що визначають якість інформації для прийняття рішень, відносяться:

– якість політики класифікації інформаційних активів;

– якість політики безпеки персоналу;

– якість політики захисту від шкідливого та мобільного коду;

– якість політики використання корпоративної електронної пошти;

– якість політики управління інцидентами інформаційної безпеки.

Оцінки зазначених вище вхідних факторів визначаються шляхом усереднення анкетних даних, тому анкети повинні містити кількісну (бальну) шкалу оцінювання. Можливі варіанти таких шкал наведені в [74]. Наприклад, в класичній голандській системі оцінювання оцінки факторів знаходяться в межах від 0 до 10: 1-4 – низька оцінка; 5-7 – середня оцінка; 8-10 – висока оцінка.

Обрана кількісна шкала оцінювання зіставляється з її лінгвістичним описом (нечіткою терм-множиною), як це показано, наприклад, в [75]. Приклад зіставлення кількісної шкали оцінювання U з нечіткою терм-множиною наведений в табл. 3.3.

Таблиця 3.3 – Шкала оцінювання

U	0,1	0,3	0,5	0,7	0,9
Нечіткий терм T лінгвістич-ної змінної L	Низький	Нижче середнього	Середній	Вище середнього	Високий

Трапецієподібні функції належності нечіткої терм-множини лінгвістичної змінної L, представленої в таблиці 3.3, наведені на рисунку 3.12.

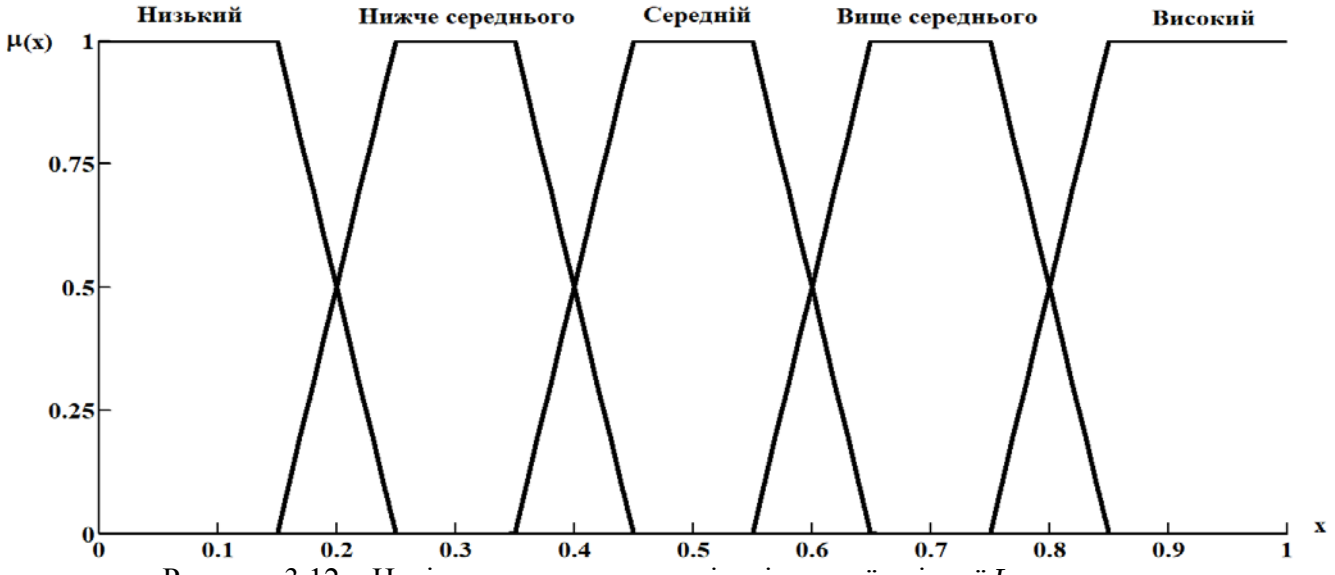


Рисунок 3.12 – Нечітка терм-множина лінгвістичної змінної L

Абсциси нейтральних точок на 01-носії (рис. 3.12) мають координати (0.2, 0.4, 0.6, 0.8). Наведена на рисунку 3.12 шкала оцінювання на трапецієподібних функціях належності нечітких термів є «сірою» шкалою Поспєлова, і лінгвістичний аналіз на її основі є несуперечливим. Наприклад, інтервал [0.15, 0.25] – це зона невизначеності в оцінці, яка може бути описана похилим ребром трапецієподібного нечіткого числа. Перевагою такого опису є його задоволення вимогам «сірої» шкали Поспєлова: наявність нейтральної точки посеред інтервалу невизначеності і монотонне спадання експертної впевненості в класифікації по мірі зростання *X*. Таким вимогам задовольняють не тільки трапецієподібні нечіткі числа. Однак вони відображають факт, що якщо немає ніяких додаткових міркувань про характер убування експертної впевненості, то лінійний вид відповідної функції належності є найбільш раціональним.

Рівень захищеності банку від кібершахрайств опишемо нечіткою ієрархічною моделлю:

$$Y=<G, L, F>, \tag{3.5}$$

де *G* – зважений ієрархічний граф, показаний на рисунку 3.11; *L* – терм-множина нечітких оцінок вхідних факторів X_{ij}; *F* – функція згортки нечітких оцінок у відповідних вершинах графа (F_i). Ваги дуг графа відповідають ступеню впливу відповідних чинників на результуючу оцінку.

Рівень захищеності банку від кібершахрайств у цілому представимо у вигляді лінгвістичної змінної $L^{(Y)}$ з множиною можливих значень (терм-множиною):

$$L^{(Y)} = \left\{ T_1^{(Y)}, \ ...,T_k^{(Y)},...,T_s^{(Y)} \right\}, \tag{3.6}$$

де *s* – кількість нечітких термів лінгвістичної змінної $L^{(Y)}$.

Рівень захищеності банку від кібершахрайств у розрізі окремих критеріїв Y_i ($i = \overline{1,3}$) представимо у вигляді лінгвістичних змінних $L^{(i)}$ з множиною можливих значень:

$$L^{(i)} = \left\{ T_1^{(i)},...,T_k^{(i)},...,T_s^{(i)} \right\}, \tag{3.7}$$

де *s* – кількість нечітких термів лінгвістичної змінної $L^{(i)}$, $i = \overline{1,3}$.

Кожен вхідний фактор X_{ij} також представимо у вигляді лінгвістичної змінної з множиною можливих значень:

$$L^{(ij)} = \left\{ T_1^{(ij)},...,T_k^{(ij)},...,T_s^{(ij)} \right\}, \ i = \overline{1,3}; \quad j = \overline{1,M_i}, \tag{3.8}$$

де *s* – кількість нечітких термів лінгвістичної змінної $L^{(ij)}$.

З метою спрощення моделі (1)-(4) сформуємо одну терм-множину для всіх лінгвістичних змінних $L^{(Y)}$, $L^{(i)}$, $L^{(ij)}$:

$T_1^{(Y)}, T_1^{(i)}, T_1^{(ij)}$ – «низький рівень»;

$T_2^{(Y)}, T_2^{(i)}, T_2^{(ij)}$ – «середній рівень»;

$T_3^{(Y)}, T_3^{(i)}, T_3^{(ij)}$ – «високий рівень».

Кожному нечіткому терму (“низький” (*k=1*), “середній” (*k=2*), “високий” (*k=3*)) лінгвістичної змінної $L^{(ij)}$ поставимо у відповідність трапецієподібну функцію належності $\mu_k(X_{ij})$ з параметрами $\underline{t_k^{(ij)}};\overline{t_k^{(ij)}};a_k^{(ij)};b_k^{(ij)}$ ($k=\overline{1,3}$):

$$\mu_k\left(X_{ij}\right)=\begin{cases} 0, \textit{якщо } X_{ij} \le \underline{t_k^{(ij)}} - a_k^{(ij)} \textit{ або } X_{ij} \ge \overline{t_k^{(ij)}} + b_k^{(ij)} \\ \dfrac{X_{ij} - \left(\underline{t_k^{(ij)}} - a_k^{(ij)}\right)}{a_k^{(ij)}}, \quad \textit{якщо} \quad \underline{t_k^{(ij)}} - a_k^{(ij)} \le X_{ij} \le \underline{t_k^{(ij)}} \\ 1, \quad \textit{якщо} \quad \underline{t_k^{(ij)}} \le \overline{t_k^{(ij)}} \\ \dfrac{\left(\overline{t_k^{(ij)}} + b_k^{(ij)}\right) - X_{ij}}{b_k^{(ij)}}, \textit{якщо} \quad \overline{t_k^{(ij)}} \le X_{ij} \le \overline{t_k^{(ij)}} + b_k^{(ij)} \end{cases} \tag{3.9}$$

Нечітка терм-множина лінгвістичної змінної $L^{(ij)}$ наведена на рисунку 3.13.

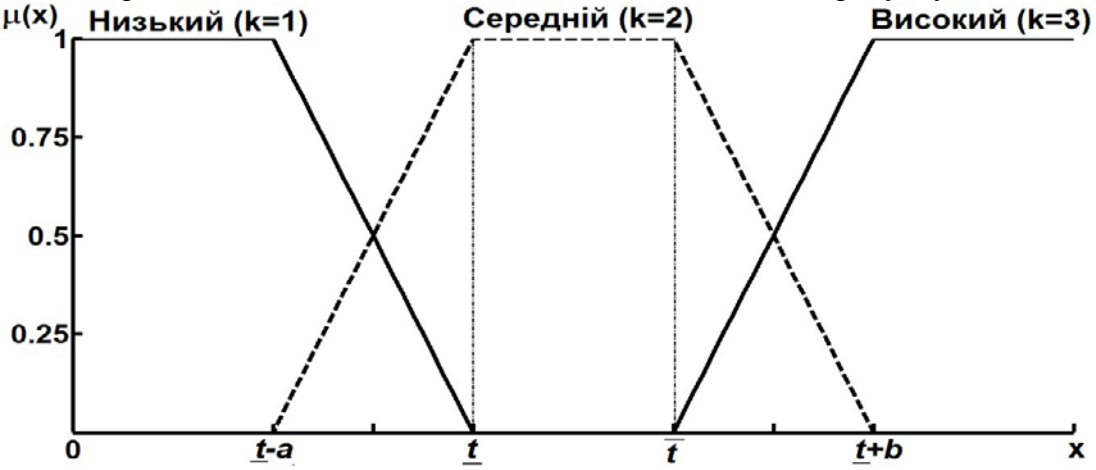


Рисунок 3.13 – Нечітка терм-множина лінгвістичної змінної $L^{(ij)}$

У загальному випадку кількісні значення вхідних факторів X_{ij} (вісь абсцис на рисунку 3.13) можуть мати різну розмірність. Їх можна агрегувати лише за умови нормування. Тобто необхідно привести параметри $\underline{t_k^{(ij)}};\overline{t_k^{(ij)}};a_k^{(ij)};b_k^{(ij)}$ ($k=\overline{1,s}$) трапецієподібних функцій належності нечітких термів лінгвістичної змінної $L^{(ij)}$ до інтервалу [0,1], як це показано, наприклад, на рис. 3.12.

Якщо вхідні фактори X_{ij} є стимуляторами, тобто їх зростання покращує значення агрегованого показника, то можна використати наступну процедуру природньої нормалізації для $L^{(ij)}=\left\{T_1^{(ij)},\ ...,T_k^{(ij)},...,T_s^{(ij)}\right\}$:

$$t_{\underline{norm\,k}}^{(ij)} = \frac{\underline{t_k^{(ij)}} - \left(\underline{t_1^{(ij)}} - a_1^{(ij)}\right)}{\left(\overline{t^{(ij)}} + b^{(ij)}\right) - \left(\underline{t^{(ij)}} - a^{(ij)}\right)},\ \overline{t_{norm\,k}^{(ij)}} = \frac{\overline{t_k^{(ij)}} - \left(\underline{t_1^{(ij)}} - a_1^{(ij)}\right)}{\left(\overline{t_s^{(ij)}} + b_s^{(ij)}\right) - \left(\underline{t_1^{(ij)}} - a_1^{(ij)}\right)}, \tag{3.10}$$

$$a_{norm}^{(ij)} = \frac{\underline{k}}{\underline{a}^{(ij)}}, b_{norm\,k} = \frac{\underline{k}}{b^{(ij)}}. \quad \underline{\quad} \qquad \underline{\quad}$$

$$\left(\overset{s}{t}{}^{(ij)} + \overset{s}{b}{}^{(ij)}\right) - \left(\overset{\underline{1}}{t}{}^{(ij)} - \overset{1}{a}{}^{(ij)}\right) \qquad \left(\overset{s}{t}{}^{(ij)} + \overset{s}{b}{}^{(ij)}\right) - \left(\overset{\underline{1}}{t}{}^{(ij)} - \overset{1}{a}{}^{(ij)}\right)$$

Якщо вхідні фактори X_{ij} є дестимуляторами, тобто їх зростання погіршує значення агрегованого показника, то можна використати наступну процедуру нормалізації Севіджа:

$$\underline{t}_{norm\,k}^{(ij)} = \frac{\left(\overline{t_s^{(ij)}} + b_s^{(ij)}\right) - \underline{t_k^{(ij)}}}{\left(\overline{t_s^{(ij)}} + b_s^{(ij)}\right) - \left(\underline{t_1^{(ij)}} - a_1^{(ij)}\right)}, \overline{t}_{norm\,k}^{(ij)} = \frac{\left(\overline{t_s^{(ij)}} + b_s^{(ij)}\right) - \overline{t_k^{(ij)}}}{\left(\overline{t_s^{(ij)}} + b_s^{(ij)}\right) - \left(\underline{t_1^{(ij)}} - a_1^{(ij)}\right)}, \quad (3.11)$$

$$a_{norm}^{(ij)} = \frac{\underline{k}}{\underline{a}^{(ij)}}, b_{norm\,k} = \frac{\underline{k}}{b^{(ij)}}. \quad \underline{\quad} \qquad \underline{\quad}$$

$$\left(\overset{s}{t}{}^{(ij)} + \overset{s}{b}{}^{(ij)}\right) - \left(\overset{\underline{1}}{t}{}^{(ij)} - \overset{1}{a}{}^{(ij)}\right) \qquad \left(\overset{s}{t}{}^{(ij)} + \overset{s}{b}{}^{(ij)}\right) - \left(\overset{\underline{1}}{t}{}^{(ij)} - \overset{1}{a}{}^{(ij)}\right)$$

В результаті лінгвістична змінна $L^{(ij)} = \left\{ T_1^{(ij)}, \ldots, T_k^{(ij)}, \ldots, T_s^{(ij)} \right\}$ набуває нормованого вигляду $L_{norm}^{(ij)} = \left\{ T_{norm1}^{(ij)}, \ldots, T_{norm\,k}^{(ij)}, \ldots, T_{norm\,s}^{(ij)} \right\}$. Для кількісних значень самих вхідних факторів X_{ij} теж виконується процедура природньої нормалізації або нормалізації Севіджа.

Для того, щоб оцінити рівень захищеності банку від кібершахрайств з використанням ієрархічної структури, представленої на рисунку 3.11, необхідно для кожного рівня ієрархії провести агрегування значень лінгвістичних змінних з пересуванням за напрямом дуг ієрархічного графа від нижніх рівнів ієрархії до верхніх.

