Міністерство освіти і науки України

Сумський державний університет

Навчально-науковий інститут бізнесу, економіки та менеджменту

Кафедра економічної кібернетики

КВАЛІФІКАЦІЙНА РОБОТА БАКАЛАВРА

на тему «МОДЕЛЮВАННЯ РИЗИКУ ШАХРАЙСТВА З БАНКІВСЬКИМИ ПЛАТІЖНИМИ КАРТКАМИ»

Виконала студентка 4 курсу, групи ЕК-81а

Спеціальності 051 «Економіка» (Економічна кібернетика)

Кільдей А. Д.

(прізвище, ініціали студента)

Керівник завідувач кафедри, д.е.н. Кузьменко О. В.

(посада, науковий ступінь, прізвище, ініціали)

Суми – 2022 рік

РЕФЕРАТ

кваліфікаційної роботи на тему

«МОДЕЛЮВАННЯ РИЗИКУ ШАХРАЙСТВА З БАНКІВСЬКИМИ ПЛАТІЖНИМИ КАРТКАМИ»

студентки ____Кільдей Анастасія Денисівна____

(прізвище, ім'я, по батькові)

Швидкі темпи модернізації банківського сектору, поява нових платіжних систем і методів розрахунків стали базою для появи різноманітних форм шахрайства, що потребують правового регулювання та визначення можливих шляхів боротьби з такими злочинами. Поширеними формами шахрайства є компрометування шахраями персональних даних, використання фішинг-сайтів, додаткове шкідливе програмне забезпечення, що можна встановити на POS-термінали тощо. Зі збільшенням частки шахрайства у фінансовому секторі наслідки несе як надавач платіжних послуг, так і безпосередньо користувач. Один із найбільших наслідків є зниження довіри громадян до фінансових установ, що в подальшому перешкоджає використанню грошей суспільства як інвестиційного інструменту для розвитку національної економіки.

Мета кваліфікаційної роботи полягає у вивченні теоретичних аспектів здійснення шахрайства з використанням банківських платіжних засобів та удосконалення науково-методичного підходу до протидії шахрайствам з банківськими картками.

Об'єктом цього дослідження є економічні відносини, що виникають між суб'єктами банківської діяльності з приводу протидії шахрайству з платіжними картками.

Предметом дослідження є науково-методичні та практичні аспекти функціонування системи протидії платіжному шахрайству в банках.

Задачами дослідження є:

– дослідити та класифікувати незаконні фінансові транзакції з платіжними картками;

– провести аналіз на предмет виявлення основних факторів, що впливають на здійснення шахрайства з платіжними картками;

– проаналізувати сучасний стан шахрайства з платіжними картками в Україні та світі;

– провести експрес-оцінку ризику шахрайств з банківськими картками;

– запропонувати заходи для удосконалення системи протидії шахрайствам з банківськими платіжними картками.

Для досягнення поставленої мети та завдань дослідження були використані такі методи дослідження: наукова абстракція, узагальнення, аналіз і синтез, порівняння – при обґрунтуванні теоретичних основ здійснення шахрайських операцій з банківськими платіжними картками; бібліометричний аналіз – при дослідженні основних векторів наукових досліджень у сфері платіжного шахрайства; методи описової статистики – для характеристики шахрайських фінансових транзакцій; методи Data Mining (алгоритм k-середніх) – для проведення експрес-оцінки ризику шахрайств з банківськими картками.

Основний науковий результат кваліфікаційної роботи полягає в тому, що було удосконалено систему протидії шахрайству з банківськими платежами включаючи в себе створення експрес-оцінки ризику здійснення шахрайства методами Data Mining. Одержані результати можуть бути використані у роботі банківських установ.

За результатами дослідження опубліковано статтю в фаховому журналі «Економічний форум» (2021 р., № 4). Наукова робота виконана в межах науково-дослідної теми «Data-Mining для протидії кібершахрайствам та легалізації кримінальних доходів в умовах цифровізації фінансового сектору економіки України» (№ д/р 0121U100467).

Ключові слова: шахрайство, банк, платіжні картки, Data Mining, кластеризація.

Зміст кваліфікаційної роботи викладено на 51 сторінках. Список використаних джерел із 28 найменувань, розміщений на 45–47 сторінках. Робота містить 2 таблиці, 30 рисунків, додатки А, Б.

Рік виконання кваліфікаційної робота – 2022 рік.

Рік захисту роботи – 2022 рік.

Міністерство освіти і науки України

Сумський державний університет

Навчально-науковий інститут бізнесу, економіки та менеджменту

Кафедра економічної кібернетики

ЗАТВЕРДЖУЮ
Завідувач кафедри
д.е.н., професор
_____ О.В. Кузьменко
“28” лютого 2022 р.

ЗАВДАННЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ БАКАЛАВРА

спеціальність 051 Економіка (Економічна кібернетика)
студенту 4 курсу, групи ЕК-81а

Кільдей Анастасії Денисівни
(прізвище, ім’я, по батькові студента)

1. Тема роботи «Моделювання ризику шахрайства з банківськими платіжними картками» затверджена наказом Про затвердження тем і керівників кваліфікаційних робіт наказ №0324-VI від 09.05.2022 року.
2. Термін подання студентом закінченої роботи «09» червня 2022 року
3. Мета кваліфікаційної роботи: вивчення теоретичних аспектів здійснення шахрайства з використанням банківських платіжних засобів та удосконалення науково-методичного підходу до протидії шахрайствам з банківськими картками.
4. Об’єкт дослідження є економічні відносини, що виникають між суб’єктами банківської діяльності з приводу протидії шахрайству з платіжними картками.
5. Предмет дослідження є науково-методичні та практичні аспекти функціонування системи протидії платіжному шахрайству в банках.
6. Кваліфікаційна робота виконується на матеріалах законодавчих та нормативних акти, статистичних даних Національного банку України та Європейського центрального банку, навчальних посібників, наукових публікацій іноземних та вітчизняних дослідників
7. Орієнтовний план кваліфікаційної роботи, терміни подання розділів керівникові та зміст завдань для виконання поставленої мети

Розділ 1. Теоретичні та прикладні аспекти здійснення шахрайства з банківськими платіжними картками – 15 травня 2022

У розділі 1.

1.1 Сутність, види та наслідки шахрайства з платіжними засобами – 15 травня 2022

1.2 Бібліометричний аналіз досліджень у сфері платіжного шахрайства – 15 травня 2022

1.3 Сучасні тенденції платіжного шахрайства в Україні та світі – 15 травня 2022

1.4 Постановка задач дослідження – 15 травня 2022

Розділ 2. Удосконалення системи протидії шахрайству з платіжними картками – 31 травня 2022

У розділі 2.

2.1 Опис вхідних даних для моделювання ризику шахрайства з банківськими платіжними картками – 31 травня 2022

2.2 Основні елементи системи протидії шахрайству з банківськими платіжними картками – 31 травня 2022

2.3 Експрес-оцінка ризику шахрайства з використанням банківської платіжної картки – 31 травня 2022

2.4 Рекомендації щодо удосконалення системи протидії платіжному шахрайству – 31 травня 2022

8. Консультації з роботи:

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
1			
2			
3			

9. Дата видачі завдання: «28» лютого 2022 року

Керівник кваліфікаційної роботи _____ О.В. Кузьменко

(підпис) (ініціали, прізвище)

Завдання до виконання одержав _____ А.Д. Кільдей

(підпис) (ініціали, прізвище)

ЗМІСТ

РЕФЕРАТ 2
ЗАВДАННЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ БАКАЛАВРА 5
ВСТУП 8
РОЗДІЛ 1. ТЕОРЕТИЧНІ ТА ПРИКЛАДНІ АСПЕКТИ ЗДІЙСНЕННЯ ШАХРАЙСТВА З БАНКІВСЬКИМИ ПЛАТІЖНИМИ КАРТКАМИ 10
1.1 Сутність, види та наслідки шахрайства з платіжними засобами 10
1.2 Бібліометричний аналіз досліджень в сфері платіжного шахрайства 14
1.3 Сучасні тенденції платіжного шахрайства в Україні та світі 19
1.4 Постановка задач дослідження 25
РОЗДІЛ 2. УДОСКОНАЛЕННЯ СИСТЕМИ ПРОТИДІЇ ШАХРАЙСТВУ З ПЛАТІЖНИМИ КАРТКАМИ 26
2.1 Опис вхідних даних для моделювання ризику шахрайства з банківськими платіжними картками 26
2.2 Основні елементи системи протидії шахрайству з банківськими платіжними картками 27
2.3 Експрес-оцінка ризику шахрайства з використанням банківської платіжної картки 30
2.3 Рекомендації щодо удосконалення системи протидії платіжному шахрайству 41
ВИСНОВКИ 43
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ 45
ДОДАТКИ 48

ВСТУП

Швидкі темпи модернізації банківського сектору, поява нових платіжних систем і методів розрахунків стали базою для появи різноманітних форм шахрайства, що потребують правового регулювання та визначення можливих шляхів боротьби з такими злочинами. Поширеними формами шахрайства є компрометування шахраями персональних даних, використання фішинг-сайтів, додаткове шкідливе програмне забезпечення, що можна встановити на POS-термінали тощо. Зі збільшенням частки шахрайства у фінансовому секторі наслідки несе як надавач платіжних послуг, так і безпосередньо користувач. Один із найбільших наслідків є зниження довіри громадян до фінансових установ, що в подальшому перешкоджає використанню грошей суспільства як інвестиційного інструменту для розвитку національної економіки.

На зростання рівня банківського шахрайства зазвичай впливають: недостатньо швидка реакція на сучасні методи шахрайства з платіжними картками, недостатній рівень інформаційного захисту бізнес-процесів банку, низький рівень фінансової грамотності, спрощена система ідентифікації клієнтів банку, а також недоліки нормативної бази.

Об’єктом цього дослідження є економічні відносини, що виникають між суб’єктами банківської діяльності з приводу протидії шахрайству з платіжними картками.

Предметом дослідження є науково-методичні та практичні аспекти функціонування системи протидії платіжному шахрайству в банках.

Метою дослідження є вивчення теоретичних аспектів здійснення шахрайства з використанням банківських платіжних засобів та удосконалення науково-методичного підходу до протидії шахрайствам з банківськими картками.

Для досягнення цієї мети необхідно реалізувати такі завдання:

– дослідження та класифікація незаконних фінансових транзакцій з платіжними картками;

– провести аналіз на предмет виявлення основних факторів, що впливають на здійснення шахрайства з платіжними картками;

– аналіз сучасного стану шахрайства з платіжними картками в Україні та світі;

– проведення експрес-оцінки ризику шахрайств з банківськими картками;

– запропонувати заходи для удосконалення системи протидії шахрайствам з банківськими платіжними картками.

Інформаційну та фактологічну основу роботи склали законодавчі та нормативні акти, статистичні дані Національного банку України та Європейського центрального банку, навчальні посібники, наукові публікації іноземних та вітчизняних дослідників з питань шахрайства з банківськими платежами.

За результатами дослідження опубліковано статтю в фаховому журналі «Економічний форум» (2021 р., № 4). Наукова робота виконана в межах науково-дослідної теми «Data-Mining для протидії кібершахрайствам та легалізації кримінальних доходів в умовах цифровізації фінансового сектору економіки України» (№ д/р 0121U100467), що фінансується Державним бюджетом України. Результати наукової роботи щодо ідентифікації ознак шахрайських транзакцій з використанням платіжних засобів розглянуті та прийняті до уваги філією Сумського обласного управління АТ «Ощадбанк».

РОЗДІЛ 1. ТЕОРЕТИЧНІ ТА ПРИКЛАДНІ АСПЕКТИ ЗДІЙСНЕННЯ ШАХРАЙСТВА З БАНКІВСЬКИМИ ПЛАТІЖНИМИ КАРТКАМИ

1.1 Сутність, види та наслідки шахрайства з платіжними засобами

Стрімкий розвиток цифрових технологій, зростання щільності покриття інтернетом території країни, а також карантинні обмеження із-за пандемії COVID-19 спровокували збільшення розрахунків в мережі Інтернет, нарощення обсягів безготівкових розрахунків з використанням банківських платіжних карток. За цих умов, банківські установи генерують значну за обсягом інформацію від своїх клієнтів. У разі порушення інформаційної безпеки фінансових установ конфіденційні дані можуть бути використані для здійснення протиправної діяльності або продані на темних веб-майданчиках, що може призвести до втрати ділової репутації як фінансових установ, так і їх клієнтів [16]. Разом з цим, причиною платіжного шахрайства є низький рівень цифрової та фінансової грамотності населення, що спричиняє втрату коштів з банківських рахунків.

Попри постійний аудит, контроль фінансових операцій, додаткові рівні перевірки клієнтської бази, безупинне вдосконалення систем інформаційної безпеки, злочинність з банківськими платіжними картками залишається одним із найбільш поширених злочинів у банківській сфері. Основними чинниками, що визначають банківську систему чутливою до злочинних дій є:

– зберігання та обробка великих об’ємів даних про фінансовий стан, діяльність клієнтів;

– низький рівень цифрової грамотності серед населення. У 2019 році 37,9% українців у віці 18-70 років володіли цифровими навичками нижче базового рівня, тоді як 15,1% – взагалі не володіють ними [26];

– відсутність стандартизованих систем верифікації клієнтів;

– низька ефективність системи контролю за інформаційною безпекою банків;

– недотримання керівниками банку стандартів установи щодо запобігання шахрайствам.

