УДК 351.72; 347.73, 004.9:004.056:343.53:[336(477)(047.31)
УККП
№ державної реєстрації 0121U100467
Інв. №

Міністерство освіти і науки України
Сумський державний університет (СумДУ)
40007, м. Суми, вул. Р.-Корсакова, 2,
тел. (0542) 66-51-10, факс (0542) 33-40-49

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

_____ А.М.Чорноус

ЗВІТ
ПРО НАУКОВО-ДОСЛІДНУ РОБОТУ
Data-Mining для протидії кібершахрайствам та легалізації кримінальних доходів в умовах цифровізації фінансового сектору економіки України

МОДЕЛЮВАННЯ КОМПЛЕКСНОЇ ОЦІНКИ РИЗИКУ КІБЕРШАХРАЙСТВ ТА ЛЕГАЛІЗАЦІЇ КРИМІНАЛЬНИХ ДОХОДІВ У ФІНАНСОВОМУ СЕКТОРІ УКРАЇНИ НА ОСНОВІ МЕТОДІВ DATA MINING

(проміжний)

Керівник НДР
д-рка екон. наук, професорка Ольга КУЗЬМЕНКО

2022

Рукопис закінчено 15 грудня 2022 р.

Результати роботи розглянуті науковою радою СумДУ протокол від __ грудня 2022 №__

СПИСОК АВТОРІВ

Керівник НДР – Головна наукова співробітниця, д-рка екон. наук, професорка	_____ 15.12.2022	Ольга КУЗЬМЕНКО (підрозділ 1.3, 2.4)
Відповідальний виконавець, старша наукова співробітниця, канд. екон. наук	_____ 15.12.2022	Вікторія БОЖЕНКО (підрозділ 1.1, 1.4, 2.1, 3.2)
Виконавці: Старший науковий співробітник, доктор екон. наук	_____ 15.12.2022	Антон БОЙКО (підрозділ 1.2, 2.4, 3.1)
Старший науковий співробітник, канд. екон. наук	_____ 15.12.2022	Андрій БОЖЕНКО (підрозділ 1.3, 2.3, 3.2)
Старша наукова співробітниця, канд. екон. наук	_____ 15.12.2022	Тетяна ДОЦЕНКО (підрозділ 1.1, 1.2, 2.2)
Виконавець за договором підряду, канд. екон. наук	_____ 15.12.2022	Андрій СЕМЕНОГ (підрозділ 1.1)
Виконавиця за договором підряду, канд. екон. наук	_____ 15.12.2022	Олена ПАХНЕНКО (підрозділ 2.1)
Виконавець за договором підряду, аспірант	_____ 15.12.2022	Олександр КУШНЕРЬОВ (підрозділ 1.3, висновки)
Виконавець за договором підряду, аспірант	_____ 15.12.2022	Сергій МИНЕНКО (підрозділ 1.4, 3.1)
Виконавиця за договором підряду, аспірантка	_____ 15.12.2022	Юлія Доля (розділ 2)
Виконавець за договором підряду, студент	_____ 15.12.2022	Артем ШТЕФАН (підрозділ 1.4)
Виконавиця за договором підряду, студент	_____ 15.12.2022	Анастасія КІЛЬДЕЙ (підрозділ 1.2, 2.1, 3.2)

РЕФЕРАТ

Звіт про НДР: 173 с. 1 ч., 53 табл., 44 рис., 1 дод., 115 джерел.

DATA MINING, КІБЕРШАХРАЙСТВА, КРИПТОВАЛЮТА, НЕЗАКОННІ ФІНАНСОВІ ОПЕРАЦІЇ, ФІНАНСОВИЙ СЕКТОР

Об’єктом дослідження – система нейромережевих зв’язків фінансово-економічних та інформаційних потоків, що виникають між економічними суб’єктами в процесі розподілу фінансових ресурсів.

Мета роботи – формування інформаційного та математичного забезпечення ідентифікації та оцінювання специфічних економічних відносин, які виникають при здійсненні протиправної діяльності у фінансовому секторі економіки країни, на основі використання технологій та методів інтелектуального аналізу даних.

У процесі дослідження застосовувалися методи бібліометричного аналізу (з використанням інструментаріїв VOSviewer v.1.6.10 та SciVal by Elsevier), методи економіко-математичного моделювання (нейромережеве моделювання з використанням багатошарового персептрону MLP-архітектури, асоціативні правила, автокореляційний аналіз, поліноміальні моделі розподіленого лагу Алмона, функція корисності Стоуна-Гірі), програмування.

При виконанні НДР були отримані наступні нові наукові та прикладні результати: 1) Вперше розроблено науково-методичний підхід до оцінювання та прогнозування ризику кібершахрайств у сфері фінансових послуг на основі побудови нейромережевої моделі; 2) Удосконалено науково-методичний підхід до оцінювання ефективності протидії використання послуг та/або інфраструктури фінансових посередників для легалізації кримінальних доходів та здійснення кібершахрайств шляхом використання функції корисності Стоуна-Гірі; 3) розроблено науково-методичний підхід до оцінювання впливу волатильності цифрових активів на рівень фінансової стабільності країни на основі системного поєднання автокореляційних

функцій та поліноміальних моделей розподіленого лагу Алмона.; 4) удосконалено методологічний базис визначення підозрілих шахрайських фінансових операцій у соціальних мережах за допомогою методів мережевого аналізу.

Практичне значення одержаних результатів полягає у тому, що вони впровадженні у навчальний процес Сумського державного університету, що підтверджується актом впровадження, а саме використано у навчальний процес наукові праці з даної проблематики, розроблено практично-орієнтовані лабораторні роботи з дисципліни «Програмне забезпечення математичного та статистичного аналізу», «Системи штучного інтелекту в моделюванні економіки».

У межах дослідження підготовлено та захищено 1 кваліфікаційну роботу Кільдей А.Д. «Моделювання ризику шахрайства з банківськими платіжними картками» [**Ошибка! Источник ссылки не найден.**], що й слугували частиною даного звіту. У межах даної науково-дослідної роботи здійснюється підготовка 2 кандидатських дисертацій (Миненко С.В., Кушнерьов О.С.), 1 докторської дисертації (Боженко В.В.).

ЗМІСТ

ВСТУП

В сучасному діловому світі фінансове шахрайство представляє собою серйозну загрозу економічній системі. А ризики фінансових злочинів у галузі інформаційних технологій ідентифікують особливу проблему для економіки, фінансів, бізнес-процесів, які складно виявити, оцінити, перевірити. При чому кількість фінансових порушень із залученням комп'ютерних технологій протягом останніх років тільки зростає. Це реалізовується шляхом вірусних атак, атак типу відмови в обслуговуванні, фінансові кібератаки, проникнення в інформаційну систему, заволодіння конфіденційною інформацією, несанкціонованого доступу, порушення цілісності, конфіденційності певних даних, та ін. Однією з основних причин зростання таких злочинів є розвиток та поширення мережі Інтернет, інтернет технологій, дистанційних послуг, новітніх фінансових технологій. Все це сприяє поширенню кібершахрайств та проведення тіньових фінансових операцій. Що представляє особливо серйозну загрозу майновій безпеці, соціальній стабільності як країни загалом, так і окремо кожної особистості зокрема, та призводить до фінансових, грошових витрат, втрати ринкової капіталізації, впливають на альтернативну вартість, погіршують імідж та довіру в майбутньому. Тож обрана проблематика є достатньо гострою та займає одне з провідних місць не лише в межах України, але й на міжнародній арені.

Мета дослідження полягає в формуванні інформаційного та математичного забезпечення ідентифікації та оцінювання специфічних економічних відносин, які виникають при здійсненні протиправної діяльності у фінансовому секторі економіки країни, на основі використання технологій та методів інтелектуального аналізу даних.

Об'єктом дослідження є система нейромережевих зв'язків фінансово-економічних та інформаційних потоків, що виникають між економічними суб'єктами в процесі розподілу фінансових ресурсів.

Предметом дослідження є комплекс методів та моделей інтелектуального збору та аналізу інформації, що використовується для ідентифікації синергетичних явних та латентних проявів нелегальних економічних операцій, спрямованих на вдосконалення системи запобігання та протидії 2 фінансовим та кіберзлочинам на мікро-, макро- та мезорівнях

Емпіричну базу дослідження становлять вивчення й використання різноманітних джерел: наукових статтей, дисертацій, нормативно-правові документи, спеціальна література, матеріали засобів масової інформації, звіти міжнародних організацій, звіти профільних організацій, бази статистичних даних, що характеризують обсяг нелегальних фінансових потоків та кібершахрайства.