В кожній вершині графа F_i ($i = \overline{1,3}$) виконується згортка значень пов'язаних з нею нормованих вхідних факторів X_{ij} , представлених відповідними нормованими лінгвістичними змінними $L^{(ij)}$ – нечіткими термами $T_k^{(ij)}$, $j = \overline{1, M_i}$, $k = \overline{1,s}$.

В якості функції згортки використовуємо OWA-оператор Ягера (OWA – Ordered Weighted Averaging):

$$L_{norm}^{(i)} = \sum_{j=1}^{M_i} \left(L_{norm}^{(ij)} \times \omega^{(ij)} \right) = \sum_{j=1}^{M_i} \left(\left\{ T_{norm1}^{(ij)}, \ldots, T_{norm\,k}^{(ij)}, \ldots, T_{norm\,s}^{(ij)} \right\} \times \omega^{(ij)} \right) =$$

$$= \sum_{j=1} \left\{ T_{norm\,1}^{(ij)} \times \omega^{(ij)}, \ldots, T_{norm\,k}^{(ij)} \times \omega^{(ij)}, \ldots T_{norm\,s}^{(ij)} \times \omega^{(ij)} \right\}, \quad (3.12)$$

де $\omega^{(ij)}$ – рівень значущості вхідного фактору X_{ij}, що через вершину F_i (функцію згортки) пов'язаний з критерієм Y_i. $\omega^{(ij)}$ описується трапецієподібною функцією належності з параметрами $\underline{t}^{(ij)}; \overline{t^{(ij)}}; 0; 0$, де ваговий коефіцієнт $\underline{t}^{(ij)} = \overline{t^{(ij)}} = k_{ij}$ В результаті отримуємо нечітку оцінку рівня захищеності банку від кібершахрайств в розрізі критерія Y_i.

Оскільки функції належності нечітких термів лінгвістичних змінних $L_{norm}^{(ij)} = \left\{ T_{norm1}^{(ij)}, \ldots, T_{norm\,k}^{(ij)}, \ldots, T_{norm\,s}^{(ij)} \right\}$ мають трапецієподібну форму, то і терми лінгвістичної змінної $L_{norm}^{(i)}$ теж мають трапецієподібну форму.

Для визначення рівня захищеності банку від кібершахрайств в цілому виконуємо згортку отриманих вище нечітких оцінок $L_{norm}^{(i)}$:

$$L_{norm}^{(Y)} = \sum_{i=1}^{3} \left(L_{norm}^{(i)} \times \omega^{(i)} \right), \tag{3.13}$$

де $\omega^{(i)}$ – рівень значущості критерію Y_i, що через вершину F_0 (функцію згортки) пов'язаний з рівнем захищеності банку від кібершахрайств в цілому Y. $\omega^{(i)}$ описується трапецієподібною функцією належності з параметрами $\underline{t^{(i)}}; \overline{t^{(i)}}; 0; 0$, де ваговий коефіцієнт $\underline{t^{(i)}} = \overline{t^{(i)}} = k_i$. В результаті отримуємо нечітку оцінку рівня захищеності банку від кібершахрайств в цілому.

Вагові коефіцієнти k_{ij} та k_i в функціях згортки (8)-(9) вершин ієрархічного дерева пропонується розраховувати за схемою Фішберна [76], яка використовується для визначення величини вагових коефіцієнтів, представлених раціональними дробами, за умови, що визначені відношення пріоритетності між критеріями. Знаменниками вказаних раціональних дробів є сума арифметичної прогресії m (кількість критеріїв) перших членів натурального ряду з кроком 1, а чисельниками – спадаючі на 1 елементи натурального ряду від до m до 1.

Наприклад, при m=3 та наявності відношення пріоритетності типу $Y_1 \succ Y_2 \succ Y_3$ вагові коефіцієнти, визначені за схемою Фішберна дорівнюватимуть $k_1 = \frac{3}{6}$, $k_2 = \frac{2}{6}$, $k_3 = \frac{1}{6}$. Тобто, відповідно до схеми Фішберна перевага виражається в спаданні на одиницю чисельника раціонального дробу вагового коефіцієнту критерію, що має слабкіший пріоритет. Зауважимо, що визначення величини вагових коефіцієнтів за схемою Фішберна відповідає максимуму ентропії наявної інформаційної невизначеності щодо вагових коефіцієнтів.

В загальному випадку, коли в системі вагових коефіцієнтів критеріїв присутні як відношення переваги, так і відношення байдужості, визначення вагових коефіцієнтів k_i критеріїв Y_i відповідно до схеми Фішберна здійснюється за наступними рекурентними співвідношеннями:

$$r_{i-1} = \begin{cases} r_i, \text{ якщо } Y_{i-1} \approx Y_i, \\ r_i + 1, \text{ якщо } Y_{i-1} \succ Y_i, \end{cases} \quad r_m = 1, \quad i = m, \ldots, 2. \tag{3.14}$$

$$K = \sum_{i=1}^{m} r_i; \quad k_i = \frac{r_i}{K},$$

де: r_i – ранг критерію Y_i; m – кількість критеріїв; k_i – ваговий коефіцієнт критерію Y_i.

Для ілюстрації в таблиці 3.4 представлені величини вагових коефіцієнтів k_i, розрахованих за схемою Фішберна для різних відношень пріоритетності критеріїв Y_i.

Таблиця 3.4 – Величини вагових коефіцієнтів, розрахованих за схемою Фішберна

Відношення пріоритетності	k_1	k_2	k_3
$Y_1 \approx Y_2 \approx Y_3$	1/3	1/3	1/3
Y_1 f $Y_2 \approx Y_3$	2/4	1/4	1/4
$Y_1 \approx Y_2$ f Y_3	2/5	2/5	1/5
Y_1 f Y_2 f Y_3	3/6	2/6	1/6

Отримані в результаті згортки значення лінгвістичних змінних у вигляді терм-множини (рис. 3.13) розпізнаються за допомогою операцій нечіткої фільтрації за показником можливості [77].

Нехай для досліджуваного банку нечіткі терм-множини нормованих лінгвістичних змінних критеріїв $L_{norm}^{(i)}$ мають вигляд, поданий на рисунку 3.14.

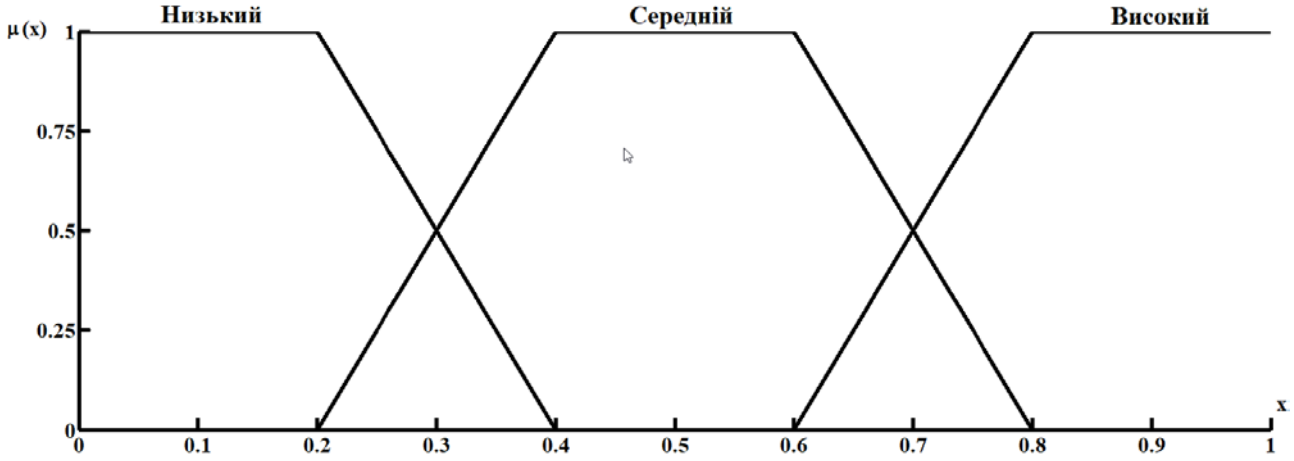


Рисунок 3.14 – Нечітка терм-множина нормованої лінгвістичної змінної $L_{norm}^{(i)}$

Абсциси нейтральних точок на 01-носії (рис. 3.14) мають координати (0.3, 0.7).

Нехай нормоване значення критерію захищеності інформаційно-телекомунікаційної системи банку $L_{norm}^{(1)} = 0{,}5$; критерію надійності персоналу банку $L_{norm}^{(2)} = 0{,}9$; критерію якості інформації для прийняття рішень $L_{norm}^{(3)} = 0{,}7$. Виконаємо згортку критеріїв $L_{norm}^{(i)}$ в комплексний показник $L_{norm}^{(Y)}$ з рівнями значущості $k_1 = 0{,}5;\quad k_2 = 0{,}3;\quad k_3 = 0{,}2.$ Нечітка терм-множина нормованої лінгвістичної змінної $L_{norm}^{(Y)}$ наведена на рисунку 3.15.

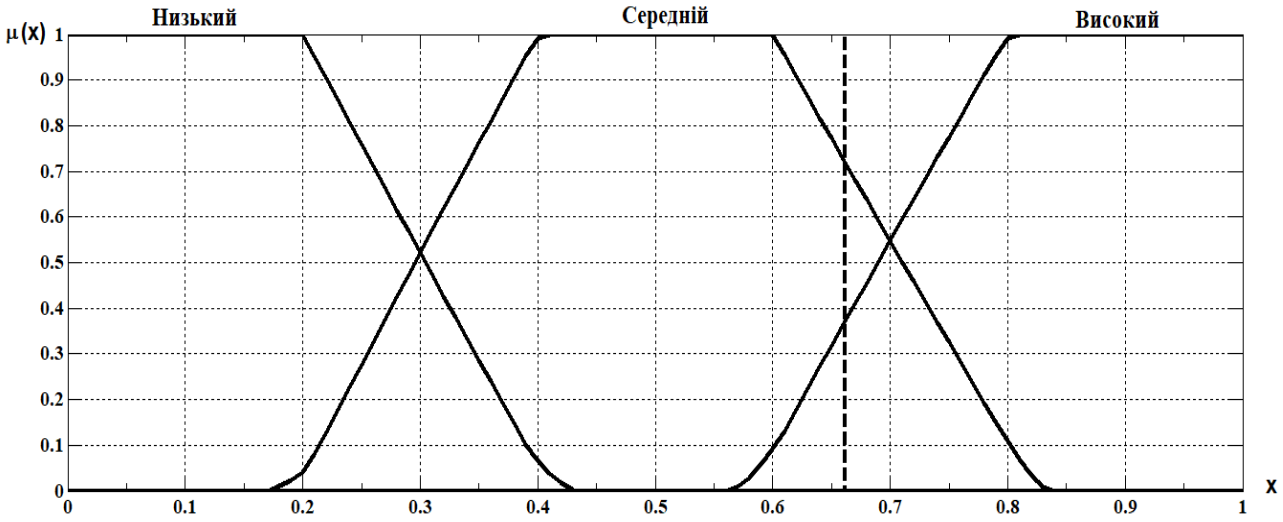


Рисунок 3.15 – Нечітка терм-множина нормованої лінгвістичної змінної $L_{norm}^{(Y)}$

Нормоване значення комплексного показника дорівнює 0,66. Таким чином, з достовірністю 0,7 оцінка рівня захищеності банку від кібершахрайств знаходиться в інтервалі середніх значень та є задовільною.

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

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

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

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

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

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

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

Інноваційний розвиток економіки будь-якої країни залежить від спрямованості суспільства до інформаційного простору. На сьогодні головним напрямком інновацій у бізнесі є передача комерційної діяльності в Інтернет-просторі. Щороку від 30% до 70% бізнесу в будь-якій країні (незалежно від рівня розвитку) переходить в онлайн сферу. Тобто компанії все частіше використовують системи електронної комерції для ведення бізнесу.

Початок Інтернет економіки може бути пов’язаний з проривом під час появи системи Всесвітньої павутини в середині 1990-х. Сьогодні для опису економічних відносин в Інтернеті використовується поняття «електронна комерція», яке є частиною Інтернет економіки. Таким чином, Організація економічного співробітництва та розвитку дає таке визначення цього терміна (у широкому розумінні): будь-яка форма ділових відносин, де взаємодія між суб'єктами відбувається за допомогою Інтернет-технологій [78].

Отже, електронну комерцію можна визначити як відносини, спрямовані на отримання прибутку, здійснювані дистанційно за допомогою інформаційно-телекомунікаційних систем, внаслідок чого учасники мають права та обов'язки майнового характеру [79].

Загалом електронна комерція поділяється на:

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

Електронний банкінг – це технологія віддаленого банкінгу, яка дає можливість отримувати банківські послуги через Інтернет [80]. Для підключення клієнта до системи Інтернет-банкінгу достатньо мати доступ до глобальної мережі, встановленої на програмі браузера комп'ютера, укласти договір з банком, отримати набір паролів або спеціальних пристроїв для входу та операцій, перейти на захищену сторінку електронного банкінгу, підпишіться та підключіться до системи.

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

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

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

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

Кібератаки проникли абсолютно у всі сфери бізнесу. На рисунку 3.16 показано 5 напрямків бізнесу, які понесли найбільші витрати через кібершахрайства у серпні 2018 року.

З рисунку 3.16 можна побачити, що найбільш збитковими кібератаки були для фінансового сектору. У той же час, близько 90% нападів припадає на банківський сектор. Особливо активно шахрайства проводяться у сфері електронного банкінгу.

Найпоширенішим видом шахрайства в секторі електронного банкінгу є фішинг та його підвиди (рис. 3.17).

Рисунок 3.16 – Середньорічні витрати, спричинені глобальною кіберзлочинністю станом на серпень 2018 року, за галузями (у млн. дол. США) [82]

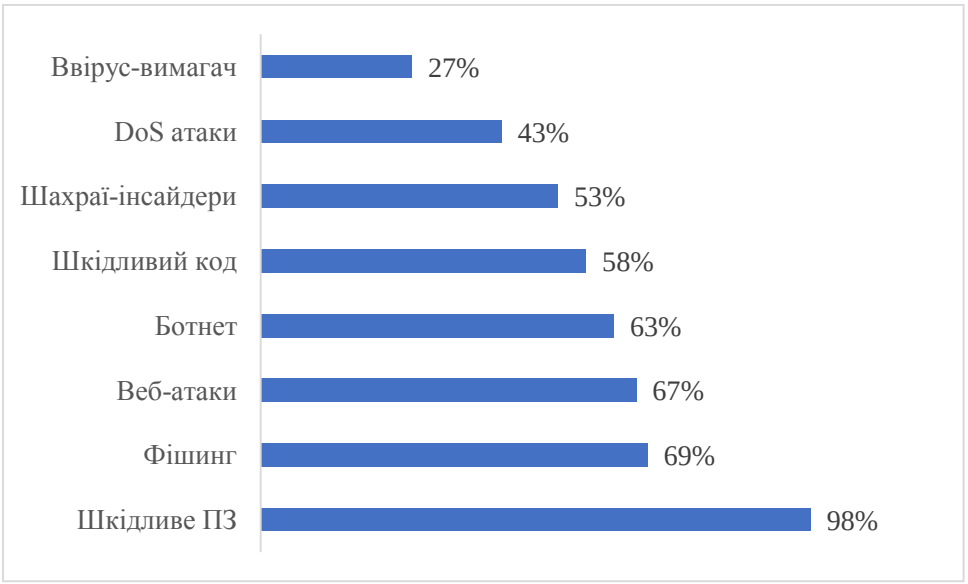


Рисунок 3.17 – Типи кібератак, які зазнавали компанії у всьому світі станом на серпень 2018 року [82]

Як правило, фішинг можна визначити як масштабований акт обману, за допомогою якого оманливість використовується для отримання інформації від цілі [81].