За даними компанії Merchant Savvy збитки від шахрайства з банківськими платежами у світі протягом 2011–2020 рр. зросли втричі: з 9,84 до 32,39 мільярдів доларів США. За їх прогнозами обсяг збитків від шахрайства з банківськими платіжними картками буде стабільно зростати і очікувано у 2027 році досягне 40,62 мільярдів доларів США, що на 25% перевищуватиме рівень 2020 року [4].

У 2020 році Європейський центральний банк інформував, що загальні збитки від шахрайських операцій в регіоні SEPA (Single Euro Payments Area або Єдина зона платежів в євро) склали 1,8 мільярда євро. Щодо видів банківських злочинів на території Європейського Союзу, то у 2020 році 79% банківських шахрайств здійснено у формі платежів через мережу Інтернет, 15% – кінцеві точки збуту (POS), 6% – платежі, здійснені через банкомат [4].

За даними опитування топ-менеджменту фінансових установ України, що проводилося фахівцями Національного банку України, станом на листопад 2021 року одним із головних джерел ризику для вітчизняного фінансового сектору є шахрайство та кібернетичні загрози (2 місце з поміж аналізованих загроз після «корупції, діяльності правоохоронних органів та судової системи»). У листопаді 2021 року 16% респондентів оцінили фактор «шахрайств та кібернетичних загроз» на дуже високому рівні, тоді як у листопаді 2020 року цей показник становив лише 3% респондентів [21].

За даними консалтингової компанії PwC 51% українських респондентів повідомили, що протягом останніх 2 років ставали жертвами банківського шахрайства. Цей показник переважає середній у світі на 4%, а також зріс у порівнянні з 2018 роком на 3% [13].

Проаналізувавши численні наукові праці [11, 18, 24], звіти національних фінансових регуляторів [22, 23], а також міжнародних організацій [9, 13],

систематизовано основні види шахрайства з банківськими платіжними картками (рис. 1.1).

Рисунок 1.1 – Види шахрайств з банківськими платіжними картками за способом вчинення

Джерело: складено на основі [9, 11, 13, 18, 22, 23, 24].

Нині одним з найбільш поширених видів шахрайства є соціальна інженерія. Суть методу полягає в тому, щоб вмотивувати «жертв» самостійно надати свої персональні дані або зробити переказ грошових коштів на рахунки шахраїв.

Вішинг, як один із методів шахрайства з використанням соціальної інженерії, полягає у використанні методів зв'язку (телефонні дзвінки, повідомлення, електронні листи) задня виманювання конфіденційної інформації. Зазвичай шахраї представляються співробітником банку, що повідомляє про незвичні транзакції на вашому рахунку. Зі слів зловмисника для перевірки рахунку потрібно повідомити CVV-код, PIN-код, номер картки та/ або інші конференційні дані.

Зазвичай дана схема розрахована на людей більш похилого віку через низьку обізнаність. Головним стимулом для розголошення своїх даних є оператор, що чинить тиск та наголошує на терміновості ситуації.

Наслідки від будь-якого виду шахрайства для споживача фінансових послуг з одної сторони очевидні: втрата довіри до банківської системи, безготівкових операцій, а також втрата грошових коштів. Але з іншого боку, при викраденні персональних даних, на людину можливо оформити десяток мікрозаймів онлайн. На виплату таких боргів або на оскарження факту їх одержання самою фізичною особою можуть витрачатися роки.

Довіра клієнтів є одним із найголовніших чинників розвитку та ефективного функціонування банківської установи. Доведено, що рівень довіри до банку, обсяг депозитів та кредитування мають між собою прямо пропорційну залежність. Зрозуміло, що високий ризик шахрайства з банківськими платежами та вразливість конфіденційних даних пророкують зниження довіри до банків, що зі сторони суспільства веде до накопичення грошової маси поза фінансовими установами. За цих умов стабільний розвиток національної економіки ускладнюється.

Поняття довіри також має психологічний характер. Клієнт банку, який довіряє свої ресурси обраній установі, приймає усі ризики, зумовлені банківською діяльністю, та розраховує, що його грошові платежі повністю захищенні від внутрішнього та зовнішнього шахрайства.

За даними опитування Українського центру економічних та політичних досліджень ім. О. Разумкова, проведеного в період липень – серпень

2021 року, встановлено, що 31,8% респондентів повністю не довіряють банкам в Україні, тоді як 38,9% – скоріше не довіряють, 15,6% – скоріше довіряють та 2,6% – повністю довіряють [17]. Дані цифри дозволяють стверджувати, що рівень довіри до вітчизняної банківської системи знаходиться на низькому рівні.

Для банківської установи наслідки від шахрайських операцій наведені нижче:

– фактична втрата коштів клієнтів банківської установи (фізичних та юридичних осіб);

– неможливість активно використовувати вільні кошти громадян як інвестиційний ресурс;

– зниження репутації, спричинені розкриттям банківської таємниці, персональних даних та інше;

– юридичні позови від постраждалих клієнтів;

– потреба у придбанні складніших засобів захисту для забезпечення належного рівня інформаційної безпеки; пошук кваліфікованих спеціалістів для вирішення поточних та майбутніх прогалин у системі інформаційної безпеки банку.

Таким чином, систематизація основних видів та причин вчинення банківського шахрайства дозволяє оцінити недоліки та прогалини, які можуть вплинути на зростання рівня банківського шахрайства та визначити можливі шляхи боротьби з цими видами злочинів.

1.2 Бібліометричний аналіз досліджень в сфері платіжного шахрайства

З розвитком технологій та безперервним економічним зростанням, що є очевидним у сучасному суспільстві, акти шахрайства стали набагато більш поширеними у фінансовій галузі. Для того, щоб підтвердити тенденції, окреслені даним дослідженням було проведено аналіз публікацій за період

2000 – 2021 рр. за такими запитами ключових слів, як «fraud» (шахрайство) та «card» (картка). Всього було знайдено 1791 документів. На рисунку 1.2 зображено темпи нарощення інтересу до теми шахрайств з платіжними картками.

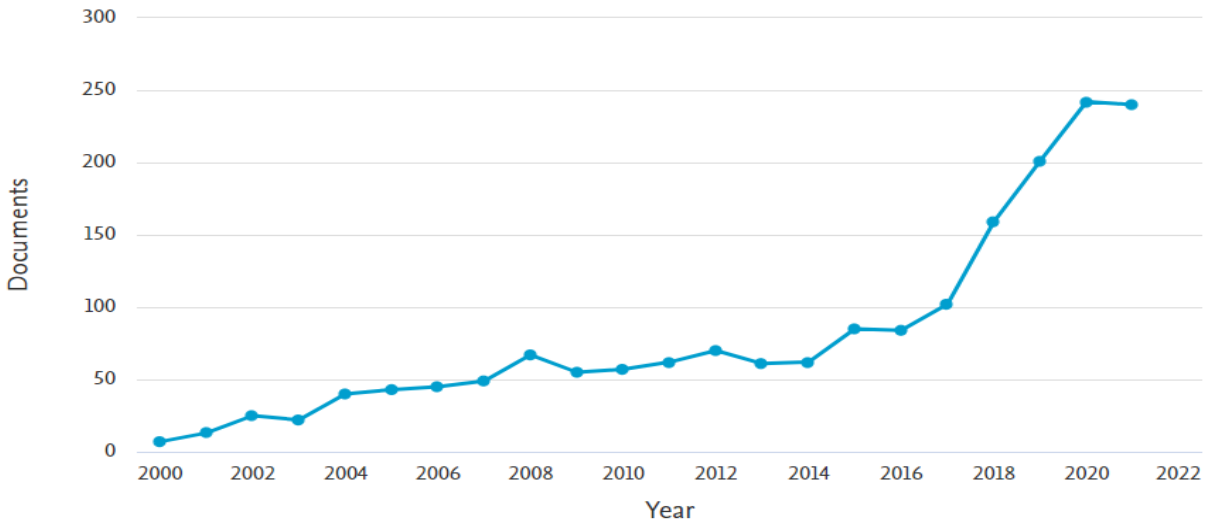

Рисунок 1.2 – Динаміка публікацій за ключовими словами «fraud» та «card» згідно з наукометричною базою Scopus протягом 2000–2021 рр., одиниць

Так, на основі даних, представлених на рисунку 1.2, можна відмітити, що питання шахрайства з платіжними операціями у середньому поступово збільшується протягом всього досліджуваного періоду. З 2017 року можна відмітити стрибкоподібне зростання кількості публікацій у даній сфері, приблизно на 50–75 публікацій щорічно. Натомість, найбільше публікацій було опубліковано у 2020 році, а саме – 242.

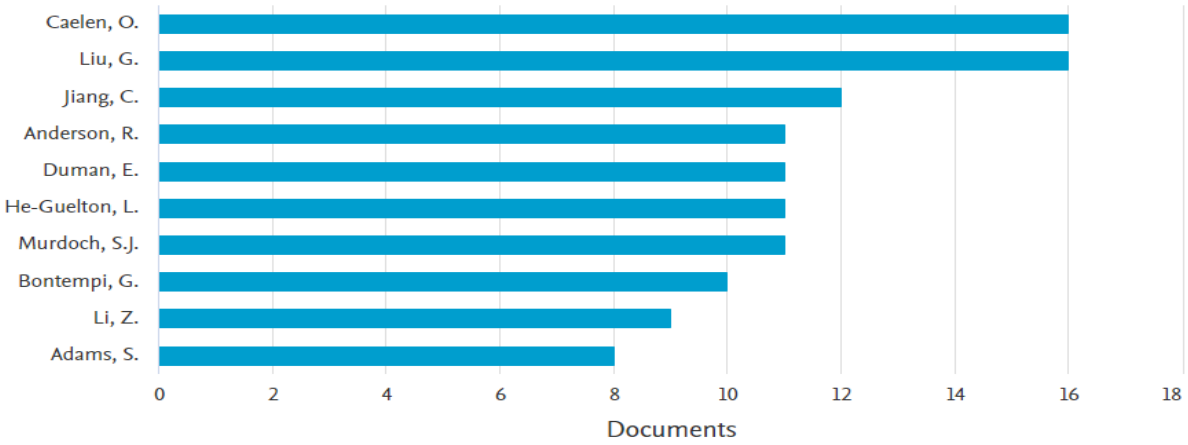

Рисунок 1.3 – Динаміка кількості публікацій за авторами з проблематики «шахрайство з банківськими картками» в базі Scopus у період 2000-2021 рр.

На рисунку 1.3 представлені науковці за кількістю публікацій з досліджуваної проблематики у наукометричній базі Scopus. Зокрема, О. Келен (O. Caelen) з науково-дослідницького центру Worldline (м. Ліон, Франція) має 16 публікацій, переважна кількість з них написана у таких сферах як: комп'ютерні науки, інженерія та математика. У своїй роботі [3] «Виявлення шахрайства з кредитними картками: реалістичне моделювання та нова стратегія навчання» автор вважає, що найбільш ефективним методом для аналізу та виявлення злочинних дій з банківськими платежами є штучний інтелект.

На прикладі роботи М. Шанмугам (M. Shanmugam) та ін. [10] доведено, що грошові перекази та оплата рахунків є найпопулярнішими засобами Інтернет-банкінгу у Великобританії. Авторами даної роботи зауважено, що безпека фінансових транзакцій є найважливішим чинником, що впливає на швидкість впровадження інтернет-банкінгу у Великобританії.

Ю. Лі (Y. Li) та К. Чжан (X. Zhang) у роботі [5] пропонують технологію, суть якої полягає в генерації одноразових номерів картки з деяким секретним параметром, відомим лише власнику картки та емітенту. За результатами

дослідження, така схема несе менше навантаження на емітентів кредитних карток та може бути організована у сфері офлайн та онлайн платежів.

У розрізі даної роботи доцільно також проаналізувати загальний перелік ключових слів у відібраних наукових публікаціях. За допомогою програмного забезпечення VOSviewer було сформовано три кластери ключових слів, що зустрічаються найчастіше в наукових працях за період з 2000 р. по 2021 р. (рис. 1.4).

Найбільшим кластером є червоний, що містить у собі 96 ключових слова (найбільш часто зустрічаються такі слова, як «data mining», «виявлення шахрайства», «шахрайства з картками», «дерева рішень», «аномальні значення»). Це дозволяє узагальнити червоний кластер як такий, що опосередковує виявлення та аналіз шахрайських операцій з картками.