У межах дослідження підготовлено та захищено 1 кваліфікаційну роботу Кільдей А.Д. «Моделювання ризику шахрайства з банківськими платіжними картками» [1], що й слугували частиною даного звіту. У межах даної науково-дослідної роботи здійснюється підготовка 2 кандидатських дисертацій (Миненко С.В., Кушнерьов О.С.), 1 докторської дисертації (Боженко В.В.).

1 ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ВИЗНАЧЕННЯ РИЗИКУ КІБЕРШАХРАЙСТВ ТА ЛЕГАЛІЗАЦІЇ КРИМІНАЛЬНИХ ДОХОДІВ У ФІНАНСОВОМУ СЕКТОРІ УКРАЇНИ

1.1. **Аналіз тенденційного та бібліографічного аналізу розвитку фінансових кібершахрайств**

Цифровізація сучасного світу, розвиток інформаційних технологій, поширення Internet, комп'ютерні мережі, використання кіберпростору, наразі виступають основою сучасного суспільства. Всі ці новітні заходи полегшили повсякденне життя суспільства, але паралельно з цим спричинило загрозу безпеки та конфіденційності інформації, особистих даних, стабільності фінансової системи. Фінансове шахрайство стає все більш серйозною глобальною макро проблемою, так як фінансова екосистема наразі розглядається як складна, комплексна мережа установ, операцій у різних обсягах, валютах, вартостях, з різних територіальних місць, за допомогою різних інструментів, в якій фінансові установи побудували та згрупували ряд продуктів та послуг з огляду на переваги глобалізації, цифровізації та можливостей високої фінансової складності, – що також використовується кримінальним світом для відмивання нелегальних коштів та проведення незаконних фінансових транзакцій [2, 3].

Фінансові шахрайства є багатогранними, різноаспектнимими, транскордонними, територіально необмеженими, і досить часто невидимими, що перешкоджає її ідентифікації, аналізу, оцінці, боротьби з нею. Вплив негативних наслідків фінансових шахрайств відчувається у багатьох сферах та напрямках. Установи, організації та корпорації загалом та фізичні особи окремо несуть значні фінансові розходи намагаючись перешкоджати здійсненню фінансових незаконних транзакцій. Але не дивлячись на ці заходи, нелегальні кошти продовжують обіг фінансовою системою, спричиняючи величезні втрати у бізнесі, недоотримання податків державою, внаслідок чого страждає економіка країни на національному ринку, інфраструктура країни,

добробут населення. В свою чергу це викликає дестабілізацію національної системи через кримінальну, шахрайську діяльність, що фінансується фінансовою злочинністю.

Тому дослідження тенденцій фінансових шахрайств наразі є особливо актуальним питанням. Це допоможе покращити поінформованість про фінансові шахрайства, створити спільні бази даних, утворити коаліції, визначити ефективні та дієві способи, що допоможуть у підвищені спроможності боротьби з фінансовими злочинами на більш ефективному національному та світовому рівні.

Злочинні угруповання діють транснаціонально, щоб уникнути виявлення, а викрадені кошти перетинають багато фізичних і віртуальних кордонів, перш ніж досягти кінцевого пункту призначення. Кіберзлочинці продовжують адаптувати свою тактику та процедури, щоб отримати доступ до складних і високозахищених систем фінансових установ.

Фінансові кібершахрайства – це явище, яке загрожує різноманітним сферам життєдіяльності, оскільки фінансові установи обслуговують домогосподарств та суб’єктів господарювання різних галузей економіки. Саме тому фінансові кібершахрайства розглядаються як складне явище, і єдиний спосіб протистояти їй – посилення співпраця у системі відносин «міжнародні організації – національний регулятор – фінансові установи – споживачі фінансових послуг (юридичні та фізичні ососби)».

«Фінансові кібершахрайства» є достатньо широким поняттям, яке включає майже всі види протиправної діяльності, спрямовані проти фінансових установ або за їх посередництва з використанням інформаційних та комп’ютерних технологій.

Фінансові кібершахрайства варіюються від простих крадіжок або злочинів, вчинених особами з лихими намірами, до великомасштабних операцій, організованих організованими злочинцями, які діють на всіх континентах. Це серйозна кримінальна діяльність, значення якої не слід

применшувати, оскільки, окрім соціального та економічного впливу, вони часто тісно пов’язані з насильницькими злочинами і навіть тероризмом.

Надзвичайно важливим та змістовним напрямом є вивчення джерел та інструментів фінансових злочинів, визначення їх основних характеристик та особливостей, виявлення типових ситуацій а схем порушень, які постійно доповнюються та змінюються у відповідь на ситуацію, що формується на фінансовому ринку, з огляду на дії кримінального світу.

Однією із головних причин появи фінансових шахрайств є зростаюча у геометричній прогресії кількість пристроїв з конфіденційними фінансовими даними, що підключаються до мережі Internet, а також розширення кіберпростору, наслідком чого є [4, 5, 6, 7, 8, 9, 10]:

– онлайн атаки на програмне та апаратне забезпечення серверів, мережевих пристроїв, одиночних кінцевих користувачів, за допомогою шкідливих програм – віруси, трояни, шпигунське програмне забезпечення, з метою крадіжки конфіденційної інформації, перевірок шахраями рівня захисту об’єкту, отримання контролю над комп’ютерним обладнанням об’єкту нападу;

– зараження USB-накопичувача з подальшим перенесенням зараженого девайсу на інші пристрої;

– ботнети Internet of Things – технологія, що дозволяє через мережу Internet чи подібну мережу встановлювати віддалені з’єднання між інтелектуальними пристроями;

– фішингова загроза для фінансових платежів – через підроблені сайти виступає причиною шахрайських операцій, компрометації особистих та корпоративних даних, розповсюдження небезпечного програмного забезпечення;

– розповсюдження спамів через розгалужені платформи соціальних мереж;

– програма ефект бабочки – шахрайська програма-вимагач, що розповсюджується через електронну пошту;

– порушення даних, вразливість від непрямих атак, через недоліки безпеки у веб-інфраструктурі, веб-додатках, веб-завантаженнях;

– прогалини у практичних навичках працівників кібербезпеки, недостатність фахівців з кіберзахисту;

– хмарна небезпека інформаційних ресурсів – через повсюдний доступ до мережі, об'єднання ресурсів для спільного використання, контроль та управління даними постачальниками хмарних послуг, зростає ризик кібератак на ці ресурси.

Також до сучасних джерел та інструментів фінансових злочинів необхідно віднести наступні [11, 12]:

– використання шахраями новітніх технологій – біометрії, штучного інтелекту (шахраї використовують такі системи для послідовного сканування обраної системи та її подальшої атаки);

– суперечливе поширення новітньої технології 5G (через свою розширену пропускну спроможність сприяє надзвичайно стрімкому зростанню обсягів пристроїв та даних, що не відповідає наявним можливостям контролю та захисту);

– надмірне використання смарт-пристроїв (кількість розумних смарт пристроїв, таких як смартфони, смарт-телевізори, смарт-годинники, смарт-колонки та ін. з функцією доступу через Bluetooth, Wi-Fi, мобільні потоки, не відповідає існуючим можливостям забезпечення їх безпечного використання);

– поширення кіберстрахування (зростають недоліки цієї опції в частині націленості кібершахраїв саме на застраховані об'єкти як ті, що потенційно можуть надати можливість зловмисникам отримати великі кошти);

– шахрайства з криптовалютою: особливості смарт-контрактів в онлайн-сервісах, що базуються на технології блокчейн;

– фінансування розповсюдження зброї масового знищення (купівля товарів подвійного призначення; використання зон вільної торгівлі, а також

транзитних центрів для незаконних операцій; застосування схем з підставними організаціями; використання офіційних фінансових установ для нелегальних транзакцій).

Проаналізувавши ключові джерела та інструменти здійснення протиправної діяльності у фінансовій сфері представимо основні види фінансових кібершахрайств на рисунку 1.1.