Точніше, фішинг – це форма соціальної інженерії, в якій зловмисник, також відомий як фішер, намагається шахрайським шляхом отримати конфіденційні дані законних користувачів шляхом автоматичної імітації електронних комунікацій або телефонних дзвінків від надійних або громадських організацій [83].

Загалом є два основних принципи фішингу:

– на мобільний телефон, іноді навіть не прив’язаний до рахунку, дзвонить працівник банку або навіть його служба безпеки. Клієнту повідомляють про сумнівні рухи на картці і просять повідомити CVV-код підтвердження платіжної картки. Ніколи не слід нічого повідомляти, якщо дзвінок не робив сам клієнт на номер служби підтримки, будь-яка

інформація може бути використана для крадіжки. Краще перервати дзвінок і зателефонувати самому своєму менеджеру банку;

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

Повна фішинг-атака включає три ролі фішерів. По-перше, фішери-поштарі розсилають велику кількість шахрайських електронних листів (як правило, через ботнети), які направляють користувачів на шахрайські веб-сайти. По-друге, фішери-колектори встановлюють шахрайські веб-сайти (зазвичай розміщуються на компрометованих машинах), які активно спонукають користувачів до надання конфіденційної інформації. Нарешті, фішери-касири використовують конфіденційну інформацію для заволодіння коштами [84]. Потік інформації показаний на рисунку 3.18.

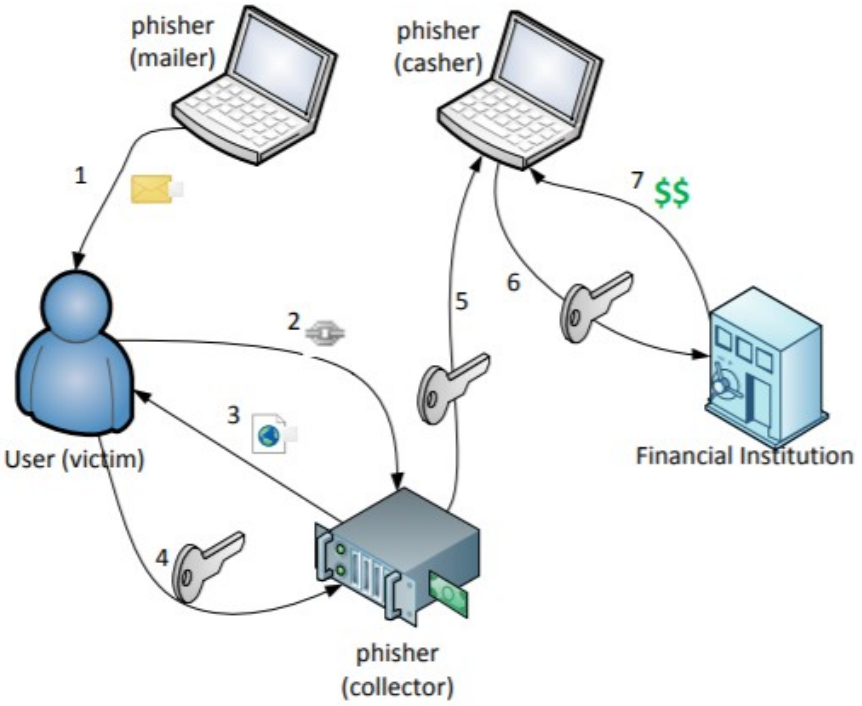


Рисунок 3.18 – Інформаційний потік при фішингу [84]

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

– атака «людина всередині» – хакери розміщуються між банками та клієнтами, поки клієнти використовують свої банківські рахунки в Інтернеті [85];

– оманлива фішинг-атака – надсилання шахрайських повідомлень електронною поштою [86]. Під час такого типу фішинг-атаки, зловмисник надсилає електронним повідомленням користувачам, маскуючись як один із представників банку [87].

– фармінг – цей спосіб складніший і працює лише з невеликими банками. Фармінг - це тип атаки, призначений для перенаправлення трафіку на підроблений Інтернет-хост. Існують різні методи нападу типу фармінг, серед яких найчастішим є модифікація налаштувань DNS [84]. Таким чином, шахрай «замінює» реальний Інтернет-банк на той

самий візуально, але підроблений, де клієнт вносить свої дані, а шахрай, відповідно, отримує всі необхідні персональні дані.

– фішинг на основі зловмисного програмного забезпечення – зловмисне програмне забезпечення – це програмне забезпечення, розроблене або з метою заподіяння шкоди обчислювальному пристрою, або для отримання користі від нього на шкоду своєму користувачеві [88]. Зловмисне програмне забезпечення може використовуватися безпосередньо для збору конфіденційної інформації або для допомоги іншим методам фішингу.

– фішинг через PDF докумнти - зловмисник або хакер може використати деякі ключові функції мови програмування PDF, щоб створити новий документ PDF на власну користь та отримати бажану особисту інформацію від потерпілого [84].

Аналіз статистики щодо загальної кількості фішинг-атак у всьому світі показує, що їх кількість поступово збільшується (рис. 3.19).

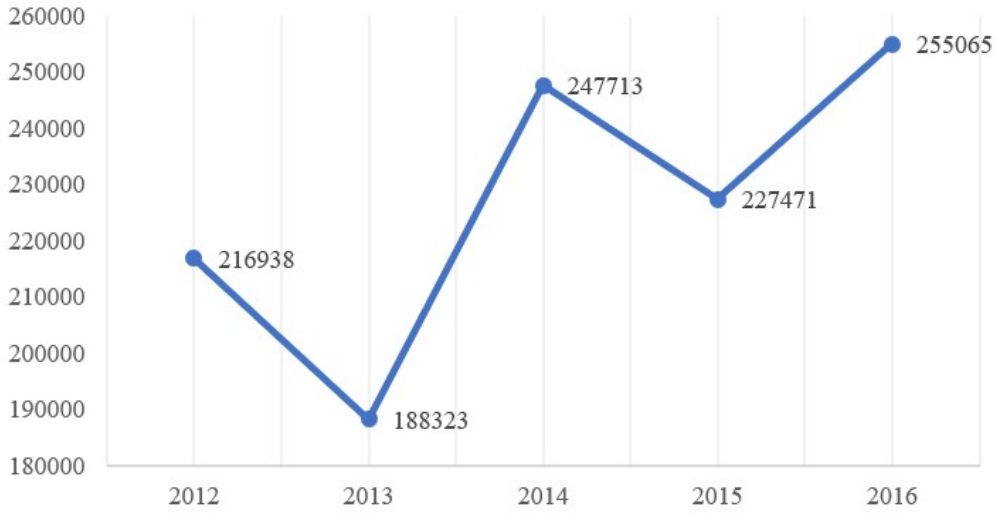


Рисунок 3.19 – Кількість глобальних фішинг-атак з 2012 по 2016 рік у всьому світі [82]

Варто зауважити, що часовий ряд має певну циклічність. Це пов’язано з тим, що створюються певні інструменти протидії існуючим шахрайським атакам. Однак, минаючи інструменти, що виникають, створюються нові типи атак. Таким чином, зменшення кількості фішинг-атак через використання протидіючих інструментів замінюється різким збільшенням їх кількості.

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

Моделювання процесу протидії кібершахрайствам в сфері електронного банкінгу є складним питанням з точки зору збору реальних даних. Відповідна статистика закрита. Крім того, величезна кількість шахрайських схем не виходить на рівень правоохоронних органів. Тому це питання можна дослідити лише в теоретичній формі.

У цьому дослідженні пропонується моделювати процес протидії шахрайству в банку за допомогою моделі економічної динаміки. Отже, використання інструментів для боротьби з кібератаками та появу нових атак можна порівняти з класичною моделлю «хижак-жертва» [85].

$$\begin{cases} x` = (a - c \cdot y)x \\ y` = -(b + d \cdot x)y \end{cases} \quad (3.15)$$

де x - кількість жертв;

y - кількість хижаків;

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

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

Використання моделі Лотки-Вольтерра з логістичним зростанням [90] і моделі Холлінга-Таннера [91] дозволяє запропонувати модель протидії банківським кібератакам:

$$\begin{cases} x` = (a - d \cdot x - b \cdot y)x \\ y` = -c \cdot y + \frac{1}{b} - y \end{cases} \quad (3.16)$$

де x - кількість кібератак на момент часу t;

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

a - коефіцієнт природного збільшення кількості шахрайських атак;

b - коефіцієнт ефективності одного інструменту протидії шахрайським атакам;

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

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

Наступним кроком є пошук особливих точок системи.

На основі символьних розрахунків отримуємо дві особливі точки.

$$(x_1; y_1) = (0; \frac{1}{(1+c)b}) \quad (3.17)$$

$$(x_2; y_2) = (\frac{(1+c)a - 1}{(1+c)d}; \frac{1}{(1+c)b}) \quad (3.18)$$

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

$$J(x, y) = \begin{pmatrix} a - b \cdot y - 2 \cdot d \cdot x & -b \cdot x \\ 0 & -c - 1 \end{pmatrix} \quad (3.19)$$

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

$$tr = a - c - \frac{2 \cdot a + 2 \cdot a \cdot c - 2}{c + 1} - \frac{b}{b + b \cdot c} - 1 \quad (3.20)$$

$$\Delta = a + a \cdot c - 1 \quad (3.21)$$

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

$$D = (c - a + \frac{b}{b + b \cdot c} + \frac{2 \cdot d(a + a \cdot c - 1)}{(1+c)d} + 1)^2 - \quad (3.22)$$
$$-4 \cdot a - 4 \cdot a \cdot c + 4$$

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

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

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

3) дійсні, різні, різних знаків - особлива точка типу сідло;

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

Для досягнення цих типів особливих точок сформуємо обмеження, які повинні бути накладені на співвідношення вхідних параметрів (табл. 3.5).

Таблиця 3.5 – Типи особливої точки залежно від співвідношення вхідних параметрів моделі

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

Для проведення чисельних експериментів та вивчення поведінки запропонованої моделі ми побудуємо імітаційну модель процесу протидії кібератаками в електронному банкінгу, використовуючи інструменти системної динаміки (рис. 3.20).

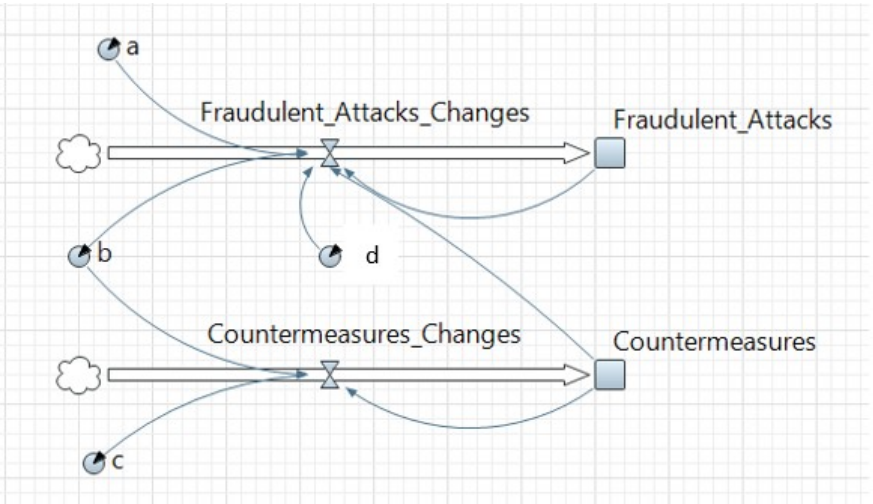


Рисунок 3.20 – Діаграма «потік-дані» для моделі процесу протидії кібершахрайствам в електронному банкінгу

Структура побудованої моделі представлена в табл. 3.6.

Таблиця 3.6 – Опис елементів діаграми

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

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

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

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

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

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

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

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

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

4. РОЗРОБКА КОМПЛЕКСУ АВТОМАТИЗОВАНИХ ПРЕВЕНТИВНИХ ЗАХОДІВ ПОПЕРЕДЖЕННЯ ШАХРАЙСТВ

4.1 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. 4.1).

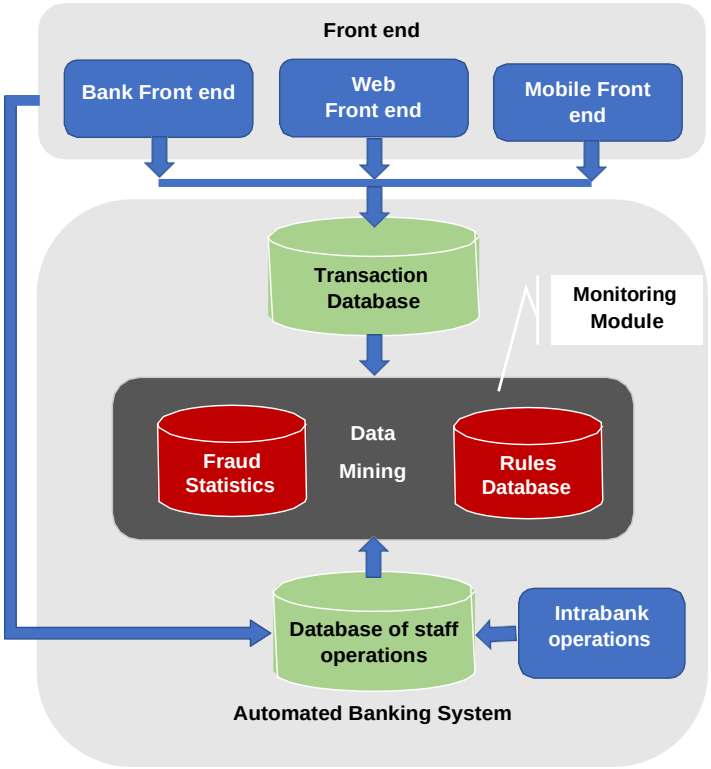


Рисунок 4.1 – Архітектура автоматизованої банківської системи з урахуванням модулю моніторингу

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” (рис. 4.1). 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 (рис. 4.2). [93]