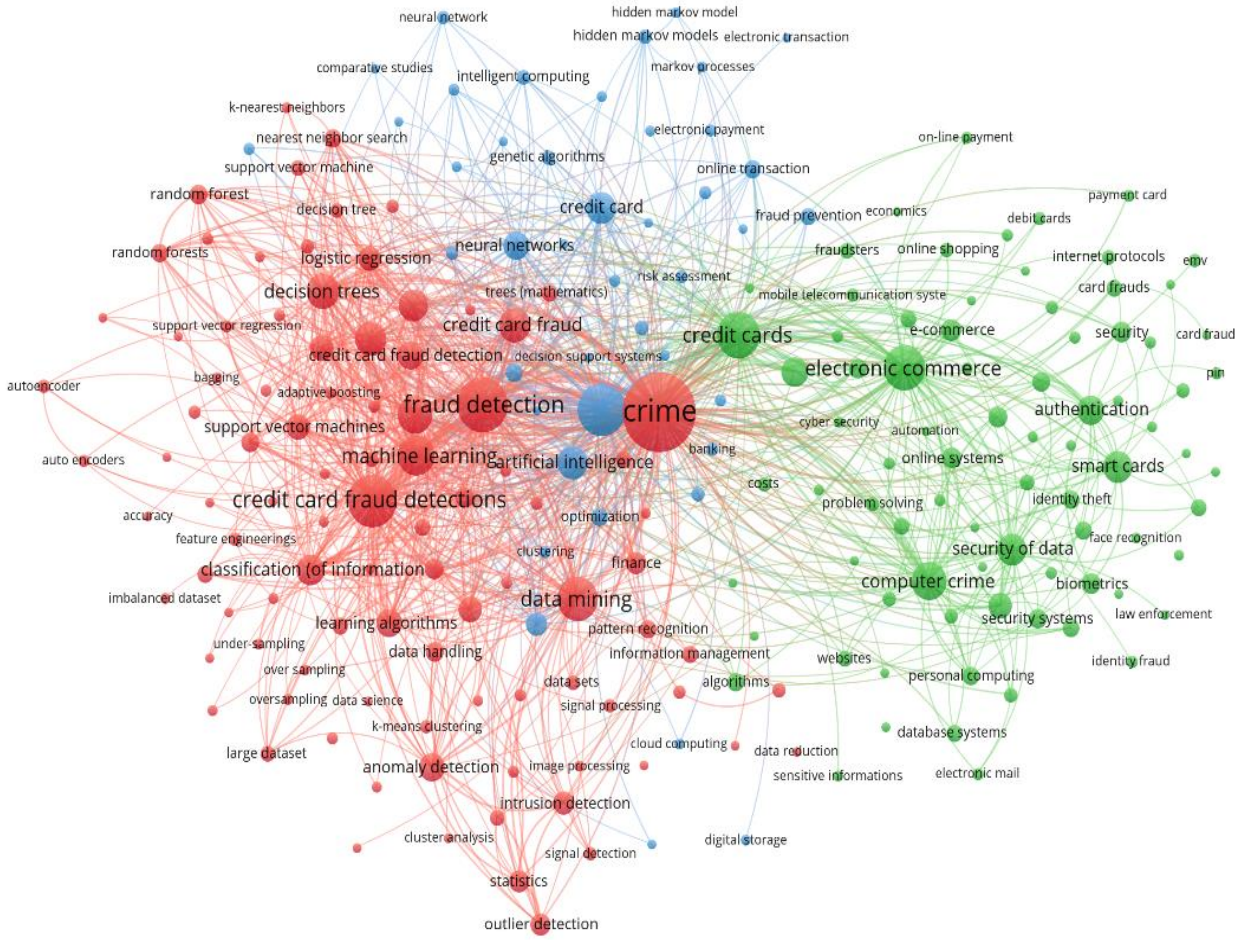

Рисунок 1.4 – Результати бібліометричного аналізу ключових слів,

що одночасно трапляються в публікаціях, проіндексованих наукометричною базою Scopus, за запитами «fraud» та «card» за допомогою інструментарію VOSviewer

Наступний за обсягом є зелений кластер, що складається з 81 ключових слів. До нього увійшли такі поняття, як «кредитні картки», «електронні платежі», «аутентифікація», «смарт картки», «онлайн-платежі». Тобто можна кластер окреслити як той, що узагальнює методи проведення та захисту банківських платежів.

Третій за обсягом кластер (47 слів) включає в себе такі поняття як «нейронні мережі», «штучний інтелект», «генетичні алгоритми», що в загальному об’єднує контекст використання інтелектуальних методів та прийомів для ідентифікації та протидії платіжному шахрайства.

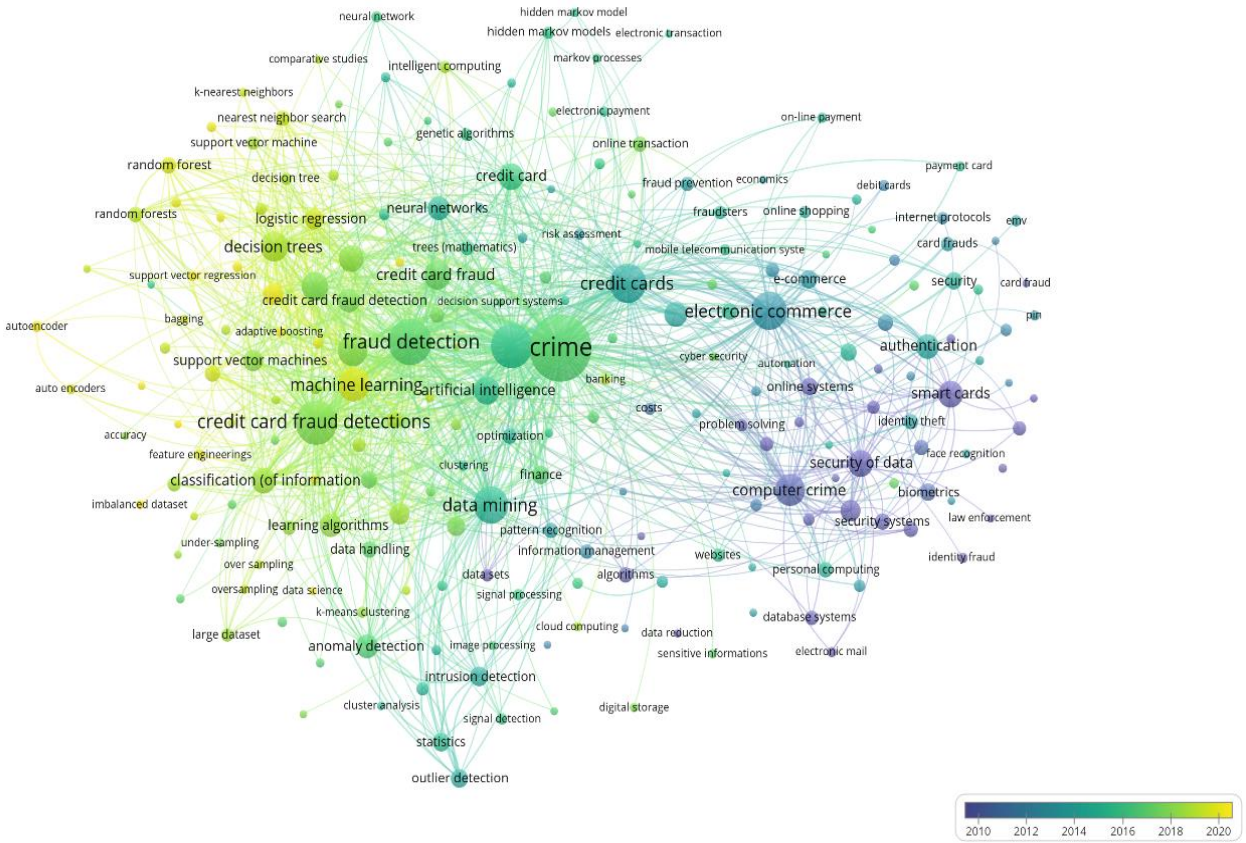

Рисунок 1.5 – Результати бібліометричного аналізу ключових слів,

що одночасно трапляються в публікаціях, проіндексованих наукометричною базою Scopus, за запитами «fraud» та «card» за допомогою інструментарію VOSviewer

На рисунку 1.5 представлено еволюцію публікації наукових публікації з досліджуваної проблематики протягом 2000–2021 років, що опублікована в наукометричній базі Scopus.

З 2010 року найбільш вживаними у наукових роботах поняттями були ті, що пов’язані з захистом даних та комп’ютерними злочинами (фіолетовий, синій кольори). Приблизно з 2013–2014 року науковцями активно досліджувалася проблема електронних продажів, використання кредитних карток (зелений колір). Починаючи з 2018 р. досліджується проблема протидії банківським шахрайствам з використанням інструментарію штучного інтелекту алгоритмами штучного навчання.

Отже, проведений бібліометричний аналіз наукових публікацій підтвердив, по-перше, актуальність обраного напрямку дослідження, по-друге, необхідність пошуку способів протидії платіжному шахрайству з використанням інтелектуальних методів аналізу даних про фінансові транзакції.

1.3 Сучасні тенденції платіжного шахрайства в Україні та світі

Шахрайськи акти з використанням банківських платіжних карток це глобальна проблема, що стосується не тільки України. Так, за даними Європейського центрального банку, загальний об’єм транзакцій на 2019 рік становить 5,16 трильйонів євро, з яких шахрайськими визнано 1,87 мільярдів євро. У 2019 році обсяг шахрайських банківських транзакцій зріс на 3,4% у порівнянні з 2018 роком.

Загальна вартість банківських операцій з використанням платіжних карток в країнах Європейського Союзу зростала швидшими темпами

порівняно з банківськими шахрайствами, що призвело до незначного зменшення частки шахрайства в загальному обсязі з 0,037% у 2018 році до 0,036% у 2019 році [9] (рис. 1.6). Показники за 2018 і 2019 роки залишаються значно нижчими за максимум, зафіксований у 2015 році (0,042%).

Обсяг шахрайств CNP (операції без наявності картки) продовжує зростати, частка якого у 2019 р. становить 80% від загальної кількості шахрайства. Натомість зафіксовано зниження шахрайства в банкоматах та POS-терміналах до 5% і 15% від загальної вартості відповідно.

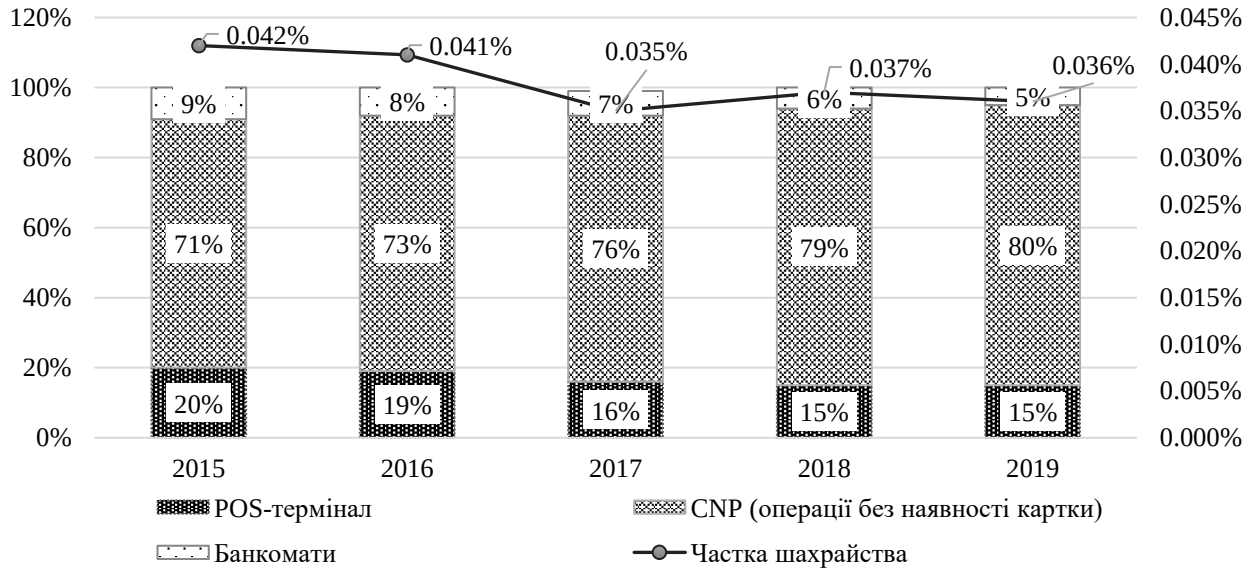

Рисунок 1.6 – Загальний об’єм шахрайств з платіжними картками на території SEPA протягом 2015-2019 рр.

Джерело: дані Європейського центрального банку [9].

У країнах Європейського Союзу кількість шахрайських операцій з банківськими картками у 2019 році зростала швидше, ніж відповідна їх вартість. У 2019 році середня вартість шахрайської операції знизилася на 10% у порівнянні з 2018 роком (рис. 1.7).

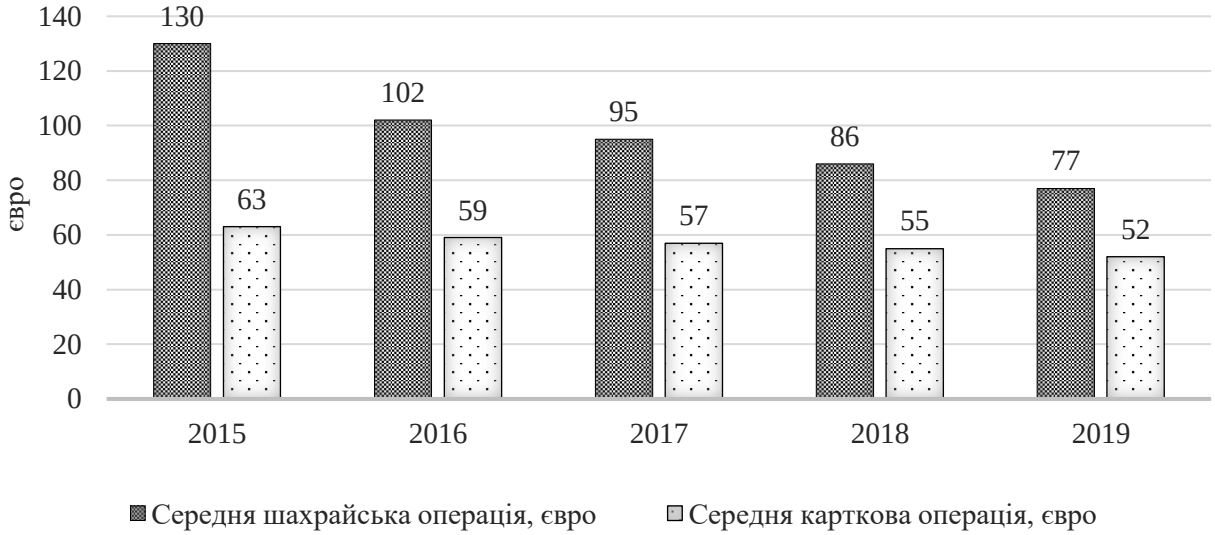

Рисунок 1.7 – Середній розмір усіх транзакцій, проведених за допомогою карток протягом 2015-2019 рр.