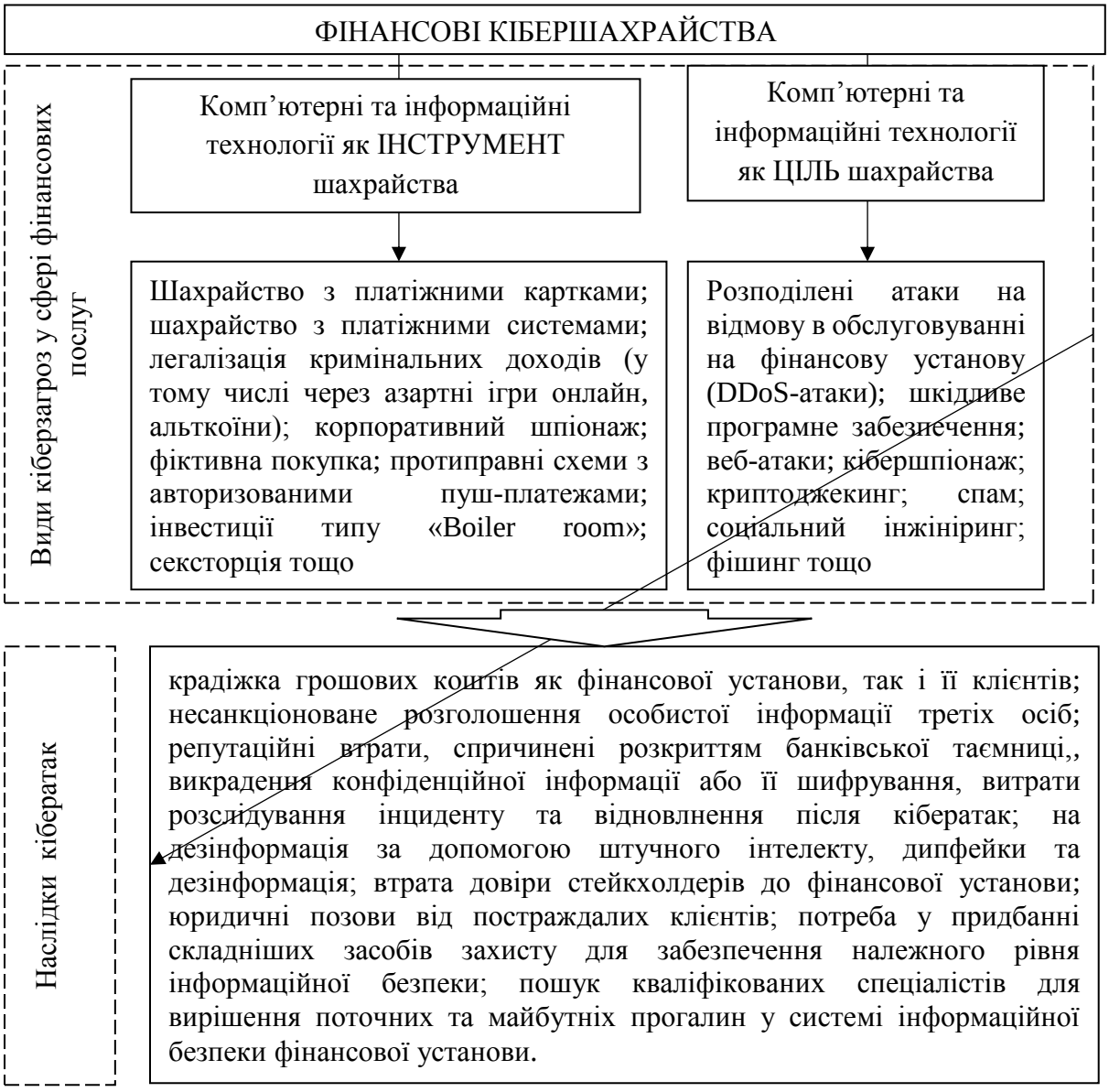


Рисунок 1.1 – Основні види фінансових кібершахрайств

Джерело: складено авторами на основі [13, 14, 15, 16]

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. 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 [17].

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 [17].

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 [18].

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% [19].

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.

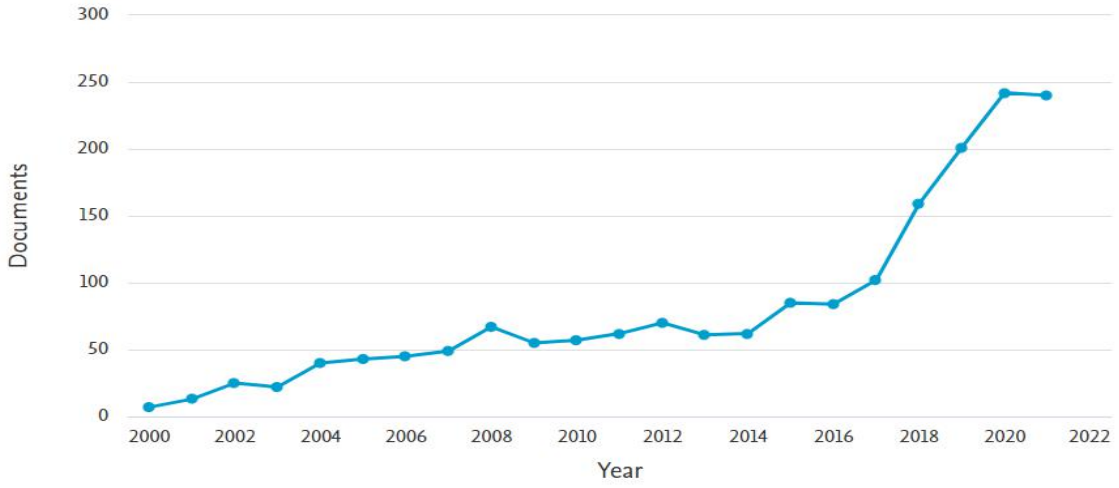


Рисунок 1.2 – Динаміка публікацій за ключовими словами «fraud» та «card» згідно з наукометричною базою Scopus протягом 2000–2021 рр., одиниць

Джерело: наукометрична база Scopus

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.

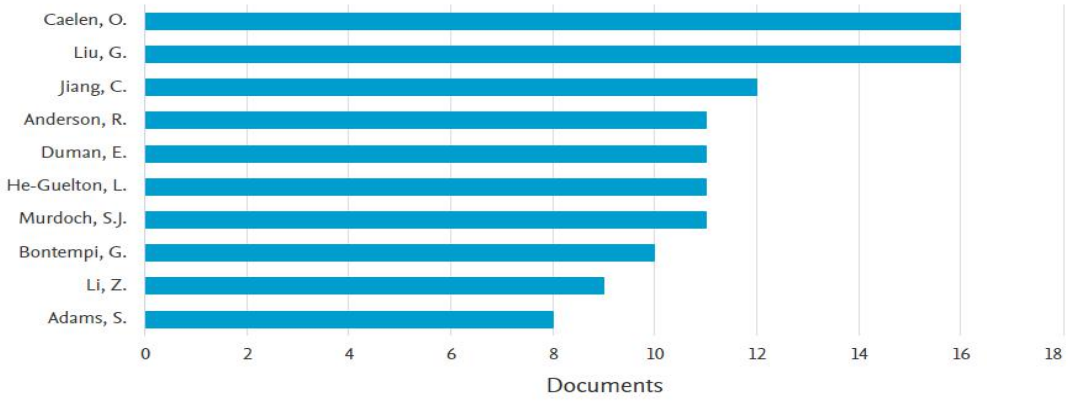


Рисунок 1.3 – Динаміка кількості публікацій за авторами з проблематики «шахрайство з банківськими картками» в базі Scopus у період 2000-2021 рр.

Джерело: наукометрична база Scopus

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, преважна кількість з них написана у таких сферах як: комп'ютерні науки, інженерія та математика. У своїй роботі [20] «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. [21] 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 [22] 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).