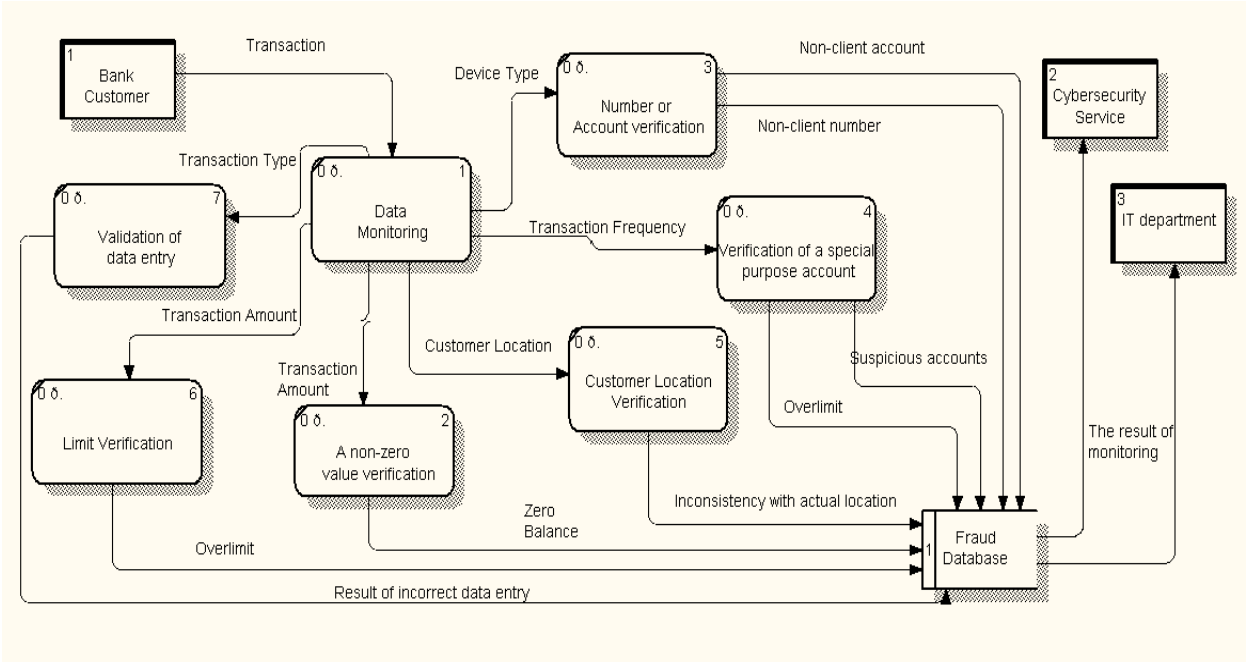


Рисунок 4.2 – Інформаційна модель виявлення ознак шахрайств клієнтів

Модель побудовано у нотації DFD (data flow diagrams) [94], 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 4.2 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 4.2) розроблено схему процесу здійснення операції клієнтом з урахуванням її перевірки на ознаки шахрайства у нотації BPMN 2.0 (Business Process Model and Notation) [95] із використанням програмного забезпечення “Bizagi Modeller” (рис. 4.3).

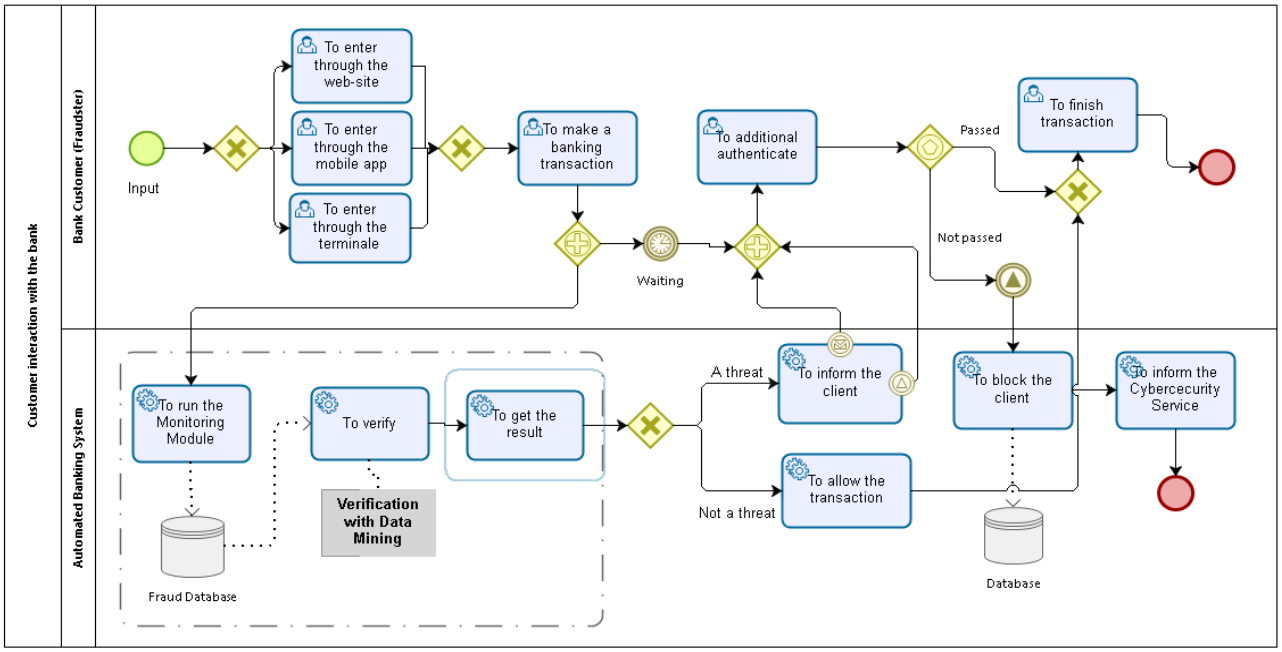


Рисунок 4.3 – Схема процесу здійснення операції клієнтом банку [93]

Процес виглядатиме наступним чином (рисунок 4.3):

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 (рис. 4.4).

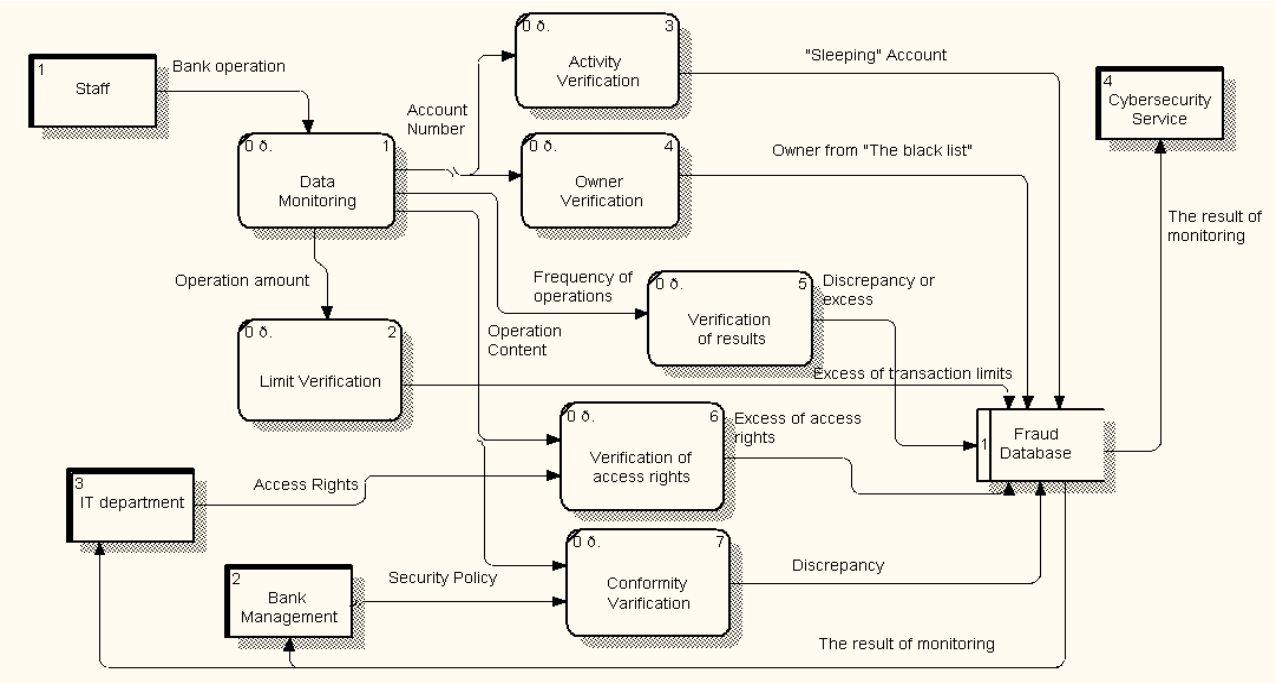


Рисунок 4.4 – Інформаційна модель виявлення ознак шахрайств персоналу банку [93]

Модель, представлена на рисунку 4.4, 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 4.4) розроблено схему процесу здійснення операції персоналом з урахуванням її перевірки на ознаки шахрайства у нотації BPMN 2.0 (рис. 4.5).

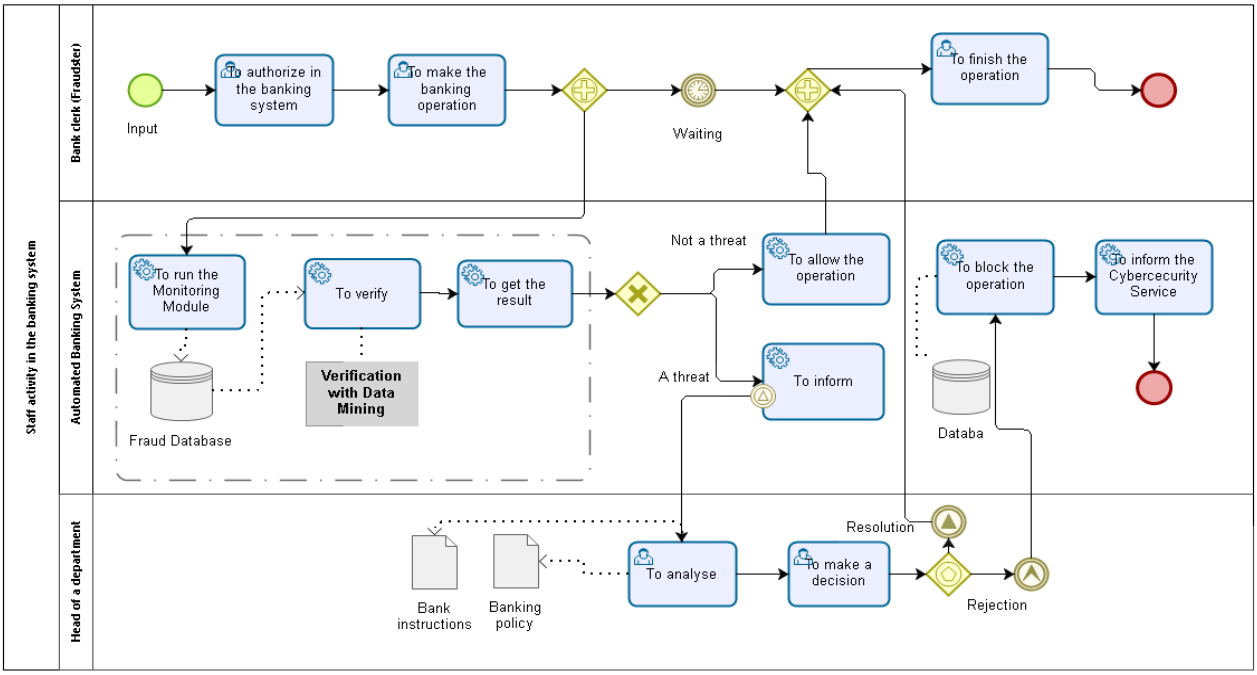


Рисунок 4.5 – Схема процесу здійснення операцій персоналом банку [93]

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 4.5;

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.

4.2 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 4.6.

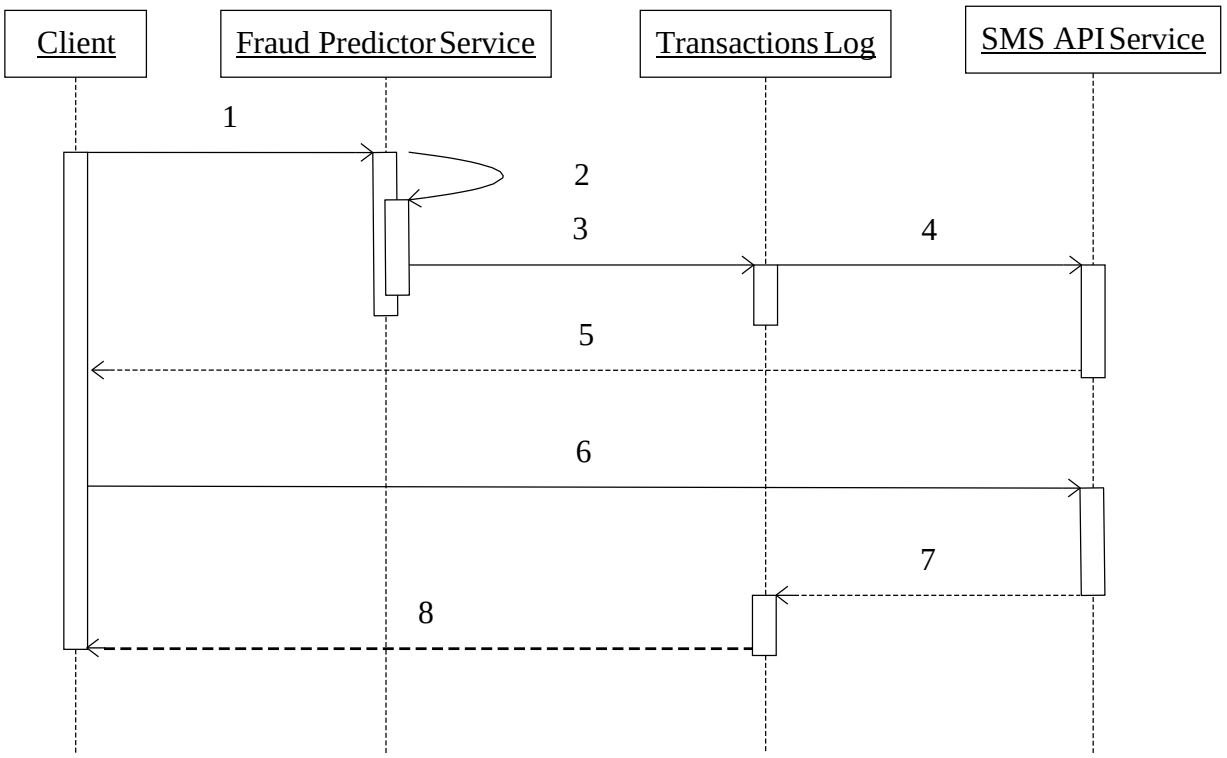


Рисунок 4.6 – Діаграма послідовності системи

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 [96].

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 [97].

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

На рисунку 4.6 зображено контекстну діаграму процесу виявлення шахрайських операцій. Після неї наведемо пояснення до кожного елементу, що присутній на діаграмі (таблиця 4.1).