Джерело: дані Європейського центрального банку [9].

Щодо України, то кількість платіжних карток в обігу стабільно зростає з кожним роком та станом на листопад 2021 року становить 43,81 млн штук (рис. 1.8). Протягом 2011-2021 рр. середньорічний темп приросту обсягу операцій з використанням електронних платіжних засобів в Україні становив 22,96%. За 11 місяців 2021 року обсяг безготівкових операцій з використанням платіжних карток становив 2766 млрд грн, що на 25,22% більше, ніж за 12 місяців 2020 року.

Рисунок 1.8 – Динаміка кількості електронних платіжних засобів, емітованих українськими банками, та суми операцій за ними за період 2011 -2021 рр.

Джерело: дані Національного банку України [22].

За даними Національного банку України протягом останніх трьох років структура видів карток для проведення банківських платежів зазнала суттєвих змін (рис. 1.9). Протягом 2019-2021 рр. відбулися наступні зміни: зменшення кількості карток з магнітною смужкою на 35%; збільшення кількості безконтактних банківських карток на 22%, що можна пояснити збільшенням кількості POS-терміналів в країні. Випуск токенізованих карток збільшився з 1% до 6% за 2019-2020 рр. та досягнув 10% у 2021р.

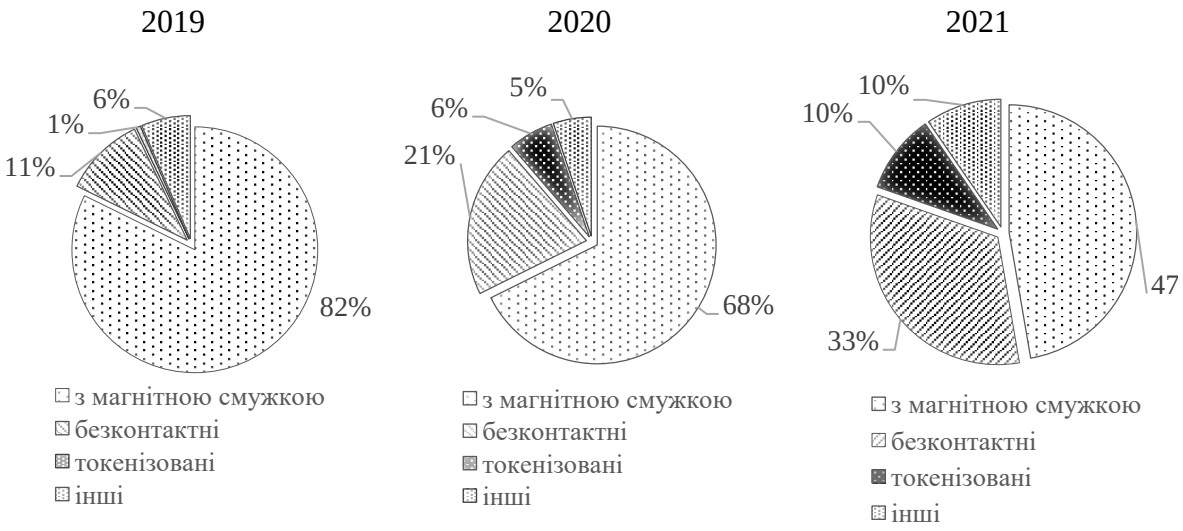

Рисунок 1.9 – Види платіжних карток в Україні протягом 2019-2021 рр. (станом на 1 січня кожного року)

Джерело: дані Національного банку України [22].

Середня сума однієї незаконної операції за 2020 рік у середньому складає 1900 грн, що на 10% менше, ніж у 2019 році. Кількість шахрайських дій з платіжними картками, навпроти, збільшився на 41% та складає 101 тис. шт. [14].

Динаміка питомої ваги сум збитку від шахрайства з платежами за способом здійснення (2019-2020 рр.):

– знизилась у торгівельній мережі з 0,0066% до 0,0061%;
– зросла в банкоматах з 0,0022% до 0,0033%;
– залишилась без змін в мережі Інтернет на рівні 0,0061%.

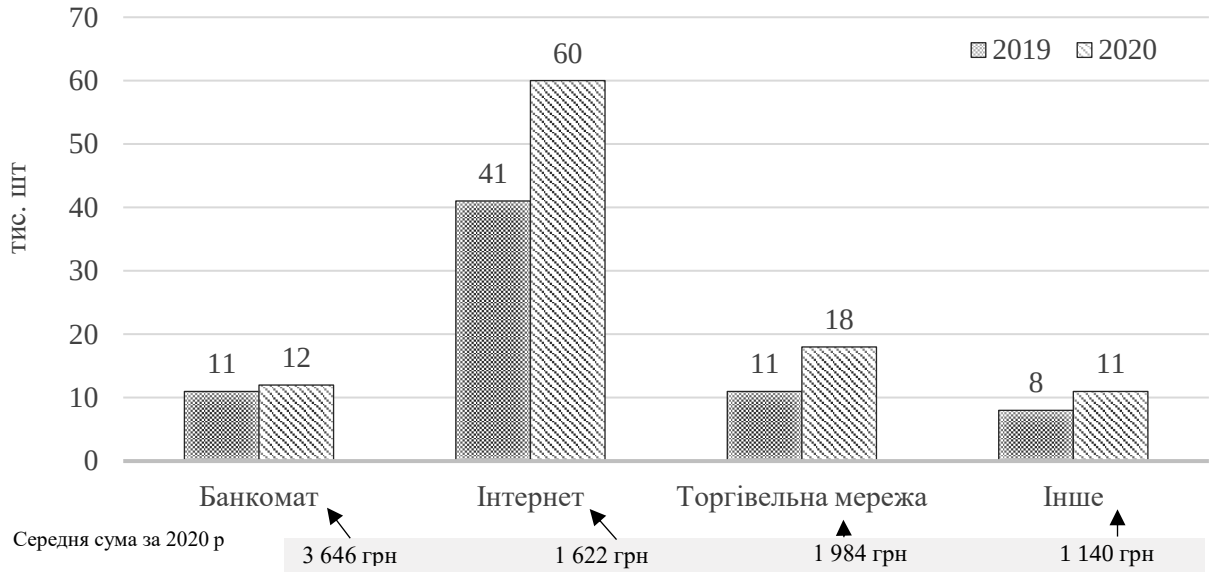

Рисунок 1.10 – Кількість збитків від незаконних дій з платіжними картками, тис. шт.

Джерело: дані Національного банку України [14].

Таким чином, проаналізувавши національні фінансові звіти, можна дійти до висновку, що чим більше безконтактних, токенізованих та інших видів карток випускається – тим більше ризик стати жертвою шахрая. На рисунку 1.10 зображена кількість збитків від шахрайства з банківськими платежами у тисячах штук. Наразі найбільше втрат несеться через Інтернет, далі – банкомати та торгівельні мережі. Середні суми, натомість, показують кардинально іншу картину: на банкомат припадає 3 646 грн середньої шахрайської операції, Інтернет – 1 622 грн, торгівельні мережі – 1 984 грн.

Ця статистика вказує на те, що питання шахрайства з банківськими платежами в Україні стоїть гостро, оскільки кількість та збитки від них зростають щорічно. У наступному розділі розглянемо шляхи удосконалення системи протидії незаконним діям з платіжними картками.

1.4 Постановка задач дослідження

Для побудови економіко математичної моделі ризику здійснення шахрайства з банківськими платежами було поставлено наступні задачі:

— провести описовий аналіз фінансових операцій, що мають ознаки шахрайства;

— провести кластеризацію та дисперсійний аналіз транзакцій з використанням електронних платіжних засобів;

— проаналізувати середні у кожному виділеному кластері;

— побудувати таблицю частот для визначення кластеру, що має найбільшу кількість шахрайських операцій з банківськими платежами.

РОЗДІЛ 2. УДОСКОНАЛЕННЯ СИСТЕМИ ПРОТИДІЇ ШАХРАЙСТВУ З ПЛАТІЖНИМИ КАРТКАМИ

2.1 Опис вхідних даних для моделювання ризику шахрайства з банківськими платіжними картками

Ключовим етапом економічного моделювання є підбір масиву даних для подальшого аналізу. Через конфіденційність банків для реалізації цього дослідження були обрані штучно створений масив даних для тренування та пошуку способів виявлення шахрайства з банківськими платіжними картками зі загальнодоступного ресурсу Kaggle [19].

Методом для аналізу обрано Data Mining (алгоритм k-середніх), оскільки його алгоритмами можна автоматично визначити оптимальну кількість кластерів, ідентифікувати кластери з найбільшим ризиком шахрайських операцій з використанням електронних платіжних засобів та працювати з великими об’ємами даних. Проведення розрахунків здійснюється програмним додатком Statistica. Об’єм вибірки складає 555 719 спостереження (2145 з них – шахрайські). У таблиці 2.1 наведені змінні, що використовуємо для аналізу.

Таблиця 2.1 – Змінні, що використовуються визначення ризиків шахрайства

№	Назва змінної	Пояснення
1	Категорія платежів /category	Вид категорій товарів/послуг, які були об’єктом фінансової транзакції. У базі зафіксовано 14.
2	Сума / amt	Сума транзакції, дол.США
3	Стать /gender	Стать особи, що проводила платіж (0 – жінка, 1 – чоловік)
4	Вік / birth	Вік особи, що проводила платіж
5	Час / time	Година проведення операції (від 0 до 23)
6	День / Week date	День тижня проведення операції (від 1 до 7)
7	fraud	Чи є операція шахрайською (0 – ні, 1 – так)

Для зручності аналізу категорії, за якими проводилися платежі було закодовано під цифрами від 1 до 14 (табл. 2.2).

Таблиця 2.2 – Кодування змінних категорій, за якими проведені транзакції

Код	Назва категорії	Переклад назви категорії
1	personal_care	Витрати на товари для краси та догляду
2	health_fitness	Витрати на здоров’я
3	misc_pos	Витрати на техніку проведені через POS-термінал
4	travel	Витрати на подорожі
5	kids_pets	Витрати на товари для дітей та тварин
6	shopping_pos	Витрати на одяг/взуття проведені через POS-термінал
7	food_dining	Витрати на продовольчі товари
8	home	Витрати на товари для дому
9	entertainment	Витрати на розважальні товари та послуги
10	shopping_net	Витрати на одяг/взуття проведені через інтернет
11	misc_net	Витрати на техніку проведені через інтернет
12	grocery_pos	Витрати на продовольчі товари проведені через POS-термінал
13	gas_transport	Витрати на оплату пального
14	grocery_net	Витрати на продовольчі товари проведені через POS-термінал

Частина масиву даних, взятого для дослідження представлена в додатку Б.

2.2 Основні елементи системи протидії шахрайству з банківськими платіжними картками

Ефективна боротьба з платіжним шахрайством потребує постійного удосконалення форм та методів протидії незаконним транзакціям, визначення вразливих місць в системі інформаційної безпеки фінансової установи, а також

запровадження комплексу превентивних заходів для зменшення кількості та частоти здійснення шахрайських операцій з банківськими картками.

Шахрайські дії з банківськими платіжними картками мають підвищену суспільну небезпеку, оскільки завдають збитків широкому колу осіб, що деструктивно впливає на рівень довіри до сфери банківських послуг та фінансової інклюзії. На сьогодні злочинність з використанням електронних платіжних засобів не має кордонів, а тому для ефективної протидії таким злочинним діям необхідно використовувати рекомендації міжнародних установ та співпрацювати з міжнародними компаніями. Саме тому вагому роль в протидії платіжному шахрайству є об'єднання зусиль фінансово-кредитних установ, а також регулюючих, наглядових та контролюючих органів влади. За умови злагодженої та спільної діяльності вищеперерахованих інституцій можна знизити ризик поширення шахрайств з платіжними засобами. Виходячи з цього, система протидії шахрайству з платіжними засобами має бути трирівневою, що включає співпрацю та взаємодію міжнародних організацій, органів державного управління, а також банківських установ та їх клієнтів (рис. 2.1). Ефективними способами боротьби з шахрайством у банківському секторі можуть бути узгоджені дії в таких сферах, як: управління банківською діяльністю (функціональна підсистема), управління інформаційно-комунікаційними технологіями (технологічна підсистема), нормативно-правове забезпечення (законодавча підсистема) та підвищення рівня цифрової та фінансової грамотності споживачів фінансових послуг (освітня підсистема).

Рисунок 2.1 – Ключові елементи системи протидії шахрайству з банківськими платіжними картками

Джерело: складено автором.

Освітня система полягає у розширенні знань щодо фінансової грамотності. Дана підсистема передбачає у собі не лише просвітницьку роботу від банківських установ, але і спеціальні предмети у навчальних закладах, тренінги для дітей. Саме таке спрямування дасть змоги виростити фінансово обізнаних громадян. Щодо більш старшого покоління, також пропонується створення інформаційних центрів, де буде змога проконсультуватися зі спеціалістом щодо будь-якої операції, яка може бути шахрайською. Пропонуємо поширювати інформацію про заходи, що можуть допомогти розпізнати банківську шахрайську операцію.