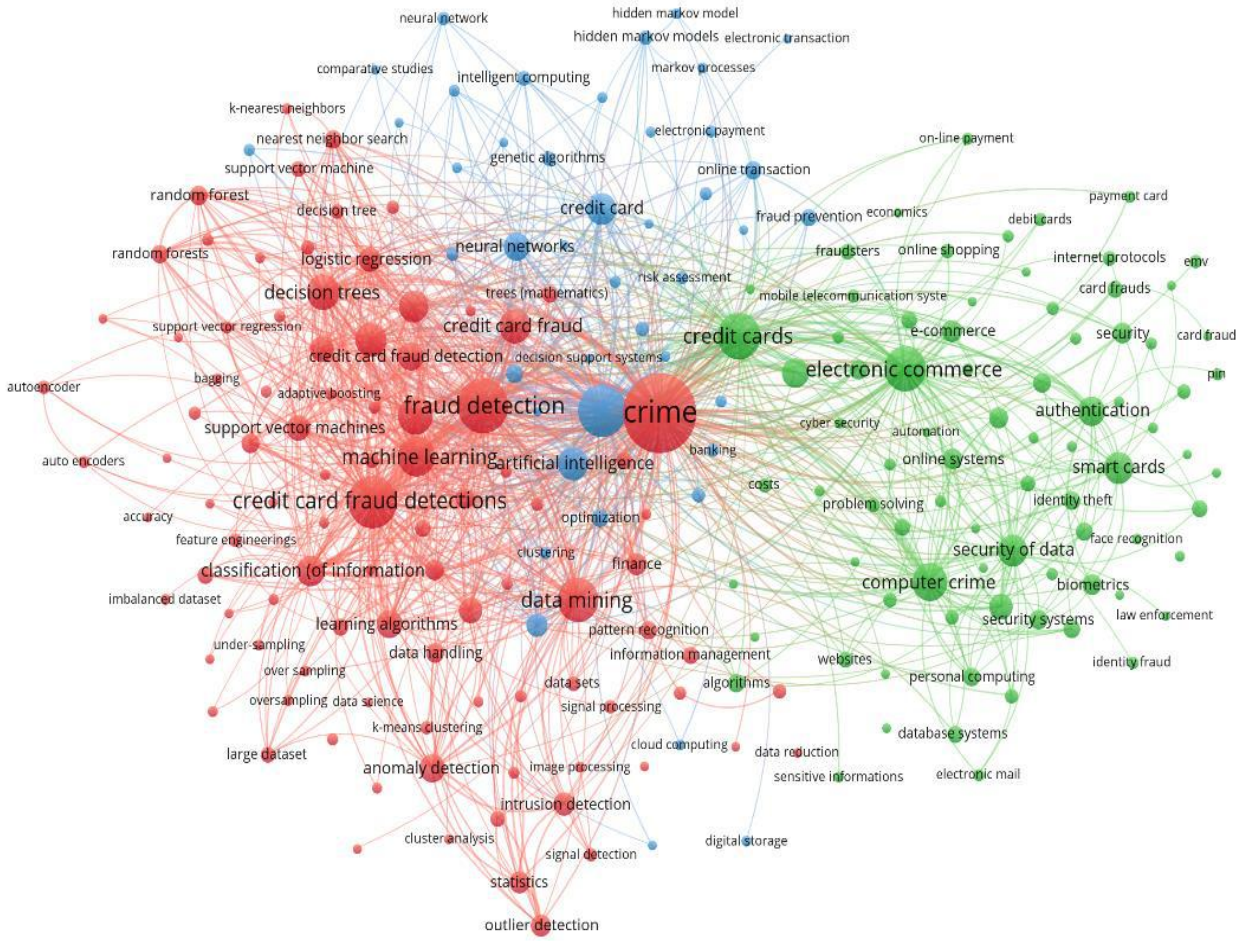


Рисунок 1.4 – Результати бібліометричного аналізу ключових слів, що одночасно трапляються в публікаціях, проіндексованих наукометричною базою Scopus, за запитами «fraud» та «card» за допомогою інструментарію VOSviewer

Джерело: складено авторами за допомогою інструментарію VOSviewer

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.

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.

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.

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.

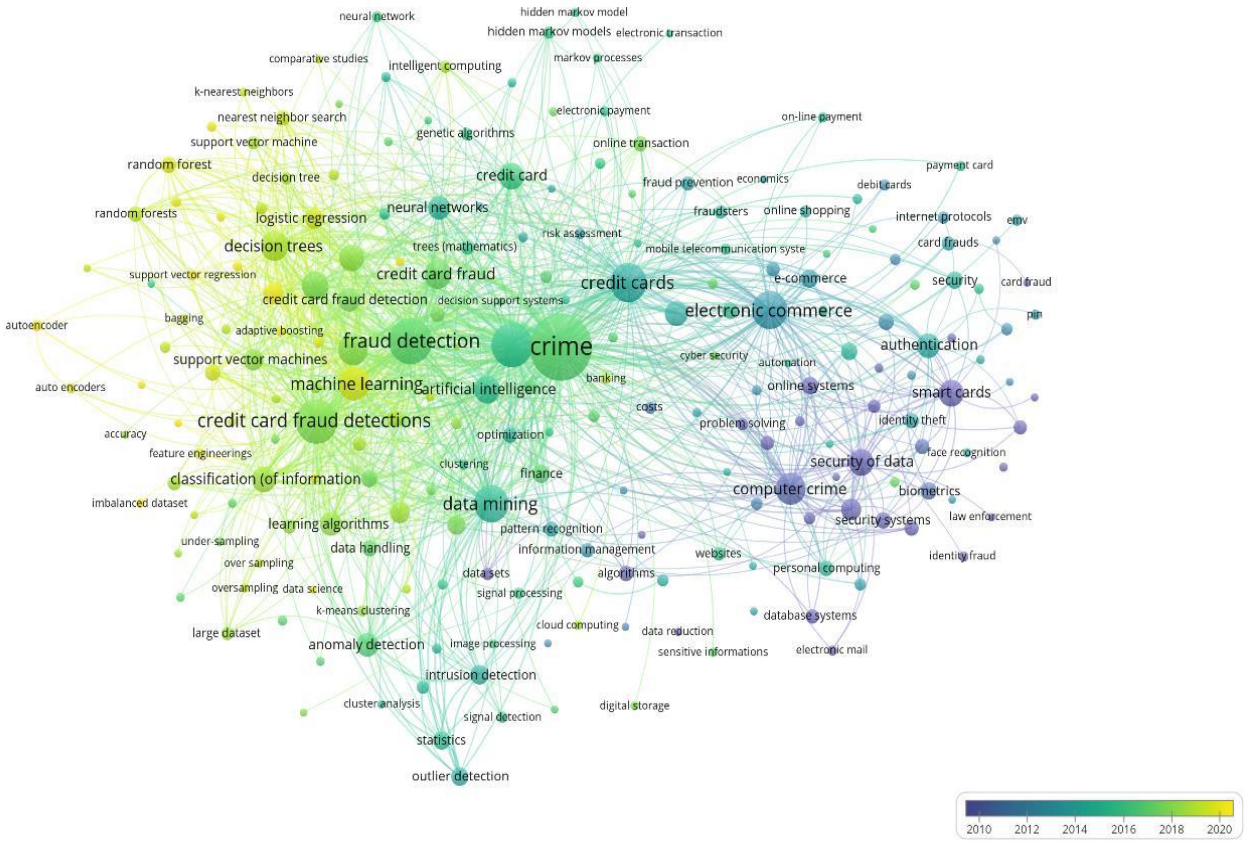


Рисунок 1.5 – Результати бібліометричного аналізу ключових слів, що одночасно трапляються в публікаціях, проіндексованих наукометричною базою Scopus, за запитами «fraud» та «card» за допомогою інструментарію VOSviewer

Джерело: складено авторами за допомогою інструментарію VOSviewer

Проаналізувавши численні наукові праці [23, 24, 25], звіти національних фінансових регуляторів [26, 27], а також міжнародних організацій [19, 28], систематизовано основні види шахрайства з банківськими платіжними картками (рис. 1.6).

Рисунок 1.6 – Види шахрайств з банківськими платіжними картками за способом вчинення

Джерело: складено на основі [19, 23, 24, 25, 26, 27, 28].

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 [29]. Дані цифри дозволяють стверджувати, що

рівень довіри до вітчизняної банківської системи знаходиться на низькому рівні.

Шахрайські 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 [28] (рис. 1.7). Показники за 2018 і 2019 роки залишаються значно нижчими за максимум, зафіксований у 2015 році (0,042%).