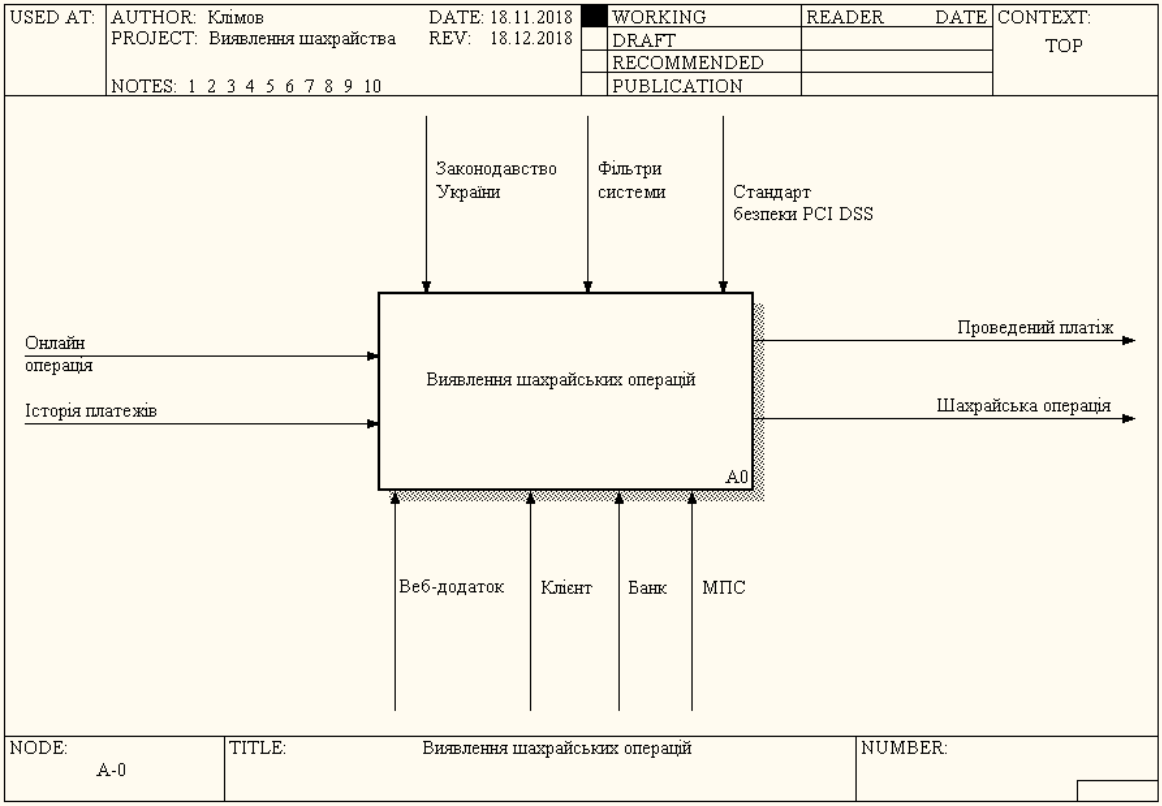


Рисунок 4.6 – Контекстна діаграма «Виявлення шахрайських операцій»

Таблиця 4.1 – 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 (рис. 4.7).

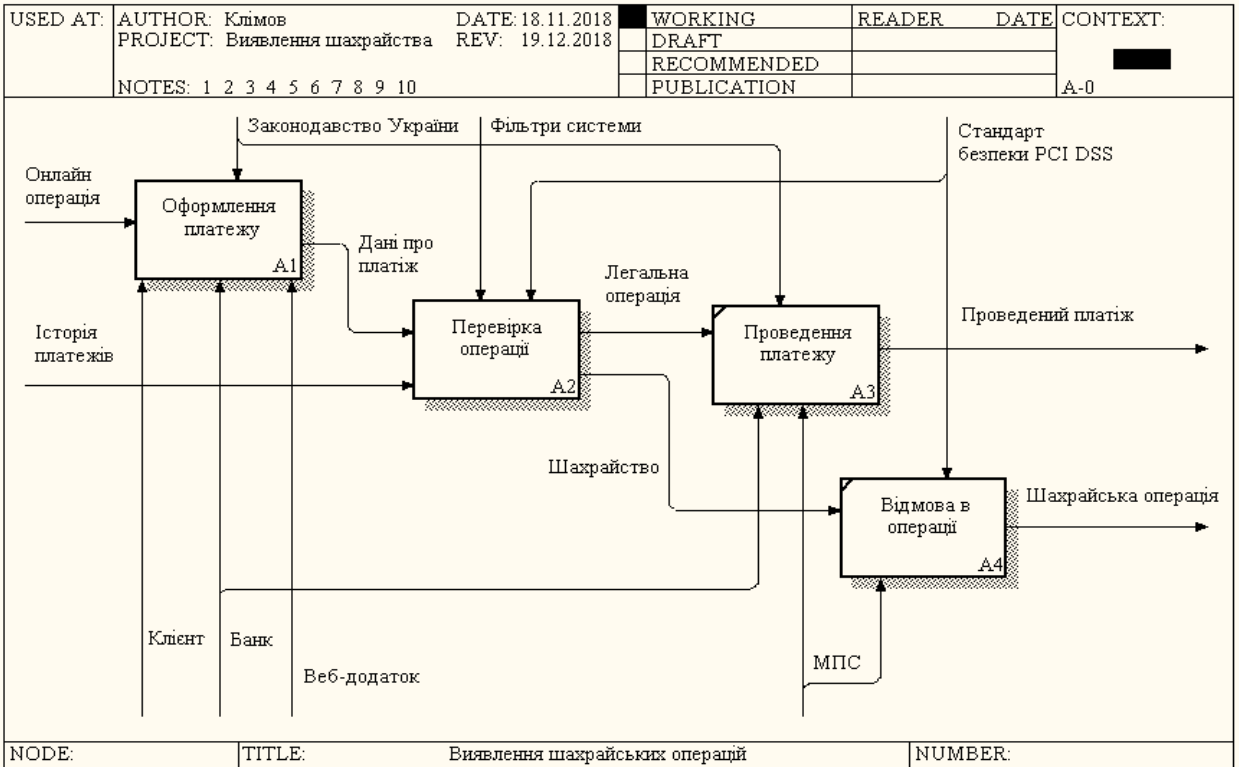


Рисунок 4.7 – Декомпозиція контекстної діаграми

Для поданого рисунка необхідно навести опис робіт (табл. 4.2).

Таблиця 4.2 – 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 (табл. 4.3).

Таблиця 4.3 – 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» (рис. 4.8), де зображено 3 роботи, які складають процес оформлення платежу. Необхідно навести їх опис у вигляді таблиці 4.4. Також потрібно продемонструвати зв’язків між ними, описавши їх в таблиці 4.5. Зв’язки об’єднують не тільки роботи в цій діаграмі-декомпозиції, а й в батьківській.

Таблиця 4.4 – Опис робіт діаграми-декомпозиції

Функціональний блок	Опис	Тип
Заповнення банківських реквізитів	Процес введення клієнтом даних банківської картки	WORKING
Заповнення адреси доставки	Процес введення регіону та місту, куди відправляти товар	WORKING
Визначення місцезнаходження	Пошук міста, в якому знаходиться клієнт, за допомогою IP-адреси	WORKING

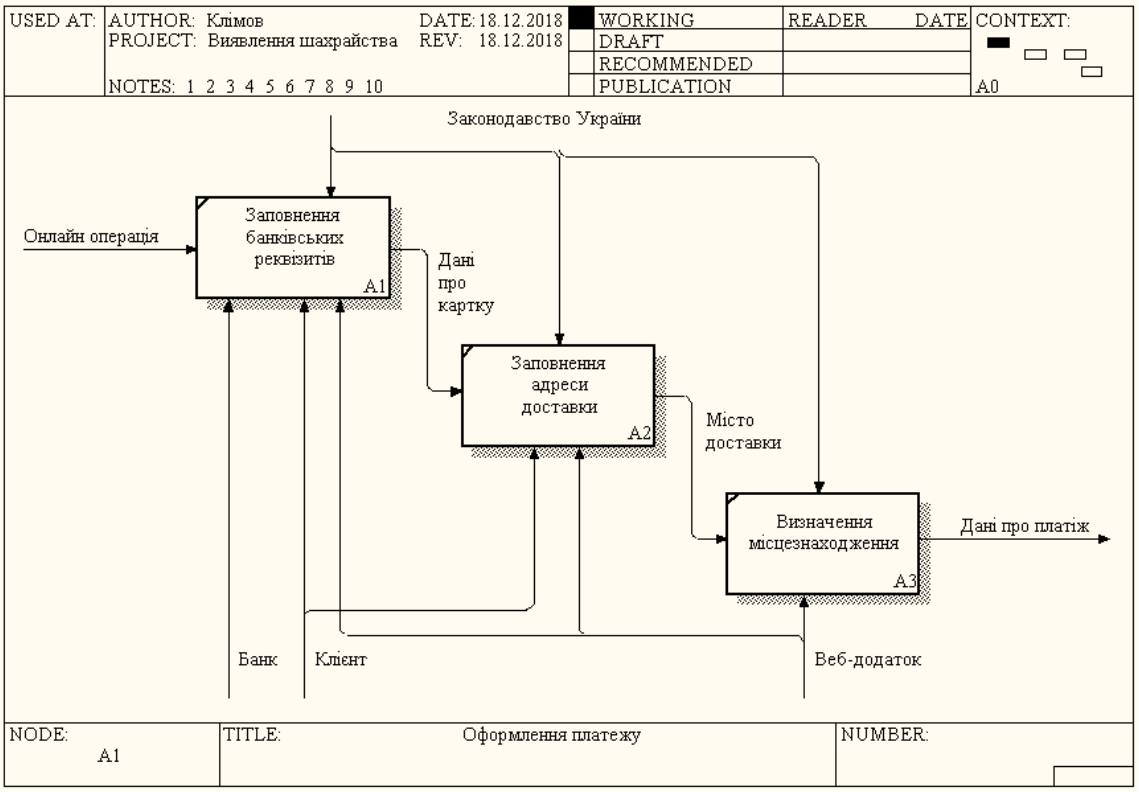


Рисунок 4.8 – Діаграма-декомпозиція процесу «оформлення платежу»

Таблиця 4.5 – 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 4.9. Детальний опис поданої діаграми наведемо в наступній таблиці 4.6.

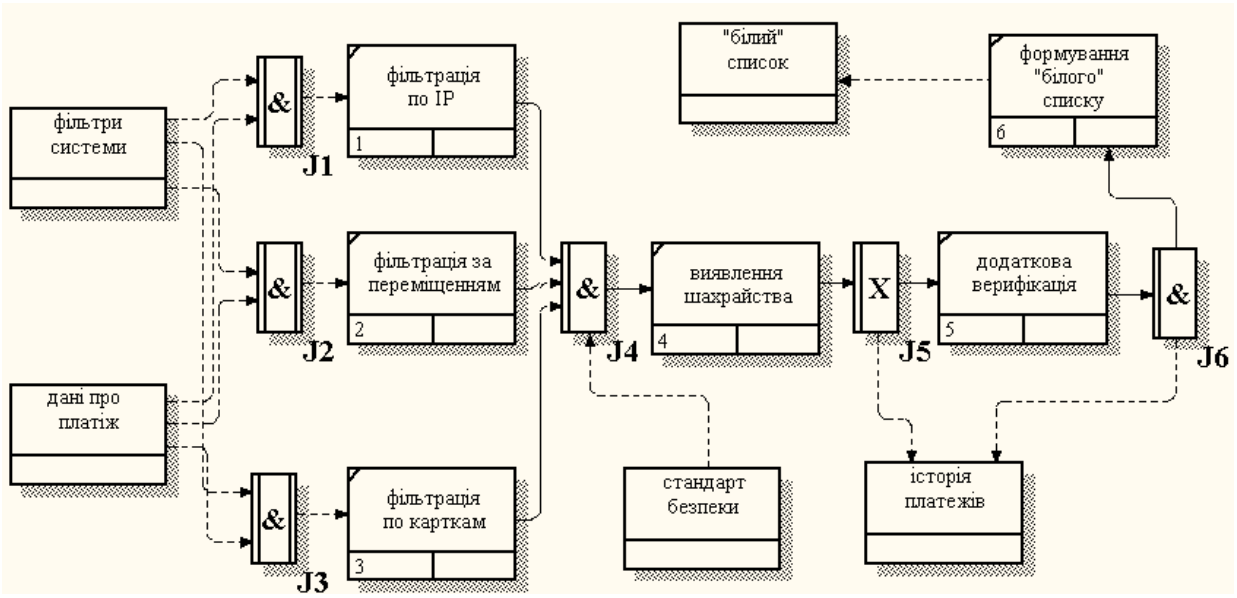


Рисунок 4.9 – IDEF3 діаграма системи виявлення шахрайства

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 4.6 – 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 діє 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 4.7 – 4.12).

Таблиця 4.7 – 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 4.8 – 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 4.9 – 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 4.10 – 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 4.11 – 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 4.12 – 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» (рис. 4.10).

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 4.11-4.14).

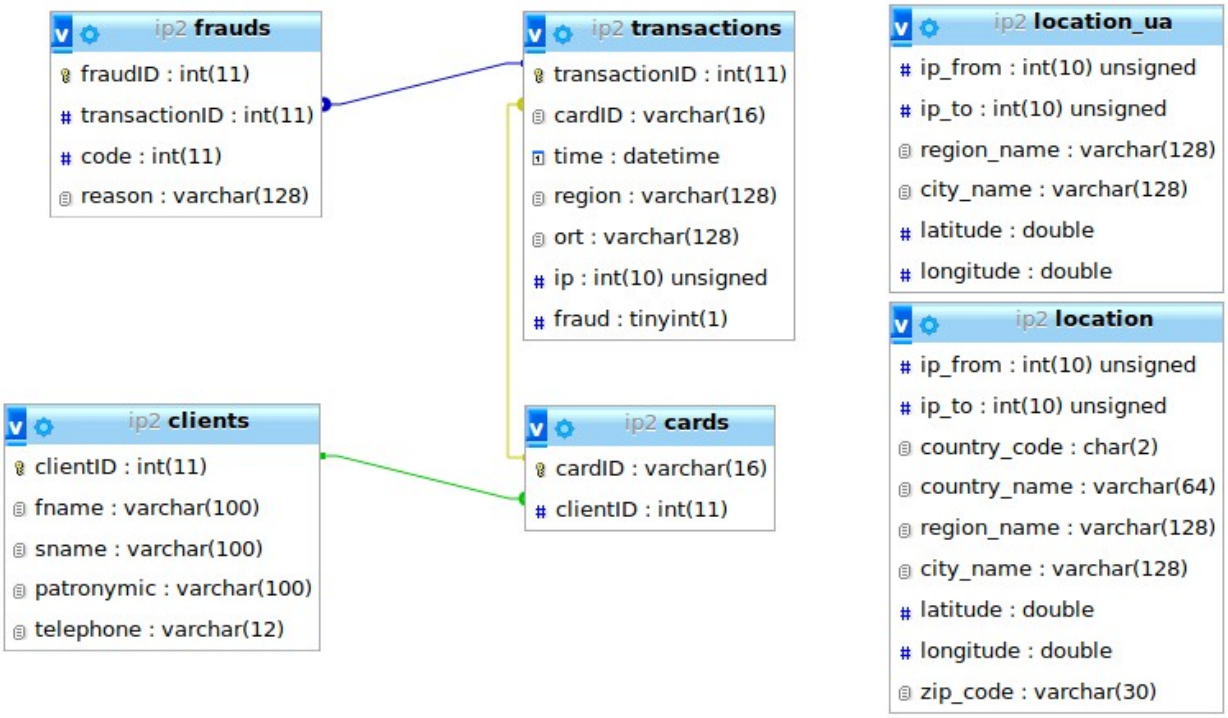


Рисунок 4.10 – Схема бази даних автоматизованого модуля виявлення шахрайських операцій з картками