Законодавча підсистема включає в себе створення сучасного регулювання шахрайських банківських операцій, притягнення до відповідальності кримінально відповідальних осіб та надання відповідного покарання. Для здійснення цих пропозицій необхідно швидко та влучно

реагувати на будь-які зміни та «тенденції» до видів шахрайства з банківськими платежами, а також активно залучати міжнародних експертів до питань превентивної безпеки.

Функціональна підсистема більшою частиною полягає у тому, щоб вести повний моніторинг та аналіз за усіма видами платежів у розрізі таких систем як інтернет-банкінг, клієнт-банкінг тощо. Головною умовою є те, щоб аналіз та моніторинг включав себе дані по усім банкам для легкого у подальшому формування списків потенційних шахраїв.

Технологічна підсистема включає у себе застосування найбільш сучасних методів для виявлення шахрайства з банківськими операціями. Для стимулювання науковців, пропонуємо створювати матеріальні заходи для підвищення інтересу з даної теми на предмет дослідження сучасних методів аналізу шахрайства. Також, важливим є постійна підтримка належного рівня конфіденційності клієнтів, їх персональних даних.

2.3 Експрес-оцінка ризику шахрайства з використанням банківської платіжної картки

Формування системи забезпечення захисту банківських операцій від шахрайства має бути напрямлена, по-перше, на найбільш вразливі до атаки об‘єкти. Саме тому в рамках даної роботи пропонуємо провести аналіз бази даних на предмет виявлення чинників, що вливають на ризик здійснення незаконних дій з банківськими картками.

Оскільки за нашими даними таблиця включає в себе змінну «is fraud», то нам необхідно методом кластеризації дізнатися, у якому кластері найчастіше трапляється факт здійснення шахрайства.

Представимо описовий аналіз за допомогою графічного інтерфейсу. Більш детальніше проаналізуємо фінансові транзакції, що мають ознаки шахрайства у розрізі досліджуваних ознак. На рисунку 2.2 зображено

гістограми, які відображають кількість спостережень у відповідному параметрі, за якими зафіксовано факт шахрайства.

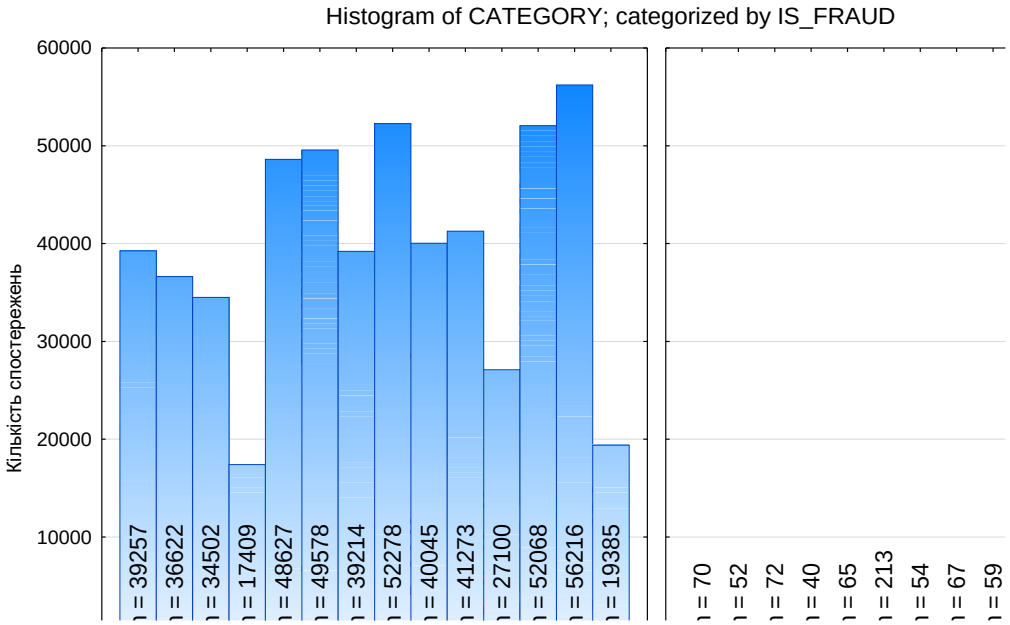

Рисунок 2.2 – Гістограма змінної «category», категоризована за ознакою «is fraud»

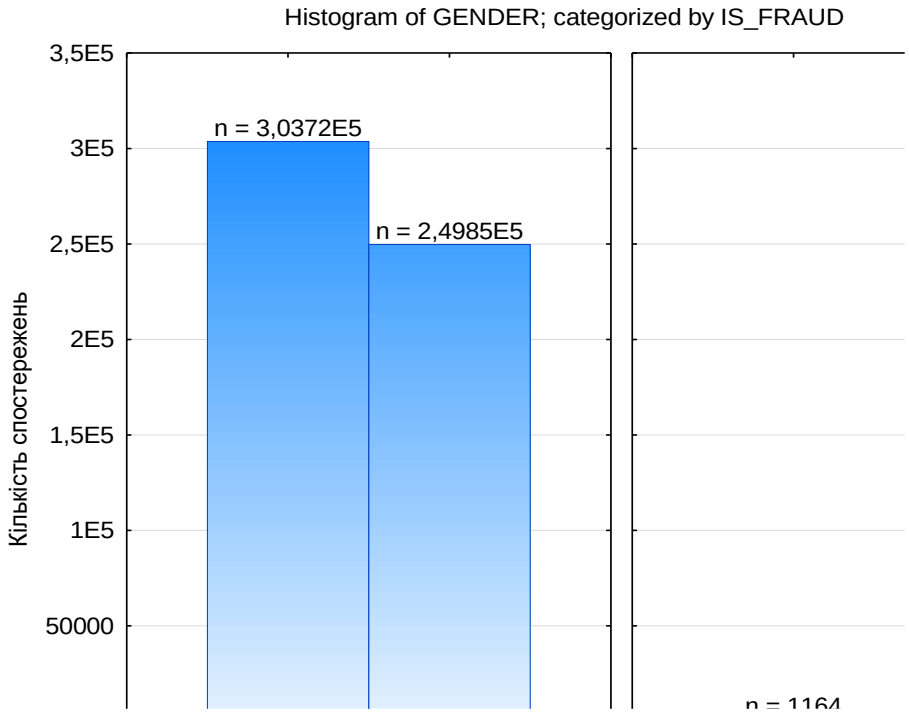

Рисунок 2.3 – Гістограма змінної «gender», категоризована за ознакою «is fraud»

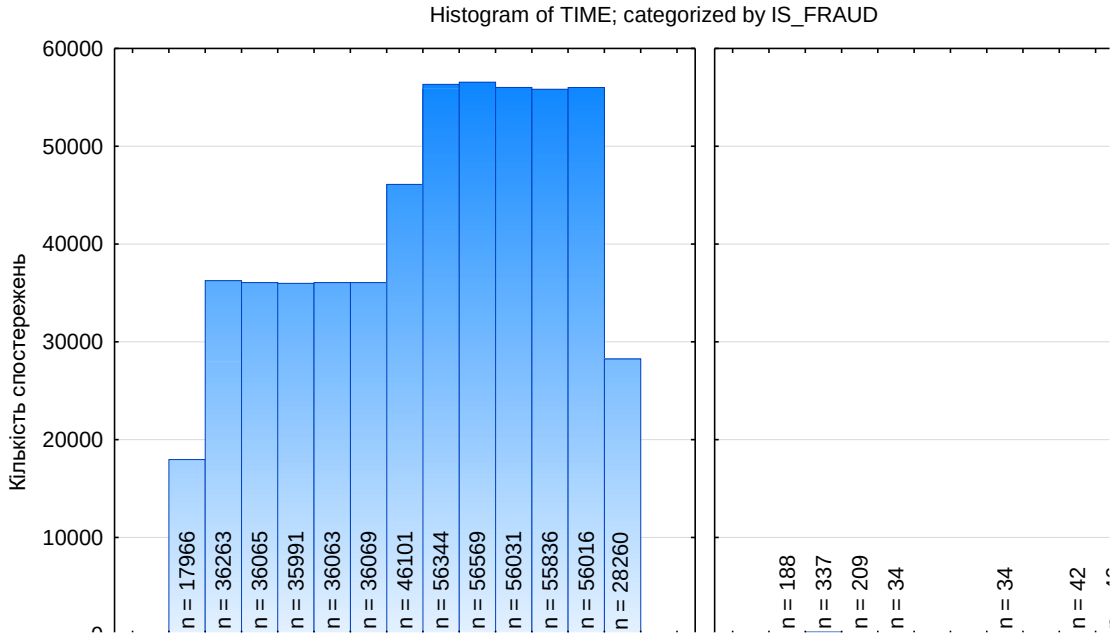

Рисунок 2.4 – Гістограма змінної «time», категоризована за ознакою «is fraud»

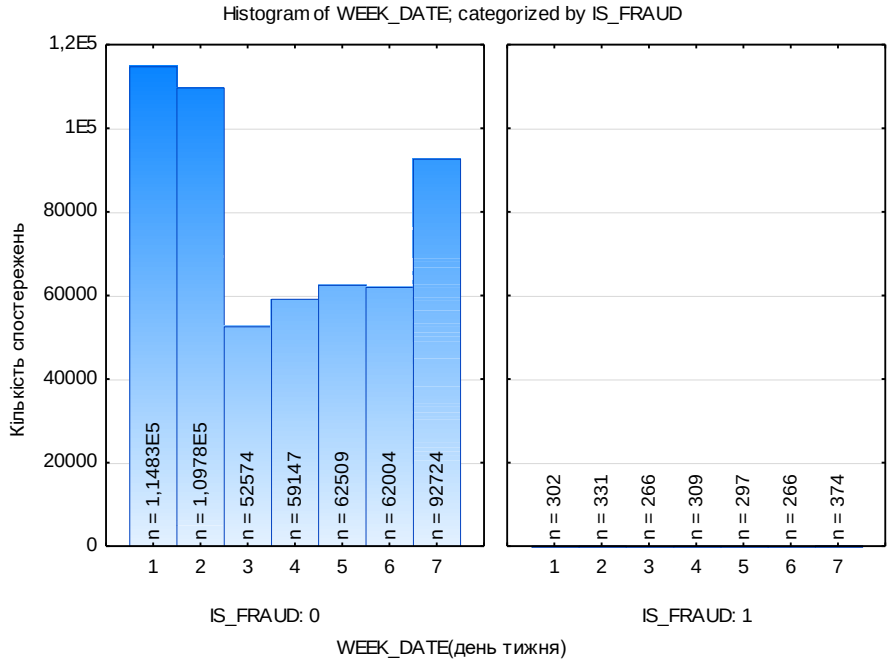

Рисунок 2.5 – Гістограма змінної «week_date», категоризована за ознакою «is fraud»

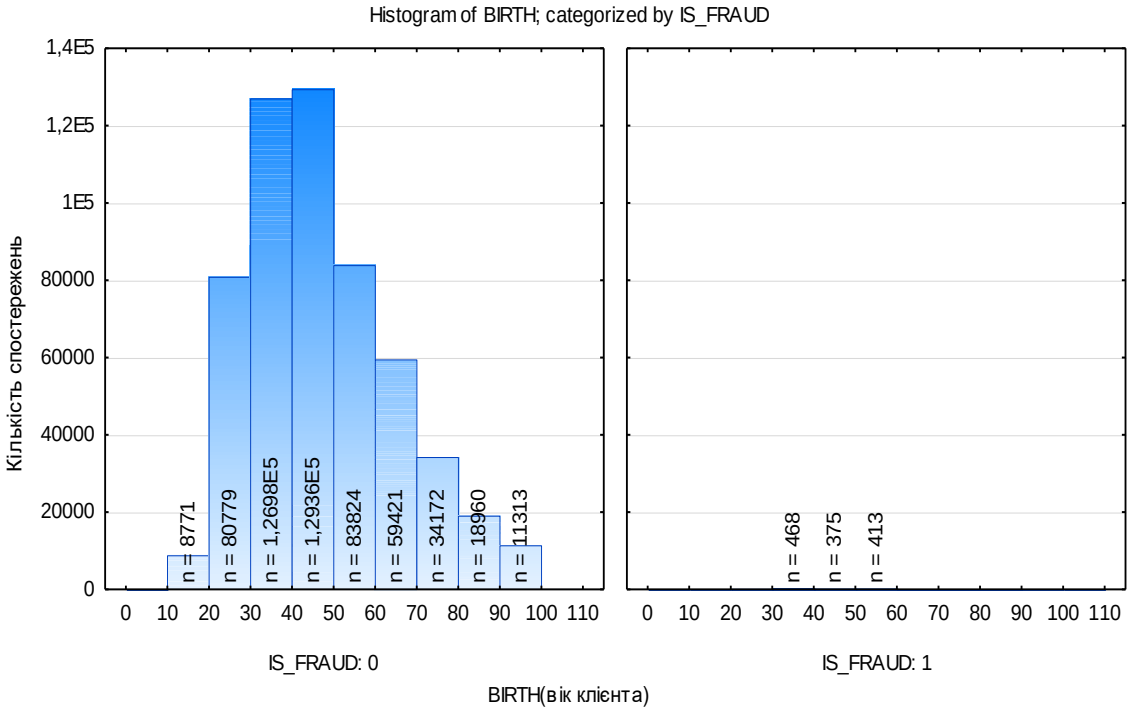

Рисунок 2.6 – Гістограма змінної «birth», категоризована за ознакою «is fraud»

Дані рисунку 2.5 наочно засвідчують, що найчастіше фінансові транзакції з використанням банківських платіжних карток здійснюється в неділю, хоча й варто відзначити майже рівномірний розподіл шахрайських операцій у розрізі днів тижня (неділя – 374 операції, вівторок – 331, четвер – 309, понеділок – 302, п’ятниця – 297, середа й субота – по 266).