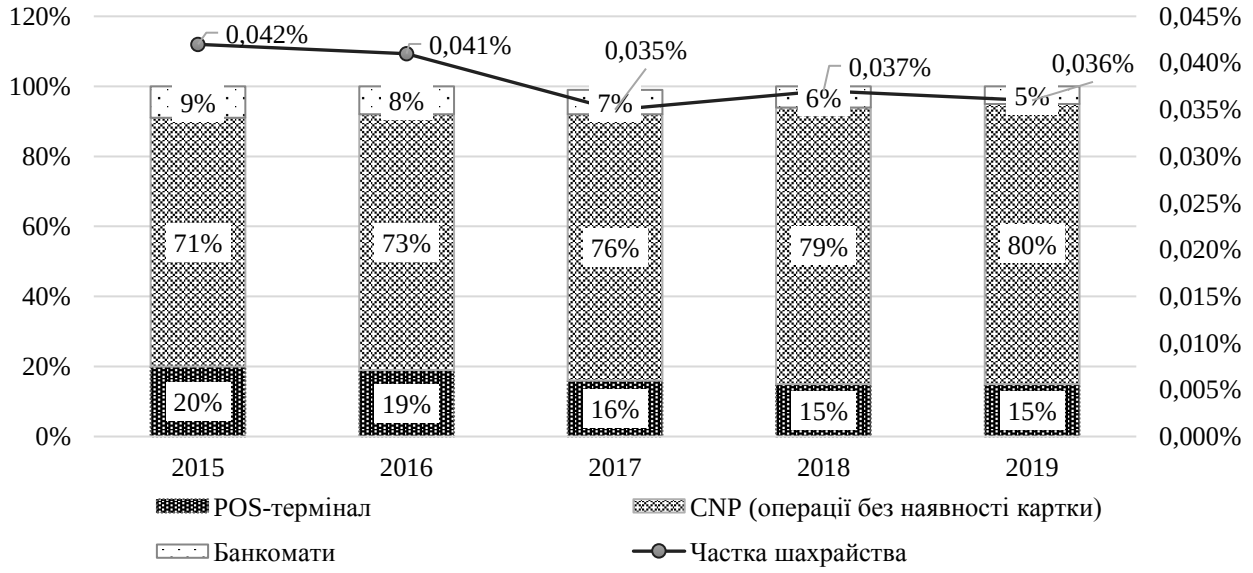


Рисунок 1.7 – Загальний об'єм шахрайств з платіжними картками на території SEPA протягом 2015-2019 рр.

Джерело: дані Європейського центрального банку [28]

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.

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. 1.8).

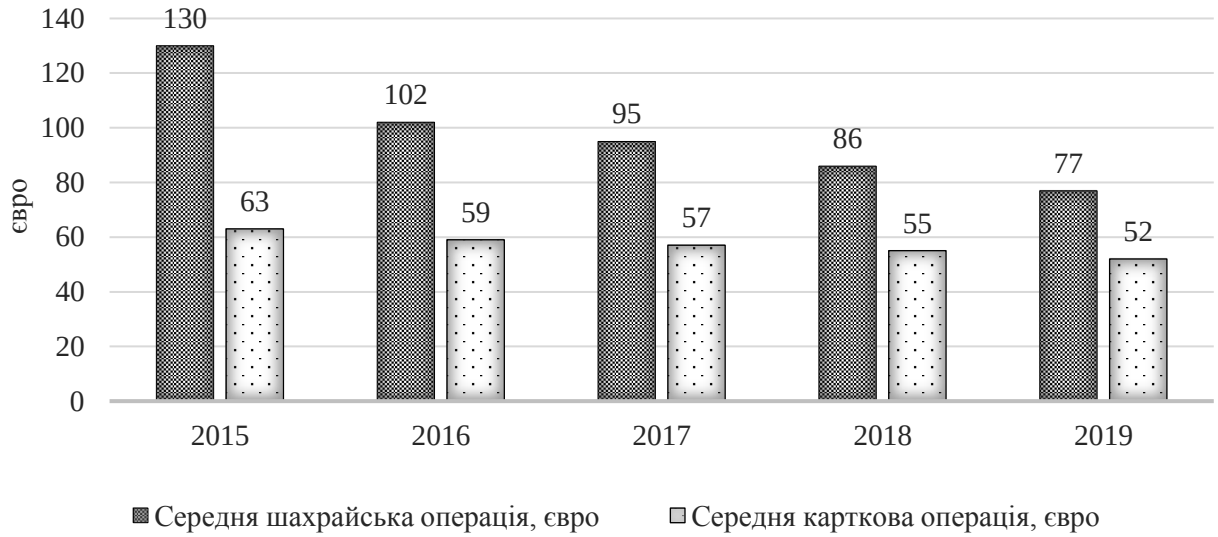


Рисунок 1.8 – Середній розмір усіх транзакцій, проведених за допомогою карток протягом 2015-2019 рр.

Джерело: дані Європейського центрального банку [28]

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. 1.9). 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 1.9 – Динаміка кількості електронних платіжних засобів, емітованих українськими банками, та суми операцій за ними за період 2011 -2021 рр.

Джерело: дані Національного банку України [26]

За даними Національного банку України протягом останніх трьох років структура видів карток для проведення банківських платежів зазнала суттєвих змін (рис. 1.10). 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.

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. [30].

2019 2020 2021

Рисунок 1.10 – Види платіжних карток в Україні протягом 2019-2021 рр. (станом на 1 січня кожного року)

Джерело: дані Національного банку України [26]

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%.

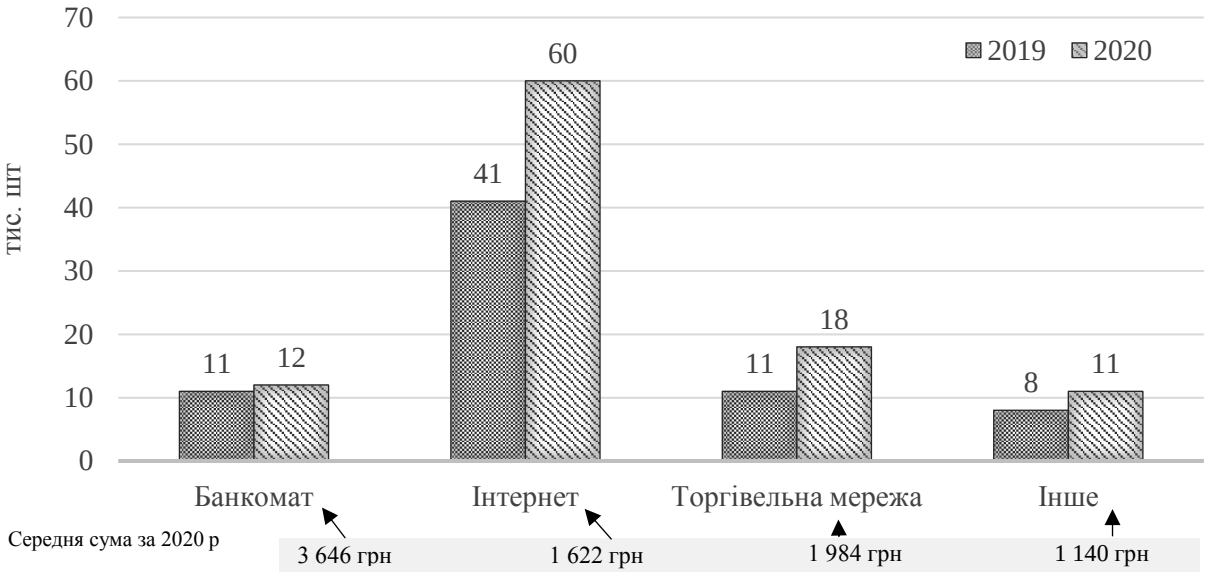


Рисунок 1.11 – Кількість збитків від незаконних дій з платіжними картками, тис. шт.

Джерело: дані Національного банку України [26]

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

1.2. **Систематизація існуючих підходів до оцінювання ризику кібершахрайств та тіньових фінансових операцій**

Попри значні інвестиції фінансових установ у підвищення рівня їх інформаційної та фінансової безпеки, фінансові злочини на сьогоднішній день дуже поширене явище. Для вирішення такої проблеми потрібно розробити комплексний, системний підхід, що буде ґрунтуватись на якісній оцінці та достовірному прогнозуванні відповідних ризиків, щоб в подальшому забезпечити формування необхідного набору дієвих інструментів, принципів та підходів до управління ризиками кібершахрайств та проведення тіньових фінансових операцій.

До вирішенням проблем кібершахрайств протягом останніх років долучились ряд сучасних науковці: так Дегтерева В., Гладкова С., Макарова О., Мелкоступов Є. [31] вивчають формування механізму запобігання порушенням у кіберпросторі, поширеним кіберзагрозам під час цифровізації та шляхи їх подолання; Чен С., Гао Ч., Цзян Д., Хао М., Дін Ф., Ма Т., Лі С. [32] описують просторово-часові закономірності та рушійні фактори злочинності кібершахрайства; Порседда М.Г., Уолл Д. С. [33] розповідають

про моделювання каскадного ефекту кіберзлочинності в сфері інформаційних злочинів; Штурц Б., Гурова Т., Зеленкова Н. та Шестак В. [34] пропонують систему показників кластеризації фінансової кіберзлочинності; Ніколлс Дж., Куппа А. і Ле-Хак Н. -. [35] розглядають фінансову кіберзлочинність шляхом всебічного огляду підходів глибокого навчання для подолання ситуації з фінансовими злочинами.