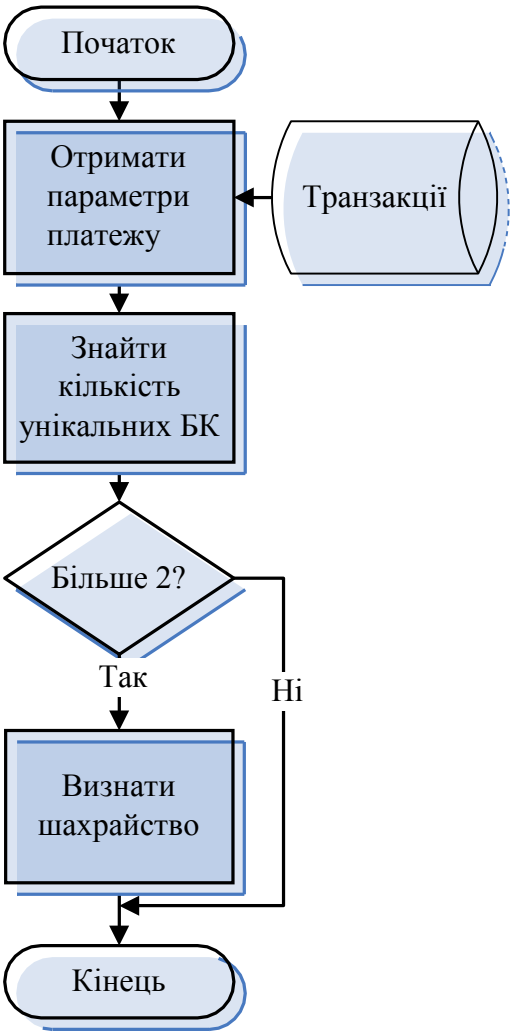


Рисунок 4.11 – Блок-схема алгоритму фільтрування за кількістю карт

Логіка алгоритму, продемонстрованого на рисунку 4.11, 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.

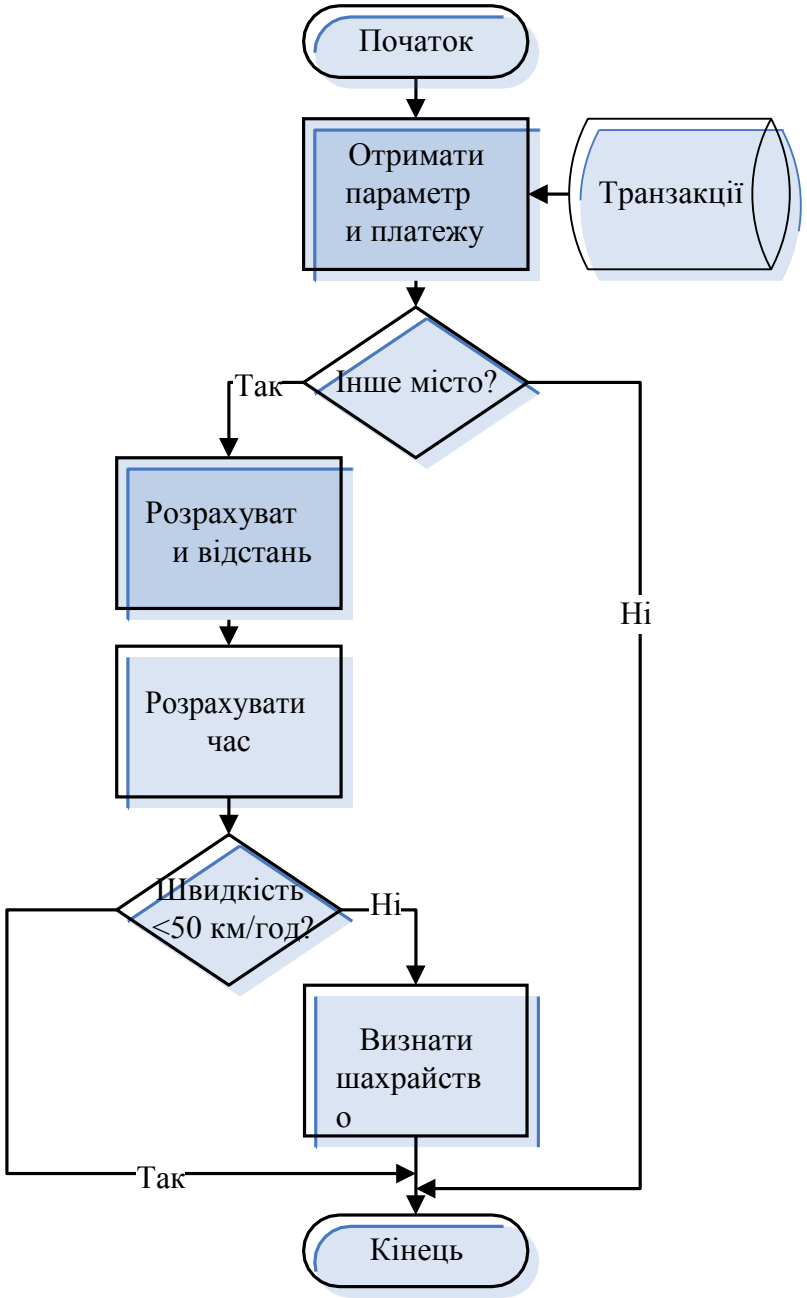


Рисунок 4.12 – Блок-схема алгоритму фільтрування за швидкістю переміщення клієнта

Рисунок 4.12 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.

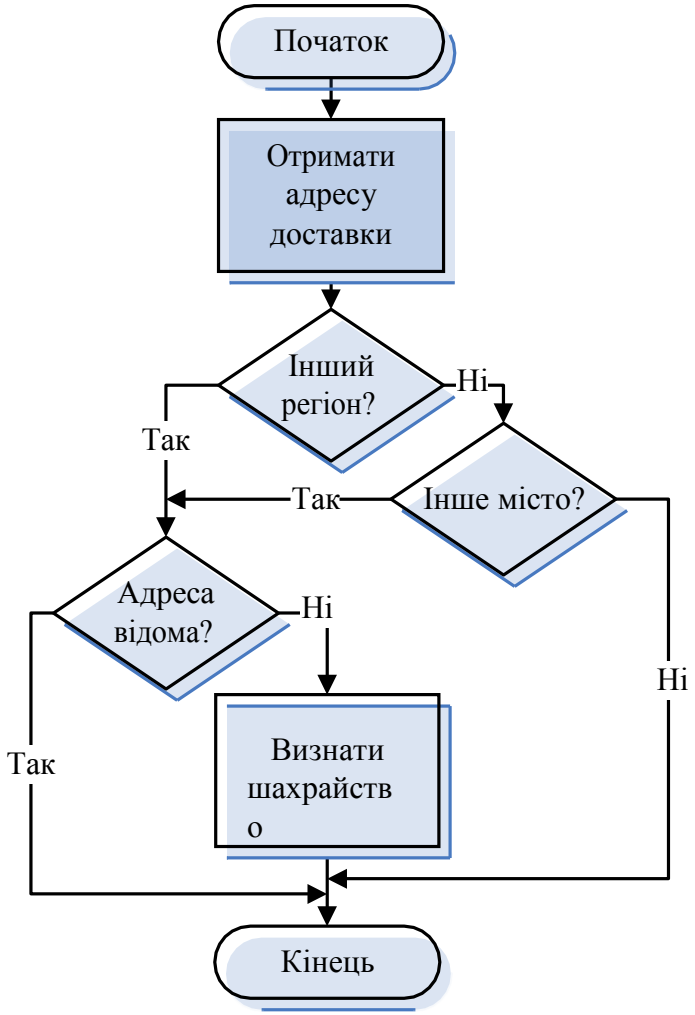


Рисунок 4.13 – Блок-схема алгоритму фільтрування за місцем знаходження та доставки

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.

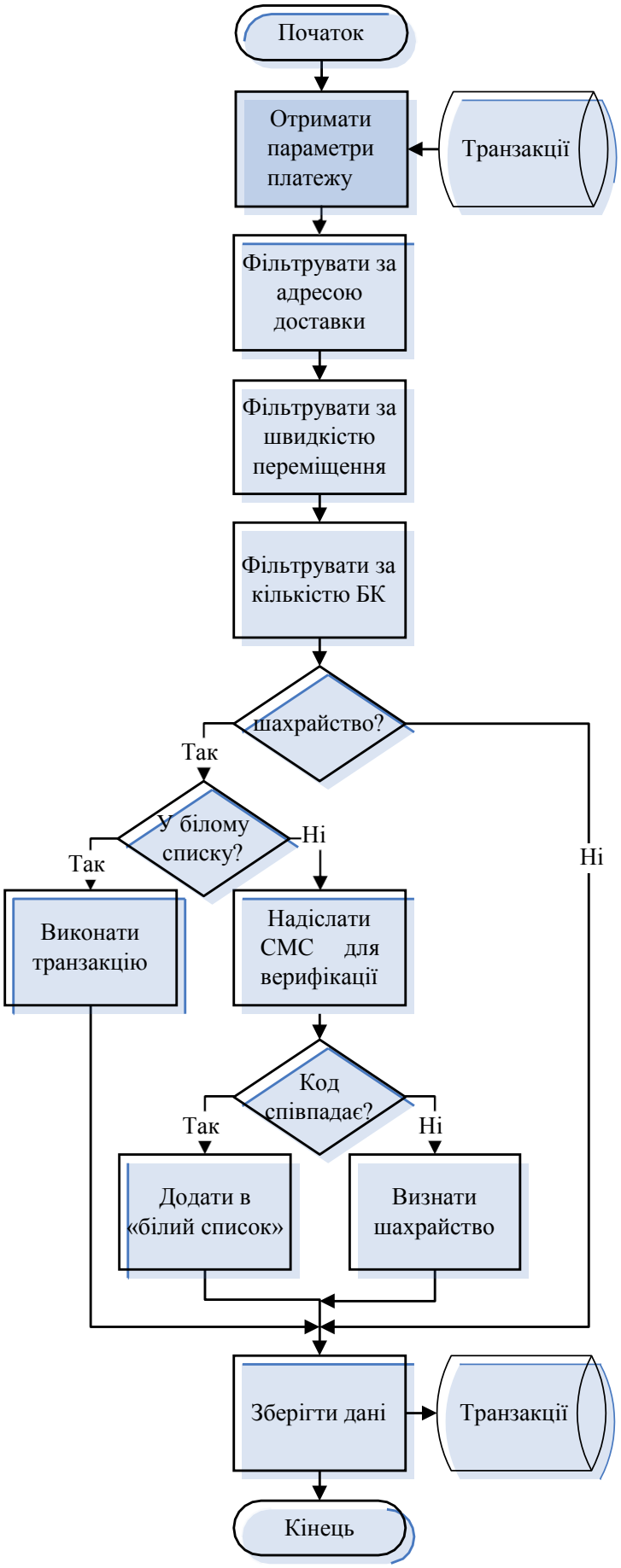


Рисунок 4.14 – Загальний вигляд алгоритму модулю виявлення шахрайства

На рисунку 4.14 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 4.14, 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 4.15). 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.

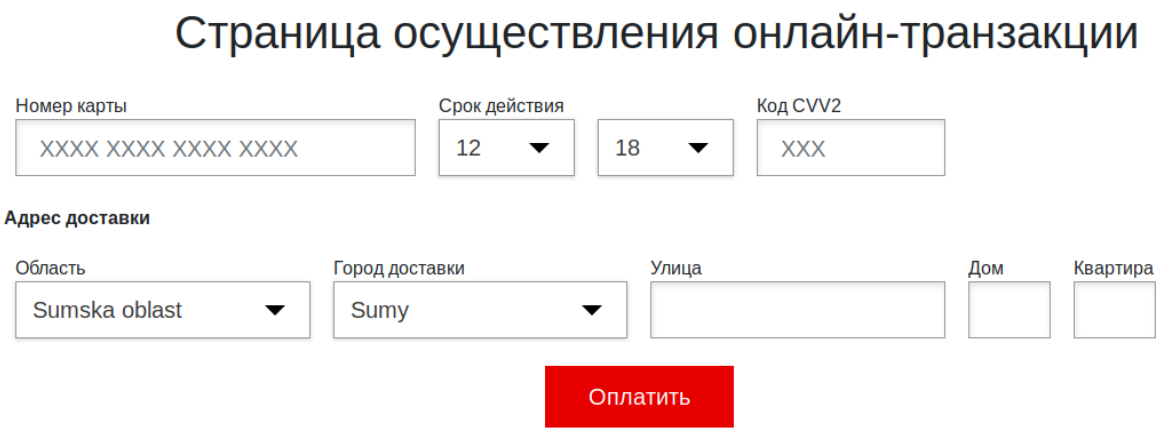


Рисунок 4.15 – Вікно здійснення онлайн-платежу

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 (рис. 4.16), який необхідно ввести у форму (рис. 4.17). 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.

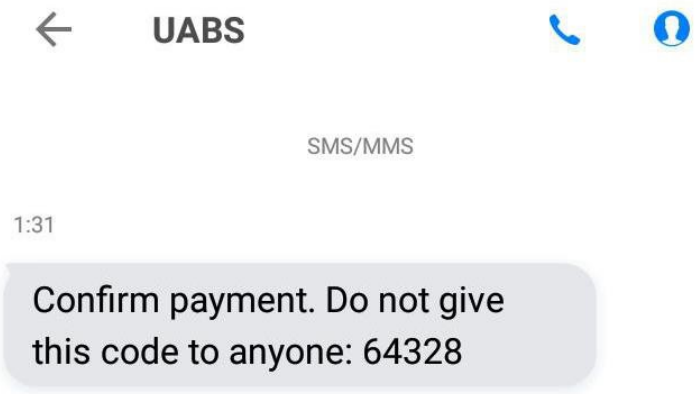


Рисунок 4.16 – СМС з кодом підтвердження

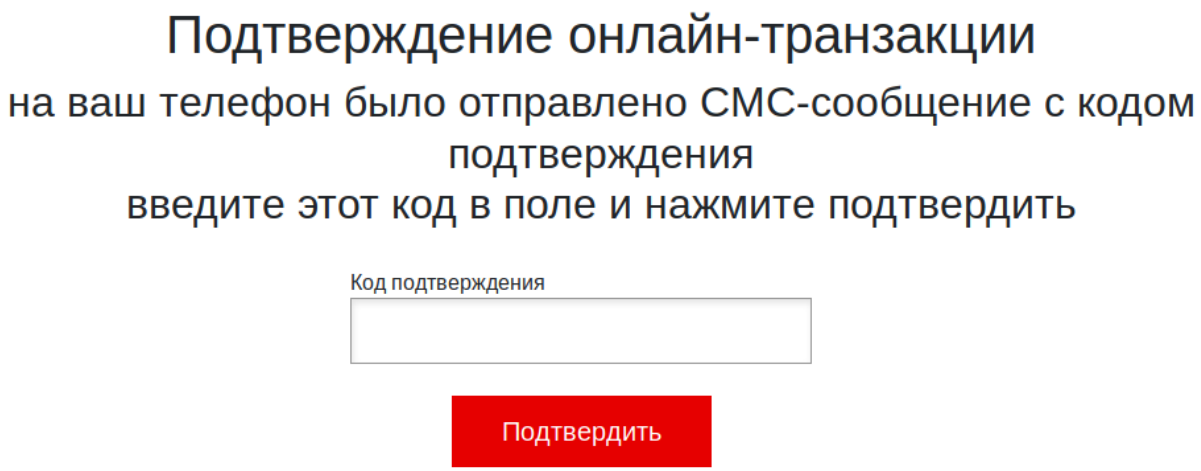


Рисунок 4.17 – Вікно підтвердження платежу

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 4.18). 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.