Водночас більш детальне дослідження часу проведення незаконної фінансової транзакції дозволяє стверджувати, що майже чверть всіх шахрайських операцій з використанням банківсько картки проведено ввечері (з 22.00 до 23.00 – 550 операцій; з 23.00 до 24.00 – 538 операцій) (рис. 2.4).

Дані рисунку 2.3 демонструють, що 55% власників банківських карток, які містили ознаки шахрайства, були жінки. Найбільше незаконні транзакції проходить на купівлю продуктів та одягу (категорія 10 та 12, рисунок 2.2).

Наступним етапом дослідження є проведення кластеризації фінансових транзакцій з використанням електронних платіжних засобів через інструмент програмного додатку Statistica – Generalized Cluster Analysis. На рисунку 2.7

зображена область з основними характеристиками кластеризації. Кількість кластерів дорівнює 7 (найоптимальніша кількість для того, щоб виділити закономірності). На вкладці визначення параметрів було обрано Cross-validation (Перехресна валідація). Суть методу полягає в тому, що вибірка поділяється на частину для навчання моделі, а інша використовується для подальшого тестування. Даний метод допомагає отримати робочу модель, що зможе передбачувати шахрайські/не шахрайські операції на нових даних.

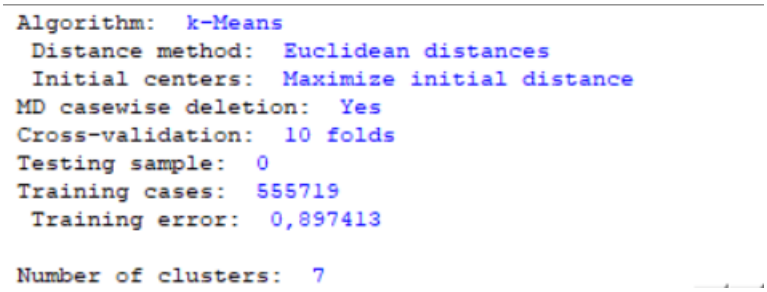

Рисунок 2.7 – Основні характеристики кластеризації

За результатами кластеризації (рис. 2.7) сформовано 7 кластерів. На рисунках 2.8-2.14 відображено зміст кластерів за показником евклідових відстаней.

Cluster members for cluster: 1 (fraudTest in Вихідні дані)
Number of cases: 113961

Case No.	CATEGORY	IS_FRAUD	GENDER	BIRTH	AMT	TIME	WEEK_DATE	Distance to centroid
2	1	0	0	32,00000	29,84	12,00000	7,000000	0,828749
8	1	0	0	49,00000	10,37	12,00000	7,000000	0,817572
20	1	0	0	24,00000	5,71	12,00000	7,000000	0,852040
30	1	0	0	64,00000	24,44	12,00000	7,000000	0,851671
67	1	0	0	36,00000	20,40	12,00000	7,000000	0,821322
94	1	0	0	35,00000	16,80	12,00000	7,000000	0,822908
108	1	0	0	29,00000	12,64	12,00000	7,000000	0,836193
119	1	0	0	50,00000	28,74	12,00000	7,000000	0,818585
123	1	0	0	51,00000	12,33	12,00000	7,000000	0,819787
129	1	0	0	57,00000	8,32	12,00000	7,000000	0,830811
130	1	0	0	66,00000	37,00	12,00000	7,000000	0,859135
170	1	0	0	46,00000	30,09	13,00000	7,000000	0,803690
183	1	0	0	37,00000	23,23	13,00000	7,000000	0,808033
185	1	0	0	46,00000	97,73	13,00000	7,000000	0,803690
189	1	0	0	50,00000	4,50	13,00000	7,000000	0,806682
275	1	0	0	62,00000	28,67	13,00000	7,000000	0,833331
279	1	0	0	26,00000	11,09	13,00000	7,000000	0,833670
288	1	0	0	33,00000	162,07	13,00000	7,000000	0,814844
336	1	0	0	45,00000	35,26	14,00000	7,000000	0,793666
338	1	0	0	31,00000	91,47	14,00000	7,000000	0,809772
361	1	0	0	74,00000	24,45	14,00000	7,000000	0,875486

Рисунок 2.8 – Зміст складових першого кластеру за показником евклідових відстаней (фрагмент)

Cluster members for cluster: 2 (fraudTest in Вихідні дані)
Number of cases: 42631

Case No.	CATEGORY	IS_FRAUD	GENDER	BIRTH	AMT	TIME	WEEK_DATE	Distance to centroid
1	1	0	1	53,00000	2,86	12,00000	7,000000	0,445719
28	1	0	1	53,00000	2,17	12,00000	7,000000	0,445719
31	1	0	1	91,00000	176,23	12,00000	7,000000	0,728357
33	1	0	1	57,00000	19,03	12,00000	7,000000	0,461370
37	1	0	1	26,00000	26,31	12,00000	7,000000	0,479977
56	1	0	1	28,00000	68,88	12,00000	7,000000	0,469471
74	1	0	1	53,00000	6,04	12,00000	7,000000	0,445718
77	1	0	1	32,00000	74,52	12,00000	7,000000	0,451797
83	1	0	1	72,00000	21,57	12,00000	7,000000	0,556374
91	1	0	1	83,00000	19,73	12,00000	7,000000	0,651192
164	1	0	1	66,00000	68,79	13,00000	7,000000	0,491064
175	1	0	1	97,00000	8,04	13,00000	7,000000	0,775646
184	1	0	1	61,00000	51,05	13,00000	7,000000	0,458736
186	3	0	1	28,00000	2,13	13,00000	7,000000	1,094950
188	1	0	1	56,00000	31,94	13,00000	7,000000	0,432846
195	2	0	1	21,00000	77,33	13,00000	7,000000	1,113165
204	9	0	1	24,00000	49,49	13,00000	7,000000	1,104567
207	9	0	1	22,00000	61,47	13,00000	7,000000	1,110169
225	10	0	1	22,00000	119,15	13,00000	7,000000	1,110171
250	10	0	1	21,00000	34,11	13,00000	7,000000	1,113167

Рисунок 2.9 – Зміст складових другого кластеру за показником евклідових відстаней (фрагмент)

Cluster members for cluster: 3 (fraudTest in Вихідні дані)
Number of cases: 74051

Case No.	CATEGORY	IS_FRAUD	GENDER	BIRTH	AMT	TIME	WEEK_DATE	Distance to centroid
11	7	0	1	25,00000	7,01	12,00000	7,000000	0,856574
14	7	0	1	84,00000	7,93	12,00000	7,000000	0,909517
36	7	0	1	63,00000	82,32	12,00000	7,000000	0,819944
75	7	0	1	44,00000	15,49	12,00000	7,000000	0,804980
81	7	0	1	54,00000	20,87	12,00000	7,000000	0,804409
84	7	0	1	41,00000	19,06	12,00000	7,000000	0,808833
85	7	0	1	36,00000	60,07	12,00000	7,000000	0,818944
89	7	0	1	54,00000	56,30	12,00000	7,000000	0,804407
92	7	0	1	44,00000	128,33	12,00000	7,000000	0,804982
97	7	0	1	56,00000	16,06	12,00000	7,000000	0,806566
117	7	0	1	39,00000	57,53	12,00000	7,000000	0,812329
120	7	0	1	24,00000	1,92	12,00000	7,000000	0,860976
146	7	0	1	22,00000	8,57	13,00000	7,000000	0,877113
150	7	0	1	61,00000	6,96	13,00000	7,000000	0,822547
157	7	0	1	26,00000	2,89	13,00000	7,000000	0,859347
191	7	0	1	46,00000	45,95	13,00000	7,000000	0,810789
211	7	0	1	24,00000	155,02	13,00000	7,000000	0,867930
212	7	0	1	30,00000	72,76	13,00000	7,000000	0,844096
230	7	0	1	51,00000	10,62	13,00000	7,000000	0,810039
240	7	0	1	31,00000	11,18	13,00000	7,000000	0,840697

Рисунок 2.10 – Зміст складових третього кластеру за показником евклідових відстаней (фрагмент)

Cluster members for cluster: 4 (fraudTest in Вихідні дані)
Number of cases: 78800

Case No.	CATEGORY	IS_FRAUD	GENDER	BIRTH	AMT	TIME	WEEK_DATE	Distance to centroid
4	3	0	1	34,00000	60,05	12,00000	7,000000	1,074669
5	4	0	1	66,00000	3,19	12,00000	7,000000	1,071092
9	6	0	1	48,00000	4,37	12,00000	7,000000	1,055059
17	6	0	1	34,00000	2,33	12,00000	7,000000	1,074672
23	4	0	1	50,00000	1,74	12,00000	7,000000	1,054543
27	2	0	1	64,00000	1,70	12,00000	7,000000	1,067039
40	9	0	1	52,00000	105,78	12,00000	7,000000	1,054602
42	8	0	1	46,00000	47,81	12,00000	7,000000	0,339783
47	8	0	1	42,00000	84,11	12,00000	7,000000	0,351750
51	8	0	1	47,00000	80,50	12,00000	7,000000	0,337853
53	9	0	1	45,00000	79,51	12,00000	7,000000	1,056912
62	8	0	1	39,00000	55,53	12,00000	7,000000	0,364878
63	2	0	1	23,00000	2,61	12,00000	7,000000	1,108898
69	8	0	1	58,00000	30,72	12,00000	7,000000	0,346250
73	10	0	1	36,00000	5,37	12,00000	7,000000	1,070185
76	10	0	1	32,00000	4,94	12,00000	7,000000	1,079706
86	9	0	1	43,00000	15,80	12,00000	7,000000	1,058871
87	3	0	1	35,00000	2,01	12,00000	7,000000	1,072360
88	9	0	1	47,00000	75,24	12,00000	7,000000	1,055530
90	9	0	1	51,00000	5,95	12,00000	7,000000	1,054501
99	9	0	1	50,00000	6,88	12,00000	7,000000	1,054543

Рисунок 2.11 – Зміст складових четвертого кластеру за показником евклідових відстаней (фрагмент)

Cluster members for cluster: 5 (fraudTest in Вихідні дані)
Number of cases: 70481

Case No.	CATEGORY	IS_FRAUD	GENDER	BIRTH	AMT	TIME	WEEK_DATE	Distance to centroid
295	12	0	0	26,00000	88,940	13,00000	7,000000	0,824631
1216	12	0	0	22,00000	51,560	19,00000	7,000000	0,982833
1471	12	0	0	17,00000	31,620	20,00000	7,000000	1,035890
1673	12	0	0	24,00000	49,670	22,00000	7,000000	1,059732
1748	12	0	0	26,00000	50,840	22,00000	7,000000	1,051417
2030	14	0	0	62,00000	99,940	0,00000	1,000000	1,081760
2031	11	0	0	52,00000	325,610	0,00000	1,000000	1,077279
2034	7	0	0	58,00000	68,390	0,00000	1,000000	1,078257
2041	14	0	0	45,00000	66,390	0,00000	1,000000	1,082463
2043	12	0	1	41,00000	48,330	0,00000	1,000000	1,088526
2045	12	0	1	39,00000	108,200	0,00000	1,000000	1,092380
2046	14	0	0	49,00000	54,070	0,00000	1,000000	1,078631
2048	3	0	0	40,00000	16,150	0,00000	1,000000	1,090390
2050	11	0	0	36,00000	432,310	0,00000	1,000000	1,099278
2051	11	0	0	68,00000	5,200	0,00000	1,000000	1,091200
2052	3	0	0	53,00000	6,390	0,00000	1,000000	1,077056
2053	6	0	0	72,00000	4,730	0,00000	1,000000	1,100217
2059	11	0	0	28,00000	8,970	0,00000	1,000000	1,123101
2062	11	0	0	68,00000	15,720	0,00000	1,000000	1,091198
2064	14	0	0	43,00000	78,540	0,00000	1,000000	1,085217
2065	12	0	0	44,00000	240,090	0,00000	1,000000	0,417848

Рисунок 2.12 – Зміст складових п’ятого кластеру за показником евклідових відстаней (фрагмент)

Cluster members for cluster: 6 (fraudTest in Вихідні дані)
Number of cases: 54220

Case No.	CATEGORY	IS_FRAUD	GENDER	BIRTH	AMT	TIME	WEEK_DATE	Distance to centroid
12	5	0	1	45,00000	42,40	12,00000	7,000000	0,758413
39	5	0	1	41,00000	36,72	12,00000	7,000000	0,760643
43	5	0	1	47,00000	18,96	12,00000	7,000000	0,758504
45	5	0	1	78,00000	30,59	12,00000	7,000000	0,856352
64	5	0	1	84,00000	1,93	12,00000	7,000000	0,893176
71	5	0	1	41,00000	5,13	12,00000	7,000000	0,760647
103	5	0	1	76,00000	127,76	12,00000	7,000000	0,845167
154	5	0	1	80,00000	49,07	13,00000	7,000000	0,855104
179	5	0	1	70,00000	38,88	13,00000	7,000000	0,801329
220	5	0	1	62,00000	155,28	13,00000	7,000000	0,769953
236	5	0	1	53,00000	169,09	13,00000	7,000000	0,748783
253	5	0	1	83,00000	20,89	13,00000	7,000000	0,873999
256	5	0	1	55,00000	140,88	13,00000	7,000000	0,752116
302	5	0	1	52,00000	103,86	13,00000	7,000000	0,747402
303	5	0	1	24,00000	16,10	13,00000	7,000000	0,790574
305	5	0	1	39,00000	45,19	13,00000	7,000000	0,748140
310	5	0	1	73,00000	84,17	13,00000	7,000000	0,815873
357	5	0	1	55,00000	68,35	14,00000	7,000000	0,739637
365	5	0	1	27,00000	17,91	14,00000	7,000000	0,766717
383	5	0	1	39,00000	55,30	14,00000	7,000000	0,735599
391	5	0	1	49,00000	8,92	14,00000	7,000000	0,731909