Проблематику актуальних тіньових фінансових операцій розкривають у своїх роботах наступні вчені: Рєзнік О., Уткіна М., Бондаренко О. [36] пропонують фінансову розвідку як ефективний засіб протидії тіньовій економіці; Маклахлан Ф. [38**Ошибка! Источник ссылки не найден.**] описує тіньовий банкінг та тіньову платіжну систему; Бричко М., Савченко Т., Васильєва Т. та Піотровський П. [39] розкривають незаконну діяльність фінансових посередників.

Оцінці та прогнозуванню ризику кібершахрайств значну увагу у свої роботах приділяють такі науковці, як:. Коста М.П.Л., та Араужо Е. [40] досліджують нечітку систему управління ризиком фінансового шахрайства в середовищі інформаційних технологій; Мухопадхьяй А., Чаттерджі С., Багчі К.К., Кірс П.Дж. і Шукла Г. К. [41] пропонують платформу оцінки та зниження кіберризиків (CRAM) з використанням логіт- та пробіт-моделей на прикладі кіберстрахування; Рубасундрам Г. А. [42] описують спосіб оцінки ризику корпоративного шахрайства та уявної кібербезпеки; Гаол Ф.Л., Будіанса А.Д., Веніко Ю.П., і Мацуо Т. [43] розкривають контроль ризику цифрового шахрайства в електронних компаніях; Крайваніт Т., і Шріяем П. [44] пропонують оцінку шахрайства з інтернет-транзакціями; Дамашевичюс Р. та Зайльскайте-Якште Л. [37] пропонують систему для прогнозування ризиків онлайн-операцій; Сільва С.М.R.D., Фейтоса Е.Л., Гарсія В.К. [45] описують евристичну стратегію для прогнозування фішингу; Суреш Бабу, М., Бхавана Радж, К., і Аша Деві, Д. [46] вивчають тенденції електронного бізнесу та його прогнозування.

В свою чергу, питаннями оцінки та прогнозування ризику тіньових фінансових операцій, займаються такі вчені: Цао К., Ма Б. і Чжу Ю. [47] досліджують ризик тіньового банківського сектору; Воямес Дреер В. [48] пропонують регулювання тіньового банківського обслуговування.

Досліджуючи ризик кібершахрайств та тіньових фінансових операцій, виділяються два рівня оцінки та прогнозування ризику кібершахрайств та тіньових фінансових операцій: макрорівень та мікрорівень.

Розглядаючи оцінку та прогнозування ризику кібершахрайств та тіньових фінансових операцій на макрорівні, необхідно враховувати перелік специфічних аспектів кроків та етапів, що характерні для такого рівня ризиків.

1 етап: визначення, дослідження та аналіз потоку кібершахрайства та незаконного обігу коштів у країні (дані отримуються з письмових рішень суду кримінального, адміністративного, цивільного та іншого спрямування в частині інтернет-шахрайств, кібершахрайств, онлайн-шахрайств, тіньових фінансових транзакцій; ці відомості включають інформацію про кількість відправлень та отримань шахраями).

2 етап: аналіз причин та факторів появи ризиків кібершахрайств та нелегальних фінансових операцій (так, до факторів та характеристик, що визначають виникнення шахрайств відносяться: ситуаційні (поведінка людини в мережі; час, що людина проводить у мережі; рутинна онлайн-діяльність; дистанційне обслуговування; онлайн-банкінг; онлайн-покупки; електронна пошта, обмін миттєвими повідомленнями, кількість користувачів мережі Інтернет; кількість користувачів мобільними телефонами); індивідуальні (характеристики особистості - вік, стать, рівень доходу, етнічна приналежність, безробіття); соціальні (оточуюче середовище, кримінальна субкультура); демографічні; економічні (економічна нерівність, економічний розвиток, покращення рівня життя, недорогі засоби для реалізації шахрайства); фактори розвитку (рівень освіти); культурні; правові; технологічні) та ін.

3 етап: визначення переліку показників макрорівня для здійснення оцінки та прогнозування ризиків фінансових електронних шахрайств (економічний рівень, рівень безробіття, розмір доходів, розмір домогосподарства, вікова структура, рівень освіти, рівень бідності, рівень нерівності, кількість інтернет-користувачів на душу населення, структурні показники суспільства) та ін.

4 етап: виявлення взаємозв'язків факторів та показників появи ризиків електронних фінансових шахрайств (табл. 1.1).

Таблиця 1.1 – Взаємозв'язки факторів та показників появи ризиків кібершахрайств та тіньових фінансових операцій

Фактор	Показник	Категорія, що вимірюється та характеризує ризик
економічний	валовий внутрішній продукт	рівень економічного розвитку
економічний	частка первинної/вторинної/третинної промисловості у ВВП	економічна структура
економічний	залишки за кредитами фінансових установ	рівень розвитку фінансової індустрії
економічний	залишки за депозитами фізичних осіб у фінансових установах	рівень споживчих звичок мешканців
економічний	електронна комерція	рівень життєздатності онлайн-покупок
економічний	виручка від телекомунікацій	рівень розвитку телекомунікаційної галузі
демографічний	загальна чисельність населення	чисельність населення
демографічний	несільськогосподарське населення та безробітне населення	структура населення
демографічний	кількість студентів вищих навчальних закладів, студентів загальноосвітніх коледжів, технікумів, професійно-освітніх навчальних закладів, учнів середніх навчальних закладів	рівень освіти
технологічний	довжина кабелю	пропускна спроможність інформаційної інфраструктури
технологічний	кількість користувачів мобільних телефонів, користувачів інтернету, рівень проникнення інтернету	масштаб інформації та зв'язку

5 етап: обрання моделі для вивчення зв’язків визначених факторів та показників появи ризиків кібершахрайств та тіньових фінансових операцій, отримання кількісної оцінки їх впливу на виникнення шахрайства (індекс І Морана –Moran’s I, узагальнена адитивна модель – GAM).

Зазначено, що індекс І Морана буває двох типів: Глобальний індекс І Морана (Global Moran’s I) та локальний індекс І Морана (Local Moran’s I) [49].

Глобальний індекс І Морана – це інструмент просторової автокореляції, що оцінює, чи наявна кластеризація об'єктів, чи вони розподілені розкидано, чи випадково. Тобто, просторова автокореляція характеризується кореляцією певного сигналу між сусідніми точками у просторі; вона є багатовимірною та багатоспрямованою. Глобальний індекс І Морана вимірюється за формулою 1.1.

$$I = \frac{N}{W}\frac{\sum_i \sum_j w_{ij}(v_i - \bar{v})\left(v_j - \bar{v}\right)}{\sum_i (v_i - \bar{v})^2} \tag{1.1}$$

де I - Глобальний індекс І Морана,

N - кількість просторових одиниць, проіндексованих i та j,

W – сума усіх w_{ij},

v – необхідна змінна,

$\bar{v}$ – середнє значення v,

w_{ij} - матриця просторових ваг із нулями на діагоналі, тобто $w_{ii} = 0$.

Глобальний індекс І Морана оцінює просторову модель географічного явища, визначаючи чи є воно розсіяним, чи згрупованим, чи випадковим на основі розташування та значень пов’язаної ознаки. Такий інструмент обчислює значення І Морана для подальшої оцінки значущості такого індексу. Цей індекс знаходиться в діапазоні від -1 до +1, де -1 – вказує на розсіювання чи дисперсію, +1 - вказує на згрупованість у просторі, а значення індексу близькі до 0 або дорівнює 0 - вказує на відсутність явища автокореляції.

Локальний індекс І Морана – це локальний, місцевий індикатор просторової асоціації. Він розраховується для кожного окремого місця вибірки з метою оцінки ступеня просторової автокореляції, з метою ідентифікації просторових кластерів характеристик з великим чи малим значенням, а також з метою виявлення просторових відхилень. Локальний індекс І Морана вимірюється за формулою 1.2.

$$I_i = v_i \sum_j w_{ij} v_j \tag{1.2}$$

де I_i - Локальний індекс І Морана,

v – необхідна змінна,

w_{ij} - матриця просторових ваг.

Локальний індекс І Морана використовується для встановлення просторових кластерів, а також випадків кібершахрайства та тіньових фінансових операцій у просторових локаціях. При чому позитивне значення індексу вказує на те, що місцерозташуванню притаманні такі ж високі чи низькі значення, як і сусіднім локаціям, а такі місця називають кластерами однакового рівня; негативне значення вказує на те, що місцерозташуванню притаманні протилежні сусіднім локаціям високі чи низькі значення, а такі місця називають кластерами протилежного рівня.