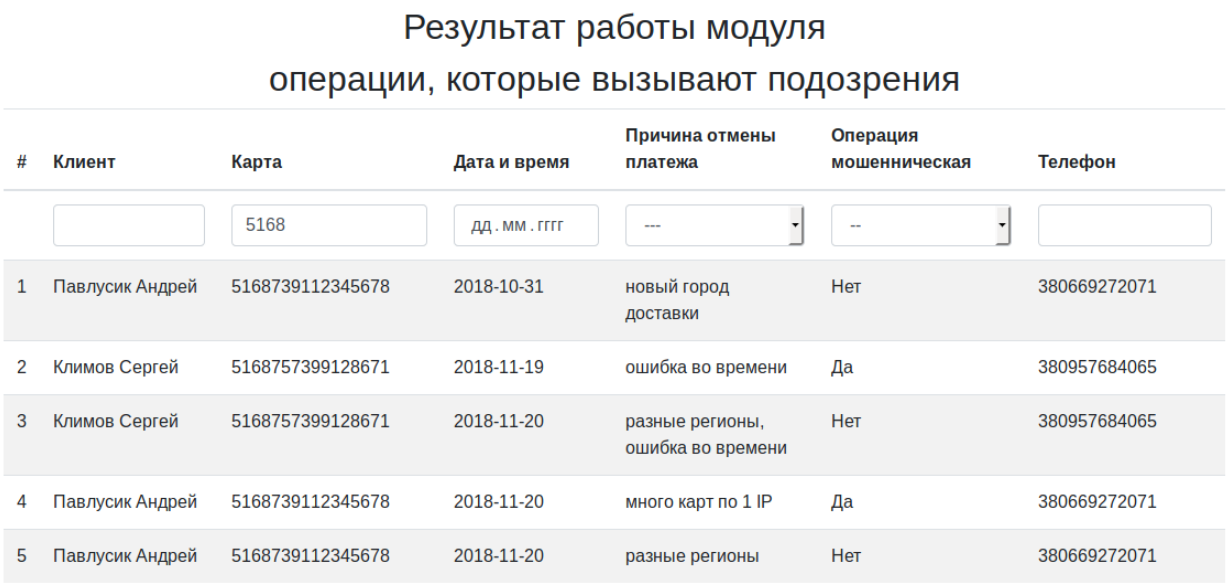


Рисунок 4.18 – Вікно виведення шахрайських операцій

Програмний код створення кожної сторінки автоматизованого модуля наведено в Додатку В. В лістингу В.4 наведено код JavaScript, який використовується для роботи з даними у вікні виведених результатів.

Важливим для роботи є програмний код, що реалізує зміну інформації в таблиці веб-додатку у режимі реального часу. Наведемо його також в Додатках, в лістингу В.5

Автоматизований модуль може використовуватися на практиці в електронній комерції для зменшення кількості шахрайських замовлень. Він також повинен бути інтегрований в інформаційну систему Інтернет-магазину та з’єднуватися з відповідним банком-еквайром.

До рекомендацій стосовно покращення автоматичної системи можна віднести її ускладнення новими функціональними можливостями. Для зменшення шахрайських операцій можна додати ще фільтри, які будуть перевіряти платежі. Проте це може призвести до зменшення конверсії. Тому важливим є налаштуванням системи під окремий вид електронної комерції. Якщо продається товар з низькою націнкою та великою собівартістю, то для погашення його втрати через шахрайство потрібно буде продати велику кількість товару. В цьому випадку необхідно максимально зменшити можливість шахрайських операцій. Якщо навпаки продається товар чи послуга, в ціну якої закладено більше 80% прибутків, то потрібно максимально збільшувати конверсію магазину. Серед можливих засобів фільтрації платежів я рекомендую реалізувати наступні:

– фільтрація за операційної системою та приладом, з якого відбувається платіж;

– фільтрація за сумою платежу (вартість покупки складає більше 90% заощаджень на рахунку);

– фільтрація по випадкам нестачі коштів;

– фільтрація за товарами.

Для удосконалення системи додатково рекомендується створити можливість для співробітника банку формувати звіти, зберігати та імпортувати їх.

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, шляхом розробки превентивних заходів контролю, як частини системи кібербезпеки;

розроблено гравітаційну модель оцінки привабливості країни для легалізації кримінальних доходів, що дозволить зменшити ризики для держави з боку легалізації кримінальних доходів та фінансування тероризму, які здійснюються за допомогою банківського сектору. Її застосування дозволить сформувати інформаційну базу для прийняття управлінських рішень щодо підвищення рівня кіберзахисту, оскільки це надає можливості концентрувати увагу саме на тих країнах, з якими ризик легалізації є підвищеним. Впровадження даної методики сприятиме розробці нових інструментів моніторингу, аналізу, оцінки та прогнозування фінансових операцій, здійснення яких можливе за межами країни;

розроблено прототип автоматизованого модулю процесу виявлення шахрайських операцій з банківськими картками, які здійснюються через Інтернет в процесі он-лайн платежів. В результаті модуль дозволяє відслідковувати операції, які потенційно можуть бути шахрайськими з урахуванням кількості карток клієнта, його місцезнаходженням та месцем здійснення операції, місцезнаходженням та адресою доставки, тощо. Запропонований модуль дозволяє попереджати клієнтів про факт здійснення шахрайства та попереджувати його.

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 ПОСИЛАНЬ

1. 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.

2. НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу [Електронний ресурс]. – Режим доступу: http://www.dstszi.gov.ua/dstszi/doccatalog/document?id=41650.

3. Майданюк Н. В. Перспективні технології підтримки інформаційної безпеки в банківській сфері [Електронний ресурс] / Н. В. Майданюк // Вісник Черкаського університету. Серія : Економічні науки. - 2017. - № 1. - С. 88-96. - Режим доступу: http://nbuv.gov.ua/UJRN/VchuE_2017_1_14.

4. Іванова Т. Г. Забезпечення безпеки інформації у галузі банківської діяльності як елемент розвитку цифрової економіки в Україні [Електронний ресурс] / Т. Г. Іванова // Молодий вчений. - 2018. - № 7(1). - С. 270-274. - Режим доступу: http://nbuv.gov.ua/UJRN/molv_2018_7(1)__62.

5. Зубок М. І. Безпека банківської діяльності: навч. посіб. / М. І. Зубок. – К. : КНЕУ, 2002. – 190 с.

6. Політика інформаційної безпеки ПАТ «МЕГАБАНК» [Електронний ресурс] // http://www.megabank.ua/articles/rules/information_security_policy.pdf.

7. Політика інформаційної безпеки ПАТ «Перший Інвестиційний Банк» [Електронний ресурс] // URL: http://www.pinbank.ua/wp-content/uploads/2017/02/Polityka_IB_2016_2.0_2_KT-1.pdf.

8. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения. Стандарт Банка России СТО БР ИББС-1.0-2010. Принят и введен в действие распоряжением Банка России от 21.06.2010 г. № Р-705.

9. Матвеев В.А. Информационная безопасность: Учебно-методическое пособие. – Нижний Новгород: Нижегородский госуниверситет, 2017. – 24 с.

10. Кібальник Л. О. Впровадження політики інформаційної безпеки банківських установ [Електронний ресурс] / Л. О. Кібальник, І. Ю. Напора // Причорноморські економічні студії. - 2016. - Вип. 12(2). - С. 119-122. - Режим доступу: http://nbuv.gov.ua/UJRN/bses_2016_12(2)_ 23.

11. Король О. Г. Аналіз загроз і механізмів забезпечення безпеки інформації в системі електронних платежів комерційного банку Украйни [Електронний ресурс] / О. Г. Король // Системи обробки інформації. - 2015. - Вип. 9. - С. 88-95. - Режим доступу: http://nbuv.gov.ua/UJRN/soi_2015_9_21

12. О Новом соглашении по оценке достаточности капитала Базельского комитета по банковскому надзору и перспективах его реализации в России

13. 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.

14. 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.

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

16. 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.

17. 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.

18. Belotti F., Daidone S., Ilardi G., Atella V. Stochastic frontier analysis using Stata. The Stata Journal. 2013. Vol. 13 (4). P. 719-758.

19. Chow-Chua C., Goh M., Wan T. B. *"Does ISO 9000 Certification Improve Business Performance?"* International Journal of Quality & Reliability Management. 2003. Vol. 20 (8). P. 936-53.

20. Francheskini F., Galetto M., Cecconi P. A worldwide analysis of ISO 9000 standard diffusion. *Benchmarking: An International Journal*. 2006. Vol. 13. No. 4. P. 523-541.

21. Hreniuc N. Coordinates of Banking Services Quality Management. URL: ftp://ftp.repec.org/opt/ReDIF/RePEc/rau/homkmg/WI11/HOMKMG-WI11-A5.pdf.

22. Manders B. ImplementationandImpactofISO 9001: thesis … degreeofDoctor. Rotterdam, 2015. 218 p.

23. Participant Guide: Information security operations. A guide to implementing effective information security controls. URL: https://www.openbanking.org.uk/wp-content/uploads/Participant-Guide-Information-Security-Operations.pdf (дата звернення 08.04.2018).

24. Psomas E. L., Pantouvakis A., Kafetzopoulos D. P. The impact of ISO 9001 effectiveness on the performance of service companies. Managing Service Quality. 2013. Vol. 23. No. 2. P. 149-164.

25. Selection and use of the ISO 9000 family of standards. ISO/TC 176, 2009. URL: http://the9000store.com/wp-content/uploads/2016/06/iso-9000-selection-and-use-2009.pdf (Last accessed: 20.04.2018).

26. Sharma D. S. "The Association between ISO 9000 Certification and Financial Performance." *International Journal of Accounting*. 2005. Vol. 40 (2). P. 151-72.

27. Terlaak A., King A. A. "The Effect of Certifi cation with the ISO 9000 Quality Management Standard: A Signaling Approach." *Journal of Economic Behavior and Organization*. 2006. Vol. 60 (4). P. 579-602.

28. Wooldridge J. Difference-in-Differences Estimation. NBER, Summer 2007. 19 p.

29. Yahia-Berrouiguet A., Mankouri I., Benarbia N. Impact of ISO 9001 Certification on Firm Performance: Case Study of Beni Saf Cement Company. *Journal of Economics and Business Research*. 2015. No.1. P. 158-165.

30. БАНК АВАНГАРД сертифіковано за стандартами ISO 9001:2015 та ISO 27001:2013 //Бюро Верітас Україна. URL: http://www.bureauveritas.com.ua/home/news/certification-avangard-bank-iso-9001-iso-27001?presentationtemplate=bv_master_v2/news_full_story_presentation_press_releases_v2 (дата звернення 10.04.2018).

31. Буряк А. В. Управління ефективністю банківського бізнесу: дис. … канд. екон. наук: 08.00.08. Суми, 2012. 268 с.

32. Історія банку // АТ «ПЕРШИЙ ІНВЕСТИЦІЙНИЙ БАНК» офіційний веб-сайт. URL: https://www.pinbank.ua/pro-bank/bank-sogodni/bank-sogodni-2/ (дата звернення 08.04.2018).

33. Показники банківської системи. Офіційний сайт Національного банку України. URL: https://bank.gov.ua/control/uk/publish/article?art_id=34661442&cat_id=34798593(дата звернення 08.04.2018).

34. Прес-центр // ПАТ «КРЕДІ АГРІКОЛЬ БАНК» офіційний веб-сайт. URL: https://credit-agricole.ua/o-banke/pres-centr/novini/kredi-agrikol-bank-za-napryamom-avtomobilne-kredituvannya-ot-445 (дата звернення 09.04.2018).

35. Річний звіт АТ «Укрексімбанк» 2013 // АТ «Укрексімбанк» офіційний веб-сайт. URL: https://www.eximb.com/upload/app_links/2001.pdf (дата звернення 08.04.2018).

36. Система якості // ПАТ «КРЕДИТПРОМБАНК» офіційний веб-сайт. URL: http://www.kreditprombank.com/ua/about/corp_managment/quality-control (дата звернення 08.04.2018).

37. 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. – №4. – С. 116–120.

38. Fraud Digest 28.09.2017 [Електронний ресурс] // Украинская межбанковская ассоциация членов платежных систем ЕМА. – 2017. – Режим доступу до ресурсу: https://ema.com.ua/fraud-digest-28-09-2017.

39. Fraud Digest 28.07.2017 [Електронний ресурс] // Украинская межбанковская ассоциация членов платежных систем ЕМА. – 2017. – Режим доступу до ресурсу: https://ema.com.ua/fraud-digest-25-07-2017/.

40. Trend Report «Financial Cyber Threats Q1 2017» [Електронний ресурс] // The official site of the company "ElevenPaths". – 2017. – Режим доступу до ресурсу: https://www.elevenpaths.com/wpcontent/uploads/2017/04/Financial_Threats_Q1-2017_EN.pdf.

41. Статистика платежного мошенничества — итоги 2017-го года [Електронний ресурс] // Украинская межбанковская ассоциация членов платежных систем ЕМА. – 2017. – Режим доступу до ресурсу: https://ema.com.ua/cyberfraud-ema-statistics-results-2017.

42. Некрасов В. Українці збагатили кібершахраїв на півмільярда: як не стати жертвою [Електронний ресурс] / В. Некрасов // FINANCE.UA. – 2018. – Режим доступу до ресурсу: https://news.finance.ua/ua/news/-/419603/ukrayintsi-zbagatyly-kibershahrayiv-na-pivmilyarda-yak-ne-staty-zhertvoyu.

43. Підсумки квартального засідання Форуму безпеки розрахунків з платіжними інструментами та кредитами 25 травня 2018р. [Електронний ресурс] // Украинская межбанковская ассоциация членов платежных систем ЕМА. – 2018. – Режим доступу до ресурсу: https://ema.com.ua/summary-fbrik-may-2018.

44. 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. – Режим доступу до ресурсу: http://www.economy.nayka.com.ua/?op=1&z=6453.

45. 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.

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

47. 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.

48. 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.

49. 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.

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

51. 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.

52. 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.

53. 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.

54. 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.

55. 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/.

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

57. #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/.

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

59. 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

60. 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

61. 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

62. 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)

63. 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

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

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

66. 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

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

68. 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.