Рисунок 2.13 – Зміст складових шостого кластеру за показником евклідових відстаней (фрагмент)

Cluster members for cluster: 7 (fraudTest in Вихідні дані)
Number of cases: 121575

Case No.	CATEGORY	IS_FRAUD	GENDER	BIRTH	AMT	TIME	WEEK_DATE	Distance to centroid
3	2	0	0	51,00000	41,28	12,00000	7,000000	1,033396
6	5	0	0	30,00000	19,55	12,00000	7,000000	1,053394
7	2	0	0	71,00000	133,93	12,00000	7,000000	1,073851
10	7	0	0	65,00000	66,54	12,00000	7,000000	1,055827
13	8	0	0	45,00000	2,91	12,00000	7,000000	1,032531
15	5	0	0	50,00000	2,91	12,00000	7,000000	1,032886
16	9	0	0	33,00000	24,73	12,00000	7,000000	1,046636
18	5	0	0	29,00000	16,60	12,00000	7,000000	1,055926
19	9	0	0	44,00000	80,11	12,00000	7,000000	1,032899
21	4	0	0	24,00000	8,53	12,00000	7,000000	1,070633
22	5	0	0	29,00000	37,95	12,00000	7,000000	1,055925
24	4	0	0	24,00000	6,02	12,00000	7,000000	1,070634
25	6	0	0	36,00000	9,87	12,00000	7,000000	1,041154
26	7	0	0	30,00000	47,06	12,00000	7,000000	1,053393
29	4	0	0	73,00000	6,21	12,00000	7,000000	1,080918
32	8	0	0	47,00000	134,39	12,00000	7,000000	1,032231
34	9	0	0	47,00000	210,36	12,00000	7,000000	1,032246
35	8	0	0	57,00000	52,81	12,00000	7,000000	1,039556
38	5	0	0	52,00000	134,60	12,00000	7,000000	1,034061
41	8	0	0	44,00000	39,95	12,00000	7,000000	1,032899
44	9	0	0	60,00000	46,67	12,00000	7,000000	1,044594

Рисунок 2.14 – Зміст складових сьомого кластеру за показником евклідових відстаней (фрагмент)

Проаналізуємо середні в кожному кластері (рис. 2.15).

Centroids for k-means clustering (fraudTest in Вихідні дані)
Number of clusters: 7
Total number of training cases: 555719

Cluster	CATEGORY	IS_FRAUD	GENDER	BIRTH	AMT	TIME	WEEK_DATE	Number of cases	Percentage(%)
1	1	0	0	44,05129	60,61678	17,61803	2,333009	113961	20,50695
2	1	0	1	43,35369	72,00378	18,18580	4,990758	42631	7,67132
3	7	0	1	49,30110	63,70660	9,32262	2,237066	74051	13,32526
4	8	0	1	50,78766	68,51402	9,92598	5,066675	78800	14,17983
5	12	0	0	53,79333	96,69198	4,99627	3,014699	70481	12,68285
6	5	0	1	45,77870	70,65206	18,42139	2,769476	54220	9,75673
7	13	0	0	47,01865	64,34890	12,43412	5,468707	121575	21,87706

Рисунок 2.15 – Середні значення ознак в кожному кластері

Кластер 1: Оплати переважно за категорією «Витрати на товари для краси та догляду»; жінки, середній вік – 44; середня сума транзакції – 60,62. Операції здійснені переважно з 17 до 18 вечора у вівторок.

Кластер 2: Оплати за категорією «Витрати на товари для краси та догляду», чоловіки (середній вік 43), середня сума транзакції – 72. Операції здійснені переважно о 18 годині у четвер.

Кластер 3: Оплати за категорією «Витрати на продовольчі товари» , чоловіки (середній вік 49), середня сума транзакції – 63,7. Операції здійснені переважно з 9 до 10 години ранку у вівторок.

Кластер 4: Оплати за категорією «Товари для дому», чоловіки (середній вік 51), середня сума транзакції – 68,5. Операції здійснені переважно з 9 до 10 години у п’ятницю.

Кластер 5: Оплати за категорією «Витрати на продовольчі товари проведені через POS-термінал», жінки (середній вік 54), середня сума транзакції – 96,7. Операції здійснені переважно о 5 годині у середу.

Кластер 6: Оплати за категорією «Витрати на товари для дітей та тварин», чоловіки (середній вік 45), середня сума транзакції – 70,6. Операції здійснені переважно з 18 до 19 години у середу.

Кластер 7: Оплати за категорією «Витрати на оплату пального», жінки (середній вік 47), середня сума транзакції – 64,34. Операції здійснені переважно о 12 годині у п’ятницю.

Standardized distance between centroids of k-means clustering (fraudTest in Вихідні дані)
Number of clusters: 7

	Cluster 1	Cluster 2	Cluster 3	Cluster 4	Cluster 5	Cluster 6	Cluster 7
Cluster 1	0,000000	1,094027	1,461006	1,525236	1,152618	1,416675	1,151203
Cluster 2	1,094027	0,000000	1,168129	1,066561	1,566504	1,066799	1,439072
Cluster 3	1,461006	1,168129	0,000000	1,106089	1,433617	1,079937	1,519603
Cluster 4	1,525236	1,066561	1,106089	0,000000	1,471149	1,134391	1,420756
Cluster 5	1,152618	1,566504	1,433617	1,471149	0,000000	1,533678	1,130866
Cluster 6	1,416675	1,066799	1,079937	1,134391	1,533678	0,000000	1,506779
Cluster 7	1,151203	1,439072	1,519603	1,420756	1,130866	1,506779	0,000000

Рисунок 2.16 – Евклідові відстані та квадрати евклідових відстаней між сформованими кластерами

Проведемо дисперсійний аналіз для визначення факторів, що впливають на приналежність об’єкта кластеру. Дані на рисунку 2.17 характеризують значення міжгрупових (Between SS) та внутрішньогрупових (Within SS) дисперсійних ознак. Чим менше значення Within SS та більше значення Between SS, тим краще окрема характеристика транзакцій характеризує приналежність кожного окремого платежу до певного кластеру. Більше значення F-критерію (критерію Фішера) та менше значення p-value (рівня значущості) відповідає кращій кластерізації.

На основі значень критерія Фішера та близькості p-рівня значущості до нуля можна зробити висновок, що різниця між середніми за кожною групою та середньому в цілому статистично значуща.

ANOVA for continuous variables (fraudTest in Вихідні дані)
Number of clusters: 7
Total number of training cases: 555719

	Between SS	df	Within SS	df	F	p value
BIRTH	6137016	6	1,627060E+08	555712	3493,43	0,00
AMT	67227475	6	1,358637E+10	555712	458,29	0,00
TIME	11450096	6	1,432880E+07	555712	74011,28	0,00
WEEK_DATE	1049621	6	1,588179E+06	555712	61211,30	0,00

Рисунок 2.17 – Дисперсійний аналіз

Для того, щоб все таки виявити чинники, що найбільше впливають на вірогідність шахрайства побудуємо таблицю частот (рис. 2.10).

Frequency table for categorical variable: IS_FRAUD (fraudTest in Вихідні дані)
Number of clusters: 7
Total number of training cases: 555719

	Cluster 1	Cluster 2	Cluster 3	Cluster 4	Cluster 5	Cluster 6	Cluster 7	Total
0	113630	42332	73949	78629	69996	53895	121143	553574
1	331	299	102	171	485	325	432	2145

Рисунок 2.18 – Таблиця частот для категоріальної змінної «is fraud»

Frequency table for categorical variable: CATEGORY (fraudTest in Вихідні дані)
Number of clusters: 7
Total number of training cases: 555719

	Cluster 1	Cluster 2	Cluster 3	Cluster 4	Cluster 5	Cluster 6	Cluster 7	Total
1	24080	15247	0	0	0	0	0	39327
2	10859	6429	2187	1954	138	6676	8431	36674
3	4942	2952	5377	5176	6522	2704	6901	34574
4	4833	3239	1075	974	92	3437	3799	17449
5	10527	0	0	0	205	27215	10745	48692
6	11934	4174	6586	6278	5690	3831	11298	49791
7	9136	0	20398	0	1056	0	8678	39268
8	15464	0	0	25713	188	0	10980	52345
9	9571	6322	3627	3233	2501	6355	8495	40104
10	9706	3111	6077	5889	4716	2912	9368	41779
11	2216	932	5072	5060	7627	870	5590	27367
12	0	225	6743	9987	35378	220	0	52553
13	0	0	12648	10303	0	0	33419	56370
14	693	0	4261	4233	6368	0	3871	19426

Рисунок 2.19 – Таблиця частот для категоріальної змінної «category»

Frequency table for categorical variable: GENDER (fraudTest in Вихідні дані)
Number of clusters: 7
Total number of training cases: 555719

	Cluster 1	Cluster 2	Cluster 3	Cluster 4	Cluster 5	Cluster 6	Cluster 7	Total
0	113961	0	1976	964	62930	5606	119449	304886
1	0	42631	72075	77836	7551	48614	2126	250833

Рисунок 2.20 – Таблиця частот для категоріальної змінної «gender»

На основі рисунку 2.18 можемо зробити висновок, що операції, занесені до кластеру 5 та 7 мають найбільший ризик бути шахрайськими (485 та 432 шахрайських операцій занесені в ці кластери тобто 42,7% з усіх). Тобто найбільший ризик мають такі транзакції: проведені переважно за категоріями: Кластер 5: Оплати за категорією «Витрати на продовольчі товари проведені через POS-термінал», жінки (середній вік 54), середня сума транзакції – 96,7. Операції здійснені переважно о 5 годині у середу. Кластер 7: Оплати за

категорією «Витрати на оплату пального», жінки (середній вік 47), середня сума транзакції – 64,34. Операції здійснені переважно о 12 годині у п’ятницю.

Даний аналіз не може бути використаний як комплексна та повна оцінка ризику здійснення шахрайства з банківськими платежами. Цей метод доцільно використовувати для експрес-оцінки діяльності банківської установи.

2.3 Рекомендації щодо удосконалення системи протидії платіжному шахрайству

Враховуючи пункт 2.1 та 2.2 даної роботи, пропонуємо такі заходи до удосконалення існуючої системи протидії шахрайству з платіжними картками:

– створення нової небанківської установи, основним завдання якої буде збирання та аналіз інформації щодо транзакцій кожного суб’єкта платіжної системи з усіх банківських установ. За допомогою такої системи, навіть якщо шахрай одночасно діє з кількох банків, буде можливість зібрати повний ланцюг факторів, що вказують на шахрайство та запобігти його скоєнню.

– посилити відповідальність за скоєння акту шахрайства з платіжними картками, а також активна співпраця з кіберполіцією;

– встановити один стандарт посиленої аутентифікації для користувачів банківських установ на законодавчому рівні;

– розвиток в Україні концепції відкритого банкінгу [20], що передбачає відкриття усіма надавачами платіжних послуг своїх API для запровадження відкритого доступу до обміну інформацією щодо банківських сервісів між учасниками ринку;

– постійна розробка методів аналізу транзакцій, зокрема таких, як Data Mining (пункт 2.2), методом який на основі тестового набору даних дозволив нам визначити, що найбільш вразливими до скоєння шахрайства є такі клієнти банків: чоловіки віком приблизно 47 років, платежі здійснюються за категорією «Оплата пального», орієнтовний час – 12 година дня, день тижня – четвер.

Таким чином, до проблеми шахрайства з платіжними картками необхідно підходити комплексно, на рівні держави із застосуванням сучасних методологій аналізу даних та залученням іноземних експертів.

ВИСНОВКИ

Дане дослідження було спрямоване на виявлення основних тенденцій розвитку причин і наслідків банківського шахрайства, особливостей і способів вчинення таких злочинів. З метою визначення ефективних шляхів боротьби з банківським шахрайством були проаналізовані статистичні дані національних та іноземних організацій, наукових видань вітчизняних та іноземних науковців. На цій основі було визначено основі види шахрайства з банківськими платежами: шахрайства з банкоматом, Інтернет шахрайство, шахрайство в термінальних мережах, системах дистанційного обслуговування, соціальний інжиніринг.

У процесі дослідження було виявлено, що на ступінь шахрайства прямо впливають такі чинники, як: низький рівень цифрової та фінансової грамотності; відсутність стандартизованої системи аутентифікації клієнтів; великий об’єм даних про фінансовий стан, діяльність клієнтів; відносно низька ефективність системи контролю за інформаційною безпекою банків.

Щодо України, був зафіксований стабільний ріст обсягів операцій з використанням електронних платежів, а саме в період 2011-2021рр. середньорічній приріст становив 22, 96%. Кількість збитків від незаконних дій з платіжними картками через Інтернет у 2020 році зросла у порівнянні з 2019 роком на 19 тис. шт. (+46,34% – найбільший ріст серед інших видів шахрайства з платежами). Середня сума однієї незаконної операції у 2020 році склала 1900 грн.