Узагальнена адитивна модель (GAM) - це узагальнена лінійна модель, тобто узагальнення моделі лінійної регресії, в якій змінні, коефіцієнти можна розкласти як лінійні плавні функції коваріатів. В цій моделі застосовується фенуція зв’язку для подальшого фіксування взаємозв’язків між очікуваними змінними та непараметричними змінними. Такий метод вважається напівпараметричним. Він може враховувати також нелінійні взаємозв’язки між залежними змінними, а також коваріатами. Узагальнена адитивна модель має ряд переваг перед іншими моделями: спроможність виявляти нелінійні

взаємозв’язки, наявність регуляризації та задовільної інтерпретації. Узагальнена адитивна модель представляється у вигляді формули 1.3 [50**Ошибка! Источник ссылки не найден.**].

$$g\big(E(Y)\big) = f\big(X_{1,\dots,}X_p\big) = a_0 + f_1(X_1) + \cdots + f_p\big(X_p\big) \quad (1.3)$$

де g – функція зв’язку;

Y – одновимірна змінна відповіді;

$\big(X_{1,\dots,}X_p\big)$ – змінні предиктори;

a_0 – константа

$f_{1,\dots,\mathrm{p}}$ – лінійні плавні функції.

Узагальнена адитивна модель використовується для кількісної оцінки багатомврних взаємозв’язків між випадками кібершахрайства та тіньових фінансових операцій та змішаними типами змінних, коваріатів оточуючого навколишнього середовища.

6 етап: здійснюється прогнозування майбутніх ризиків кібершахрайства та тіньових фінансових операцій шляхом використання певних моделей [37]: методи машинного прогнозування – модель логістичної регресії, метод розрідженого онлайн-прогнозування, байєсовська систему онлайн-прогнозування для двійкового передбачення (лінійна модель, а також та факторизуючий розподіл достовірності за вагами ознак для розрахунку приблизного апостеріорного значення), модель із вбудовуванням числових функцій для прогнозування із збереженням унікальних атрибутів представлення; методика глибоких нейронних мереж (вивчають більш глибокі зв’язки, аналізують функції високого порядку) - рекурентна нейронна мережа, уважна мережеву модель (базується на глибокому інтересі), мережу уваги з подвійним уявленням, двонаправлена закрита рекурентна модель одиниць, гібридна модель передбачення, багатомасштабний стековий пул, та ін.; методика машин факторизації - моделювання поліноміальної регресії, машини нейронної факторизації вищого ладу, та ін.

7 етап: формування заходів по управлінню ризиками кібершахрайства та тіньових фінансових операцій для підвищення рівня економічного розвитку, покращення економічної структури, зростання рівня розвитку фінансової індустрії, стабілізації рівня споживчих звичок мешканців, урегулювання рівня життєздатності онлайн-покупок, покращення рівня розвитку телекомунікаційної галузі, збільшення пропускної спроможності інформаційної інфраструктури та масштабів інформації та зв'язку та ін.

Зупиняючись на специфіці оцінки та прогнозування ризику кібершахрайств та тіньових фінансових операцій на мікрорівні, тобто на рівні установ, підприємств та організацій, варто виділити ряд особливостей, притаманних цьому рівню ризиків. Здійснення оцінки та прогнозування таких ризиків реалізуються шляхом виконання наступних етапів:

1 етап: керівництвом підприємства ініціюється оцінка ризиків можливого кібершахрайства та тіньових фінансових операцій шляхом налаштування системи оцінки ризиків кібершахрайства та тіньових фінансових операцій.

2етап: організовується спеціалізована група, метою якої є виявлення можливостей, цілей, схильностей, схем та методів реалізації заходів кібершахрайства та тіньових фінансових операцій. Реалізація цього етапу здійснюється за допомогою методик мозкового штурму, картирування відповідних процесів, реалізації необхідних перевірок, аудіювання, ревізування, тестування, інтерв’ювання, опитування, обговорення в середині організації серед співробітників.

3 етап: здійснення безпосередньої оцінки ризиків кібершахрайства та тіньових фінансових операцій з урахуванням наступних факторів, чинників, критеріїв, категорій та ключових аспектів: середовище установи, характер управління, форма бізнесу, внутрішні відділи, організація внутрішніх та зовнішніх процесів, функції посадових осіб, власники та ін. Оцінювання проводиться на основі таких особливостей: можливість здійснити поглиблене вивчення загально-організаційної системи установи, її інформаційної системи,

документації, співробітників, корпоративної культури, впливів оточуючого середовища, бізнес-процесів; уміння виконати перевірку наявної середи, системи контролю, актуальних операцій. Виділяють основні критерії для оцінки ризиків кібершахрайства та тіньових фінансових операцій установи: визначення ключових індикаторів ризиків фінансового шахрайства; ідентифікація ризикових фінансових операцій; встановлення проблемних місць у системі роботи організації. До видів оцінки ризику відносять: оцінка ризику мережевих кібератак, оцінка ризику атак з використанням електронні пошти; оцінка ризику атак кінцевих точок; оцінка вразливостей програмного коду та ін.

4 етап: проводиться прогнозування майбутніх ризиків кібершахрайства та тіньових фінансових операцій шляхом використання перехресних методик перевірки обраних критеріїв: встановлення можливих сценаріїв шахрайства, потенційних схем злочинів; виявлення факторів фінансових та кібершахрайств; визначення впливу факторів шахрайських дій.

5 етап: організація заходів по управлінню ризиками кібершахрайства та тіньових фінансових операцій: перегляд та аналіз визначених недоліків, прогалин у діючій фінансовій системі установи, вжиття дій щодо їх контролю, нівелювання, зменшення, шляхом розробки та запровадження ряду пропозицій, утворених на базі здійсненого оцінювання відповідно до ризик-апетиту установи, ворганізація періодичного контролю та перегляду ризиків кібершахрайств та тіньових фінансових операцій, визначення фінансової ризик стратегії.

Таким чином, з популяризацією Інтернету, розвитком технологій, кібернетичний простір почав відігравати особливе місце у багатьох життєвих аспектах людей, в тому числі й тих, що займаються незаконною діяльністю та фінансовими шахрайствами. І хоча інновації більшою мірою мають позитивні характеристики, але останнім часом фінансова сфера постійно потерпає від кіберзагроз та нелегального обігу коштів. Отже, кібершахрайства та тіньові фінансові операції наразі представляють собою серйозну загрозу та шкоду

безпеці та стабільності фінансової системи, та, відповідно, кожного громадянина. Такі шахрайства мають ряд причин, факторів, чинників, критеріїв та особливостей. Тому для вирішення проблем із електронним фінансовим шахрайством, необхідно провести оцінку та прогнозування ризику кібершахрайств та тіньових фінансових операцій.

1.3. **Методичні засади до оцінювання ризику фінансових кібершахрайств**

Ефективна боротьба з фінансовим 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.

Формування системи забезпечення захисту банківських операцій від шахрайства має бути напрямлена, по-перше, на найбільш вразливі до атаки об‘єкти. У межах даного дослідження розроблено науково-методичний підхід для оцінювання ризику фінансових шахрайств на основі аналізу набору індикаторів, що характеризують фінансову транзакцію, шляхом нейронного моделювання. Оскільки жоден банк не надає повну інформацію щодо реально здійснених транзакцій через конфіденційність, об’єктом дослідження було обрано згенеровану базу даних з загальнодоступного ресурсу Kaggle [51].

Штучна нейронна мережа побудована за принципом організації та функціонування біологічних нейронних мереж – нервових клітин живого організму Штучна нейронна мережа є системою з’єднаних і взаємопов’язаних між собою простих процесорів (штучних нейронів). Кожен процесор подібної мережі має справу лише з сигналами, які він періодично отримує, та сигналами, які він періодично надсилає іншим процесорам. Нейрони організовані у шари. Кількість шарів для кожної мережі індивідуально і залежить від прикладного завдання, що розв'язується. Технічно нейронні мережі не програмуються, а навчаються. Тобто штучні нейронні мережі спроможні моделювати закономірності у певній інформаційніій базі навіть без

відомостей щодо можливих значень результативного показника завдяки своїй здатності до самоорганізації.

Структурно штучний нейрон складається із вхідних сигналів (синапси), суматора (додавання зважених сигналів, які надходять по міжнейронних зв'язках від інших нейронів або зовнішніх вхідних сигналів) та функціонального перетворювача (функція активація). У загальному випадку функція активації є нелінійною, що дозволяє описати нелінійну природу нейронної мережі та ефективно відтворити складні нелінійні функціональні залежності [52].