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

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

71. 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

72. Бурячок В.Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В.Л. Бурячок, В.Б. Толубко, В.О. Хорошко, С.В. Толюпа]; за заг. ред. д-ра техн. наук, професора В.Б. Толубка. – К.: ДУТ, 2015. – 288 с.

73. Велігура А.В. Оцінювання стану інформаційної безпеки підприємства // Управління проектами та розвиток виробництва: зб. наук. пр. – Луганськ: вид-во СНУ ім.В.Даля, 2014. – №4(52). – С. 28-39.

74. Grading systems in the Netherlands, the United States and the United Kingdom [Електронний ресурс]. – Режим доступу: https://people.eecs.berkeley.edu/~marten/pdf/gradingsystems.pdf

75. Бутенко Л.М., Лозовик Ю.М. Аналітичні моделі швидкої діагностики підприємства та механізми їх забезпечення // Економіка та держава. – 2010. – №4. – С. 50-54.

76. Мірських Г.О., Реутська Ю.Ю. Комбіновані методи визначення вагових коефіцієнтів в задачах оптимізації та оцінювання якості об’єктів // Вісник Національного технічного університету України «КПІ». Серія «Радіотехніка. Радіоапаратобудування». – 2011. – №47. – С. 199-211.

77. Бирський В.В. Оцінювання стану економічної системи методами теорії нечітких множин // Держава та регіони. – 2010. – №4. – С. 11-15.

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

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

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

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

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

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

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

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

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

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

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

89. Hussein, S.: Predator-Prey Modeling. Und. J. of Math. Mod. **3**(1),20 (2010). doi: 10.5038/2326-3652.3.1.32

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

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

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

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

94. 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.

95. 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.

96. 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

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

ДОДАТКИ

Додаток А

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ СИСТЕМИ

Лістинг А.1 – Створення бази даних, ключових таблиць та зв’язків між ними

```
CREATE DATABASE ip2;
CREATE TABLE `cards` (
  `cardID` varchar(16) COLLATE utf8_bin NOT NULL,
  `clientID` int(11) NOT NULL
) ENGINE=InnoDB DEFAULT CHARSET=utf8 COLLATE=utf8_bin;
CREATE TABLE `clients` (
  `clientID` int(11) NOT NULL,
  `fname` varchar(100) COLLATE utf8_bin NOT NULL,
  `sname` varchar(100) COLLATE utf8_bin NOT NULL,
  `patronymic` varchar(100) COLLATE utf8_bin NOT NULL,
  `telephone` varchar(12) COLLATE utf8_bin NOT NULL
) ENGINE=InnoDB DEFAULT CHARSET=utf8 COLLATE=utf8_bin;
CREATE TABLE `frauds` (
  `fraudID` int(11) NOT NULL,
  `transactionID` int(11) NOT NULL,
  `code` int(11) NOT NULL,
  `reason` varchar(128) COLLATE utf8_bin NOT NULL
) ENGINE=InnoDB DEFAULT CHARSET=utf8 COLLATE=utf8_bin;
CREATE TABLE `location` (
  `ip_from` int(10) UNSIGNED DEFAULT NULL,
  `ip_to` int(10) UNSIGNED DEFAULT NULL,
  `country_code` char(2) COLLATE utf8_bin DEFAULT NULL,
  `country_name` varchar(64) COLLATE utf8_bin DEFAULT NULL,
  `region_name` varchar(128) COLLATE utf8_bin DEFAULT NULL,
  `city_name` varchar(128) COLLATE utf8_bin DEFAULT NULL,
  `latitude` double DEFAULT NULL,
  `longitude` double DEFAULT NULL,
  `zip_code` varchar(30) COLLATE utf8_bin DEFAULT NULL
) ENGINE=MyISAM DEFAULT CHARSET=utf8 COLLATE=utf8_bin;
CREATE TABLE `location_ua` (
  `ip_from` int(10) UNSIGNED DEFAULT NULL,
  `ip_to` int(10) UNSIGNED DEFAULT NULL,
  `region_name` varchar(128) COLLATE utf8_bin DEFAULT NULL,
  `city_name` varchar(128) COLLATE utf8_bin DEFAULT NULL,
  `latitude` double DEFAULT NULL,
  `longitude` double DEFAULT NULL
) ENGINE=MyISAM DEFAULT CHARSET=utf8 COLLATE=utf8_bin;
CREATE TABLE `transactions` (
  `transactionID` int(11) NOT NULL,
  `cardID` varchar(16) COLLATE utf8_bin NOT NULL,
  `time` datetime NOT NULL DEFAULT CURRENT_TIMESTAMP,
  `region` varchar(128) COLLATE utf8_bin NOT NULL,
```

```
  `ort` varchar(128) COLLATE utf8_bin NOT NULL,
  `ip` int(10) UNSIGNED NOT NULL,
  `fraud` tinyint(1) NOT NULL DEFAULT '0'
) ENGINE=InnoDB DEFAULT CHARSET=utf8 COLLATE=utf8_bin;
ALTER TABLE `cards`
  ADD PRIMARY KEY (`cardID`),
  ADD KEY `userID` (`clientID`);
ALTER TABLE `clients`
  ADD PRIMARY KEY (`clientID`);
ALTER TABLE `frauds`
  ADD PRIMARY KEY (`fraudID`),
  ADD KEY `transactionID` (`transactionID`);
ALTER TABLE `location`
  ADD KEY `idx_ip_from` (`ip_from`),
  ADD KEY `idx_ip_to` (`ip_to`),
  ADD KEY `idx_ip_from_to` (`ip_from`,`ip_to`);
ALTER TABLE `location_ua`
  ADD KEY `idx_ip_from` (`ip_from`),
  ADD KEY `idx_ip_to` (`ip_to`),
  ADD KEY `idx_ip_from_to` (`ip_from`,`ip_to`);
ALTER TABLE `transactions`
  ADD PRIMARY KEY (`transactionID`),
  ADD KEY `cardID` (`cardID`);
ALTER TABLE `clients`
  MODIFY `clientID` int(11) NOT NULL AUTO_INCREMENT,
AUTO_INCREMENT=3;
ALTER TABLE `frauds`
  MODIFY `fraudID` int(11) NOT NULL AUTO_INCREMENT,
AUTO_INCREMENT=7;
ALTER TABLE `transactions`
  MODIFY `transactionID` int(11) NOT NULL AUTO_INCREMENT,
AUTO_INCREMENT=11;
ALTER TABLE `cards`
  ADD CONSTRAINT `cards_cl ` FOREIGN KEY (`clientID`) REFERENCES
`clients` (`clientID`) ON DELETE CASCADE ON UPDATE CASCADE;
ALTER TABLE `frauds`
  ADD CONSTRAINT `frauds_ibfk_1` FOREIGN KEY (`transactionID`)
REFERENCES `transactions` (`transactionID`) ON DELETE CASCADE ON
UPDATE CASCADE;
ALTER TABLE `transactions`
  ADD CONSTRAINT `trans_card` FOREIGN KEY (`cardID`) REFERENCES
`cards` (`cardID`) ON DELETE CASCADE ON UPDATE CASCADE;
```

Лістинг А.2 – Підключення бази даних

```
<?php
define('DB_NAME', 'ip2');
define('DB_USER', 'root');
define('DB_PASSWORD', '123qsc');
define('DB_HOST', 'localhost');
define('DB_CHARSET', 'utf8');
```

```
$link = mysqli_connect(DB_HOST, DB_USER, DB_PASSWORD, DB_NAME)
or die(‘ошибка подключения БД’);
mysqli_set_charset($link, "utf8");
?>
```

Додаток Б

АЛГОРИТМІЧНЕ ЗАБЕЗПЕЧЕННЯ СИСТЕМИ

Лістинг Б.1 – Програмний код фільтрування операції з банківською картою

```
$bregion = $_POST['region_name'];
$bcity = $_POST['city_name'];
$fraudrisk = 0; $fraud = [];
$cardID = str_replace(" ","",$_POST['cardID']);
$sql = "SELECT `ort` FROM transactions WHERE cardID = '"
.$cardID . "' AND fraud=0";
$arr = mysqli_query($link,$sql);
while ($result = mysqli_fetch_assoc($arr)) {
    $array[] = $result['ort'];
}
/* фильтр 1 местоположение по IP и адрес доставки*/
if(!empty($array)) {
    if ($region == $bregion) {
        if($city != $bcity) {
            if (!in_array($bcity, $array)) {
                $fraud[] = "новый город доставки";
                $fraudrisk++;
            }
        }
    } else {
        if (!in_array($bcity, $array)) {
                $fraud[] = "разные регионы";
                $fraudrisk++;
        }
    }
}
/* фильтр 2 время и расстояние между заказами*/
if(!empty($array)) {
    $sql = "SELECT `time`, `ort`, `ip`, `latitude`, `longitude`,
`city_name` FROM transactions, location WHERE cardID = '" .
$cardID . "' AND `ip` <= ip_to ORDER BY `time` DESC LIMIT 1";
    $arr = mysqli_query($link,$sql);
    $res = mysqli_fetch_assoc($arr);
    if($res['city_name'] != $city) { // город текущий и город
последней транзакции
        $time_dif = (strtotime("now")-
strtotime($res['time']))/3600; // разница в часах
        $sql = "SELECT `latitude`, `longitude` FROM location
WHERE city_name = '" . $city . "'";
        $result = mysqli_fetch_assoc(mysqli_query($link,$sql));
// координаты текущего города
        $lat1 = $res['latitude'];
        $long1 = $res['longitude'];
        $lat2 = $result['latitude'];
        $long2 = $result['longitude'];
```

```
        $dist = calculateTheDistance($lat1, $long1, $lat2,
$long2) / 1000; // расстояние в км
        if($time_dif < $dist/50) { // скорость 50 км/ч
            $fraudrisk=1;
            $fraud[] = "ошибка во времени";
        }
    }
}
/* фильтр 3 несколько карт по 1 IP*/
if(!empty($array)) {
    $sql = "SELECT DISTINCT cardID as `Cards` FROM
`transactions` WHERE `time` > DATE_SUB(NOW(), INTERVAL 1 DAY)
AND `ip` = '" . $ipnum . "'";
    $result = mysqli_query($link,$sql);
    $cards = [];
    foreach ($result as $res) {
        $cards[] = $res['Cards'];
    }
    $cards[] = $cardID;
    $cards = count(array_unique($cards));
    if ($cards > 2) {
        $fraudrisk=2;
        $fraud[] = "много карт по 1 IP";
    }
}
```

Лістинг Б.2 – Розрахунок відстані між містами

```
define('EARTH_RADIUS', 6372795);
function calculateTheDistance ($φA, $λA, $φB, $λB) {
    // перевести координаты в радианы
    $lat1 = $φA * M_PI / 180;
    $lat2 = $φB * M_PI / 180;
    $long1 = $λA * M_PI / 180;
    $long2 = $λB * M_PI / 180;
    // косинусы и синусы широт и разницы долгот
    $cl1 = cos($lat1);
    $cl2 = cos($lat2);
    $sl1 = sin($lat1);
    $sl2 = sin($lat2);
    $delta = $long2 - $long1;
    $cdelta = cos($delta);
    $sdelta = sin($delta);
    // вычисления длины большого круга
    $y = sqrt(pow($cl2 * $sdelta, 2) + pow($cl1 * $sl2 - $sl1 *
$cl2 * $cdelta, 2));
    $x = $sl1 * $sl2 + $cl1 * $cl2 * $cdelta;
    $ad = atan2($y, $x);
    $dist = $ad * EARTH_RADIUS;
    return $dist;
}
```

Лістинг Б.3 – Збереження результатів в базі даних

```
if ($fraudrisk > 0) {
    $sql = "SELECT tr.cardID, tr.ip FROM frauds f, transactions
tr WHERE f.transactionID = tr.transactionID AND tr.fraud = 0
            AND tr.time > DATE_SUB(NOW(), INTERVAL 3 HOUR)";
    $frauds = mysqli_query($link, $sql);
    while ($result = mysqli_fetch_assoc($frauds)) {
        $WL_cards[] = $result['cardID'];
        $WL_ip[] = $result['ip'];
    }
    if(in_array($cardID, $WL_cards) || in_array($ipnum, $WL_ip))
    {
        $sql = 'INSERT INTO `transactions`(`cardID`, `region`,
`ort`, `ip`, `fraud`) VALUES ("' . $cardID . '", "' . $bregion .
'", "' .
        $bcity . '", "' . $ipnum . '", "0")';
        echo $sql;
        mysqli_query($link, $sql);
    } else {
        $fraud = implode(" ",$fraud);
        $sql = 'INSERT INTO `transactions`(`cardID`, `region`,
`ort`, `ip`, `fraud`) VALUES ("' . $cardID . '", "' . $bregion .
'", "' .
        $bcity . '", "' . $ipnum . '", "1")';
        mysqli_query($link, $sql);
        $transactionID = mysqli_insert_id($link);
        $code = mt_rand(10000, 99999);
        $sql = "INSERT INTO `frauds`(`transactionID`, `code`,
`reason`) VALUES ('" . $transactionID . "', '" . $code . "', '"
.$fraud . "')";
        mysqli_query($link, $sql);
        include_once('send.php');
        mysqli_close($link);
        echo '<form method="post" accept-charset="UTF-
8"action="send_form.php" name="send_form">
                <input type="hidden" name="transaction" value="'
. $transactionID . '">
            </form>';
        echo '<script type="text/javascript">
        document.forms["send_form"].submit();
        </script>';
    }
}
```

Додаток В

КЛІЄНТСЬКИЙ ВЕБ-ДОДАТОК

Лістинг В.1 – Створення вікна здійснення онлайн-платежу

```
<?php include_once('ip.php'); ?>
<!DOCTYPE html>
<html lang="en">
<head>
     <meta charset="utf-8">
    <meta name="viewport" content="width=device-width, initial-
scale=1, shrink-to-fit=no">
     <title>Anti-fraud system</title>
     <link rel="stylesheet"
href="https://stackpath.bootstrapcdn.com/bootstrap/4.1.3/css/boo
tstrap.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/boo
tstrap.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/boo
tstrap.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
/popper.min.js" integrity="sha384-
ZMP7rVo3mIykV+2+9J3UJ46jBk0WLaUAdn689aCwoqbBJiSnjAK/l8WvCWPIPm49
" crossorigin="anonymous"></script>
<script
src="https://stackpath.bootstrapcdn.com/bootstrap/4.1.3/js/boots
trap.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');
          });
    });
```

Кузьменко Ольга Віталіївна,
Яровенко Ганна Миколаївна,
Лєонов Сергій Вячеславович

СУЧАСНІ ІНСТРУМЕНТИ БОРОТЬБИ З КІБЕРШАХРАЙСТВАМИ У БАНКАХ

Монографія
За загальною редакцією О. В. Кузьменко, Г. М. Яровенко

Відповідальний за випуск О. В. Кузьменко

Підписано до друку 16.11. 2018.
Формат 60х84/16. Папір офсетний. Друк офсетний.
Умовн. друк. арк. 9,98. Обл.-вид. арк. 9,86
Наклад 300 прим. Вид. №128/218.

Видавець і виготовлювач: видавництво «Ярославна», Україна,
40030, м. Суми, вул. Горького, 2,

Свідоцтво про внесення суб'єкта видавничої справи до державного реєстру
ДК № 332 від 09.02.2001 р.