За результатами аналізу сучасного стану та тенденцій у фінансовому секторі були виявлені такі підсистеми, що складають загальну систему протидії шахрайству з банківськими платежами, як: управління банківською діяльністю (функціональна підсистема), управління інформаційно-комунікаційними технологіями (технологічна підсистема), нормативно-

правове забезпечення (законодавча підсистема) та підвищення рівня цифрової та фінансової грамотності споживачів фінансових послуг (освітня підсистема).

У кваліфікаційній роботі було реалізовано моделювання ризику здійснення шахрайства з банківськими платежами засобами методу Data Mining. Для цього було сформовано вхідний масив даних з характеристик банківських транзакцій (категорія платежів, вік клієнта, стать, сума платежу, день та час проведення транзакції, чи є транзакція шахрайською). Кількість спостережень 555 719 значень (2145 з них – шахрайські). Усі транзакції було розділено на 7 кластерів, у двох з яких було зафіксовано найбільшу кількість шахрайських операцій (у сумі 44% з 2145 операцій). Найбільший ризик з вибірки мають такі транзакції: кластер 5 – оплати за категорією «Витрати на продовольчі товари проведені через POS-термінал», жінки (середній вік 54), середня сума транзакції – 96,7, операції здійснені переважно о 5 годині у середу; кластер 7 – оплати за категорією «Витрати на оплату пального», жінки (середній вік 47), середня сума транзакції – 64,34, операції здійснені переважно о 12 годині у п’ятницю.

Із основних заходів, що дозволять удосконалити систему протидії можна виокремити: створення окремих органів аналізу та регулювання шахрайства в банківському секторі, посилення відповідальності за скоєння шахрайства на законодавчому рівні, встановлення єдиного стандарту системи аутентифікації для клієнтів, розвиток в Україні системи відкритого банкінгу, активне залучення сучасних науковців з сучасними методологіями аналізу великих об’ємів даних на предмет виявлення шахрайства.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Agwu, E. M. Cyber criminals on the internet superhighways: A technical investigation of different shades and colors within the Nigerian cyber space: International Journal of Online Marketing. 2013. P. 56–74.

2. Bhasin, M. Frauds in the Banking Sector: Experience of a Developing Country. Asian Journal of Social Sciences and Management Studies. 2016. P. 69-80 c.

3. Dal Pozzolo A., Boracchi G., Caelen O., Alippi C., Bontempi G. Credit Card Fraud Detection: A Realistic Modeling and a Novel Learning Strategy. IEEE Transactions on Neural Networks and Learning Systems. 2017. P. 1–14.

4. Global Payment Fraud Statistics, Trends & Forecasts. Merchant Savvy: веб-сайт. URL: https://www.merchantsavvy.co.uk/payment-fraud-statistics/ (дата звернення 25.04.2022).

5. Li Y. and Zhang X. Securing Credit Card Transactions with One-Time Payment Scheme. Electronic Commerce Research and Applications. 2005. №4, (4), P. 413–426.

6. Nafchi A. R., Dastgir, M. Identification and Ranking of Risk Factors Affecting the Probability of Bank Fraud (Case Study, Isfahan Province Resalat Bank): International journal of Business Management. 2019. №4 (4), P. 50–64. URL: https://inlnk.ru/20Qk5d (дата звернення: 27.05.2022).

7. Omar N. B., Faizal H., Din M. Fraud Diamond Risk Indicator. An Assessment of Its Importance and Usage: CSSR 2010. P. 607-612.

8. Sanusia Z. M., Ramelib M., Nor F., Isab Y. M. Fraud Schemes in the Banking Institutions: Prevention Measures to Avoid Severe Financial Loss. Procedia Economics and Finance. 2015. P. 107–113.

9. Seventh report on card fraud. European Central Bank, 2019. URL: https://www.ecb.europa.eu/pub/pdf/cardfraud/ecb.cardfraudreport202110~cac4c418e8.en.pdf (дата звернення 21.05.2022).

10. Shanmugam M., Wang Y.-Y., Bugshan H., Hajli N. Understanding customerperceptions of internet banking: the case of the UK, Journal of Enterprise Information Management, 2015. Vol. 28. P. 622 – 636.

11. Vitvitskiy S. S., Kurakin O. N., Pokataev P. S., Skriabin O. M., Sanakoiev D. B. Peculiarities of cybercrime investigation in the banking sector of Ukraine: review and analysis. Banks and Bank Systems, 2021, 16(1).

12. Vitvitskiy S. S., Kurakin O. N., Pokataev P. S., Skriabin O. M., Sanakoiev D. B. Formation of a new paradigm of anti-money laundering : The experience of Ukraine. Problems and Perspectives in Management, 2021. P. 354-363.

13. Worldwide research economic crimes and fraud 2020. PwC : веб-сайт. URL: https://www.pwc.com/ua/uk/survey/2020/economic-crime-survey.html (дата звернення 24.05.2022).

14. Аналіз ринку платіжних карток та шахрайських операцій з їх використанням. URL: https://docs.google.com/presentation/d/1B3jtIWzbAJQngatOnIMwWcyvHfMnuDv3/edit#slide=id.p5 (дата звернення 17.05.2022).

15. Афанасенко С. І. Віктимологічна профілактика шахрайства: автореф. дис. канд. юр. наук: 12.00.08. Київ. С. 18.

16. Боженко В. В., Кушнерьов О. С., Кільдей А. Д. Детермінанти поширення кіберзлочинності у сфері фінансових послуг. Економічний форум. 2021. № 4. С. 166-121. URL: https://doi.org/10.36910/6775-2308-8559-2021-4-16.

17. Довіра до інститутів суспільства та політиків, електоральні орієнтації громадян України (липень–серпень 2021р.) Разумков центр : веб-сайт. URL: https://inlnk.ru/1PLk89 (дата звернення 19.05.2022).

18. Криушенко Л. І. До питання класифікації способів шахрайства в банківській сфері. Вісник Харківського національного університету імені В. Н. Каразіна. Право. 2015. С. 261–266. URL: http://nbuv.gov.ua/UJRN/VKhIPR_2015_20_64 (дата звернення: 28.05.2022).

19. Набір даних для виявлення шахрайства транзакцій з кредитними картками. Kaggle : веб-сайт. URL: https://www.kaggle.com/kartik2112/fraud-detection?select=fraudTrain.csv (дата звернення 17.05.2022).

20. Нова якість платіжних послуг: Верховна Рада ухвалила сучасний закон про платіжні послуги. URL: https://bank.gov.ua/ua/news/all/nova-yakist-platijnih-poslug-verhovna-rada-uhvalila-suchasniy-zakon-pro-platijni-poslugi

21. Опитування про системні ризики фінансового сектору. Національний банк України. Листопад 2021 року. URL: https://bank.gov.ua/admin_uploads/article/Risk_Survey_2021-H2.pdf?v=4 (дата звернення 25.05.2022).

22. Платежі та розрахунки. Національний банк України : веб-сайт. URL: https://bank.gov.ua/ua/payments (дата звернення 27.05.2022).

23. Рекомендації для зниження ризику шахрайських операцій. Лист НБУ від 04.07.2018. № 57-0009/36366.

24. Родченко С. С., Живко, З. Б. Шахрайство в банківській системі України: способи боротьби із врахуванням зарубіжного досвіду. Науковий вісник Ужгородського національного університету. Міжнародні економічні відносини та світове господарство. 2020. Вип. 31. С. 103–108.

25. Сайт Національного банку України. URL: https://bank.gov.ua/ (дата звернення 25.05.2022).

26. Цифрова грамотність населення України. Міністерство цифрової трансформації України. 2019. URL: https://osvita.diia.gov.ua/uploads/0/585-cifrova_gramotnist_naselenna_ukraini_2019_compressed.pdf (дата звернення 25.05.2022).

27. Чернишов Г. М. До питання про визначення фінансового шахрайства. Науковий вісник Ужгородського національного університету. Право. 2014. Вип. 26.

28. Чернявський С. С. Фінансове шахрайство: методологічні засади розслідування : монографія. Київ, 2010. С. 624.

ДОДАТКИ

Додаток А

SUMMARY

Kildei A. D. Modeling risk of fraud with bank payment cards. Bachelor's thesis. Sumy State University, Sumy, 2022.

The rapid pace of modernization of the banking sector, the emergence of new payment systems and payment methods have become the basis for the emergence of various forms of fraud that require legal regulation and identify possible ways to combat such crimes. As the share of fraud in the financial sector increases, there are consequences for the payment service provider and the user. One of the biggest consequences is the decline of public confidence in financial institutions, which further hinders the use of public money as an investment tool for the development of the national economy. In the content fraud methods by the method of perpetration are classified, the main trends of fraud with payment cards in Ukraine and the world are analyzed, a system and individual offers for improvement of fraud prevention in the financial sector are formed. The Data Mining method (k-means algorithm) is used to quickly assess the risk of fraud with bank payments.

Keywords: fraud, bank, payment cards, Data Mining, clustering.

АНОТАЦІЯ

Кільдей А. Д. Моделювання ризику шахрайства з банківськими платіжними картками. Кваліфікаційна робота бакалавра. Сумський державний університет, Суми, 2022 рік.

Швидкі темпи модернізації банківського сектору, поява нових платіжних систем і методів розрахунків стали базою для появи різноманітних форм шахрайства, що потребують правового регулювання та визначення

можливих шляхів боротьби з такими злочинами. Зі збільшенням частки шахрайства у фінансовому секторі наслідки несе як надавач платіжних послуг, так і безпосередньо користувач. Один із найбільших наслідків є зниження довіри громадян до фінансових установ, що в подальшому перешкоджає використанню грошей суспільства як інвестиційного інструменту для розвитку національної економіки. У роботі класифіковано шахрайства за методом вчинення, проаналізовано основні тенденції шахрайства з платіжними картками в Україні та світі, а також сформовано систему та окремі пропозиції щодо удосконалення протидії шахрайствам в фінансовому секторі. Методом Data Mining (алгоритм k-середніх) проведено експрес-оцінку ризику шахрайств з банківськими платежами.

Ключові слова: шахрайство, банк, платіжні картки, Data Mining, кластеризація.

Додаток Б

Частина масиву даних, обрана для створення моделі оцінки ризику здійснення шахрайства з банківськими платежами

CATEGORY	AMT	BIRTH	GENDER	TIME	WEEK_DATE	IS_FRAUD
1	2.86	53	1	12	7	0
1	29.84	32	0	12	7	0
2	41.28	51	0	12	7	0
3	60.05	34	1	12	7	0
4	3.19	66	1	12	7	0
5	19.55	30	0	12	7	0
2	133.93	71	0	12	7	0
1	10.37	49	0	12	7	0
6	4.37	48	1	12	7	0
7	66.54	65	0	12	7	0
7	7.01	25	1	12	7	0
5	42.4	45	1	12	7	0
8	2.91	45	0	12	7	0
7	7.93	84	1	12	7	0
5	2.91	50	0	12	7	0
9	24.73	33	0	12	7	0
6	2.33	34	1	12	7	0
5	16.6	29	0	12	7	0
9	80.11	44	0	12	7	0
1	5.71	24	0	12	7	0
4	8.53	24	0	12	7	0
5	37.95	29	0	12	7	0
4	1.74	50	1	12	7	0
4	6.02	24	0	12	7	0
6	9.87	36	0	12	7	0
7	47.06	30	0	12	7	0
2	1.7	64	1	12	7	0
1	2.17	53	1	12	7	0
4	6.21	73	0	12	7	0
1	24.44	64	0	12	7	0
1	176.23	91	1	12	7	0
8	134.39	47	0	12	7	0
1	19.03	57	1	12	7	0
9	210.36	47	0	12	7	0
8	52.81	57	0	12	7	0
7	82.32	63	1	12	7	0
1	26.31	26	1	12	7	0
5	134.6	52	0	12	7	0

5	36.72	41	1	12	7	0
9	105.78	52	1	12	7	0
8	39.95	44	0	12	7	0
8	47.81	46	1	12	7	0
5	18.96	47	1	12	7	0
9	46.67	60	0	12	7	0
5	30.59	78	1	12	7	0
8	3.94	49	0	12	7	0
8	84.11	42	1	12	7	0
5	31.19	35	0	12	7	0
7	4.91	27	0	12	7	0
2	5.36	47	0	12	7	0
8	80.5	47	1	12	7	0
9	49.57	92	0	12	7	0
9	79.51	45	1	12	7	0
2	34.17	33	0	12	7	0
8	9.75	87	0	12	7	0
1	68.88	28	1	12	7	0
8	30.73	57	0	12	7	0
8	63.27	35	0	12	7	0
9	121.46	42	0	12	7	0
10	9.23	22	0	12	7	0
5	8.86	34	0	12	7	0
8	55.53	39	1	12	7	0
2	2.61	23	1	12	7	0
5	1.93	84	1	12	7	0
9	20.03	37	0	12	7	0
6	7.93	49	0	12	7	0
1	20.4	36	0	12	7	0
2	181.87	73	0	12	7	0
8	30.72	58	1	12	7	0
9	129.58	22	0	12	7	0
5	5.13	41	1	12	7	0
6	189.99	46	0	12	7	0
10	5.37	36	1	12	7	0
1	6.04	53	1	12	7	0
7	15.49	44	1	12	7	0
10	4.94	32	1	12	7	0
1	74.52	32	1	12	7	0
6	4.4	51	0	12	7	0
8	71.68	32	0	12	7	0
8	33.97	37	0	12	7	0
7	20.87	54	1	12	7	0
5	19.41	21	0	12	7	0
1	21.57	72	1	12	7	0