У межах даного дослідження запропоновано науково-методичний підхід для визначення шахрайських фінансових операцій в соціальних мережах, що передбачає поетапне виконання наступних кроків:

Етап 1. Відбір системи інформативних ознак, що несуть у собі достатню для побудови нейромоделі інформацію, та формування статистичної інформації по ним.

Етап 2. Структурний синтез – етап, на якому ідентифікується топологія зв'язків, обираються нейрони, що надалі визначають принцип функціонування мережі та її ефективність для оцінювання ризику фінансових кібершахрайств

Етап 3. Параметричний синтез – етап, на якому відбувається навчання нейромережевої моделі.

Етап 4. Оптимізація побудованої нейромоделі для оцінювання та прогнозування ризику фінансових кібершахрайств.

Проведення розрахунків здійснюється програмним додатком Statistica. Об'єм вибірки складає 549 645 спостереження (2141 з них – шахрайські). У таблиці 1.2 наведені змінні, що використовуємо для аналізу.

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

Таблиця 1.2 – Змінні, що використовуються визначення ризиків шахрайства

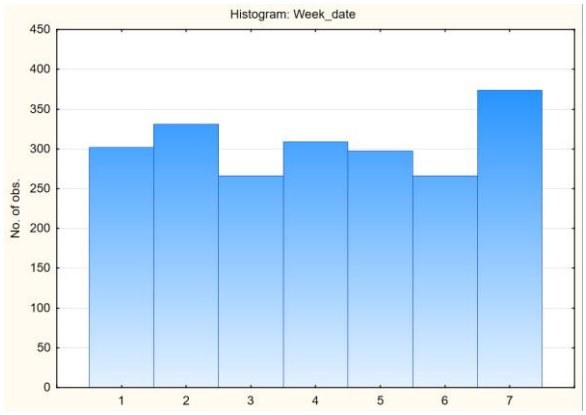
№	Назва змінної	Пояснення
1	Категорія платежів /category	Вид категорій товарів/послуг, які були об'єктом фінансової транзакції. Датасет містить 16 категорій платежів: 1 – personal_care; 2 – health_fitness; 3 – misc_pos; 4 – travel; 5 – kids_pets; 6 – shopping_pos; 7 – food_dining; 8 – home; 9 – food_dining; 10 – entertainment; 11 – shopping_net; 12 – misc_net; 13 – misc_pos; 14 – grocery_net; 15 – grocery_pos; 16 – gas_transport
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 тижня / Week date	День тижня проведення операції (від 1 до 7)
7	fraud	Чи є операція шахрайською (0 – ні, 1 – так)
8	cc_num	Номер карткового рахунку

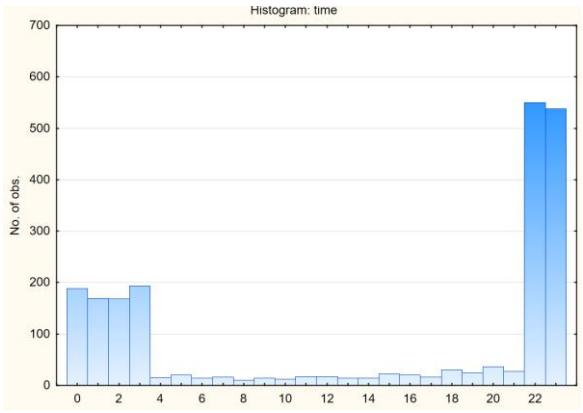
Фрагмент вхідної статистичної бази для оцінювання ризику фінансових шахрайств подано в таблиці 1.3.

Таблиця 1.3 – Вхідні дані характеристику ризику кібершахрайств

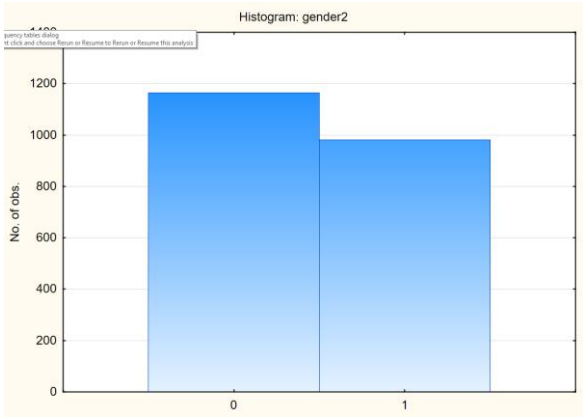
Fraud	Week date	cc_num	job	amt	birth	time	gender	Category
0	7	2,29116E+15	Mechanical engineer	2.86	53	12	M	personal_care
0	7	3,57303E+15	Sales professional, IT	29.84	32	12	F	personal_care
0	7	3,59822E+15	Librarian, public	41.28	51	12	F	health_fitness
0	7	3,59192E+15	Set designer	60.05	34	12	M	misc_pos
0	7	3,52683E+15	Furniture designer	3.19	66	12	M	travel
0	7	3,04077E+13	Psychotherapist	19.55	30	12	F	kids_pets
0	7	2,13181E+14	Therapist, occupational	133.93	71	12	F	health_fitness
0	7	3,58929E+15	Development worker, international aid	10.37	49	12	F	personal_care
0	7	3,59636E+15	Advice worker	4.37	48	12	M	shopping_pos
0	7	3,5469E+15	Barrister	66.54	65	12	F	food_dining
…	…	…	…	…	…	…	…	…

А Б





В Г



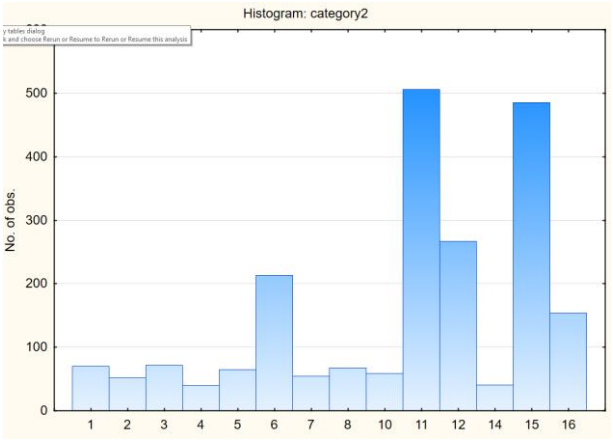


Рисунок 1.12 – Графік розподілу частоти транзакцій у розрізі досліджуваних ознак

Дані рисунку 1.12а 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. 2.2б).

Дані рисунку 1.12в демонструють, що 55% власників банківських карток, які містили ознаки шахрайства, були жінки. Найбільше незаконні транзакції проходить на купівлю продуктів та товарів (категорія 11 та 15).

Наступним етапом розробленого науково-методичного підходу є структурний синтез, що передбачає побудову нейромережевних моделей залежності ризику шахрайств від ключових факторів його формування з використанням багатошарового персептрону MLP-архітектури з використанням алгоритму BFGS.

Результати побудови нейромережевої моделі залежності ризику кібершахрайств від факторів-складових з використанням багатошарового персептрону MLP-архітектури подано на рисунку 1.13.

Summary of active networks (Spreadsheet1.sta)

Index	Net. name	Training perf.	Test perf.	Training error	Test error	Training algorithm	Error function	Hidden activation	Output activation
1	MLP 7-6-	0,58637	0,55240	0,00571	0,00584	BFGS 87	SOS	Exponentia	Exponentia
2	MLP 7-10-	0,69692	0,67258	0,00447	0,00459	BFGS 270	SOS	Tanh	Tanh
3	MLP 7-5-	0,59891	0,55348	0,00557	0,00582	BFGS 138	SOS	Tanh	Exponentia
4	MLP 7-5-	0,59372	0,56108	0,00564	0,00575	BFGS 341	SOS	Exponentia	Exponentia
5	MLP 7-8-	0,66196	0,63011	0,00489	0,00505	BFGS 338	SOS	Logistic	Tanh

Рисунок 1.13 – Результати побудови нейромережевих моделей залежності ризику кібершахрайств від факторів-складових

Детальний аналіз даних рисунку 1.13 дозволяє стверджувати, що спектр побудованих нейронних мереж у вигляді багатошарового персептрону MLP. Дві із п’яти представлених нейромережевих моделей (друга модель з архітектурою MLP 7-10-1, п’ята модель з архітектурою MLP 7-8-1) мають найвищий рівень ефективності, а саме на рівні не менше 0,6620 частки одиниці. Водночас три з п’яти нейромережевих моделей мають

продуктивність на рівні від 0,5864 до 0,5989 частки одиниці. Достовірність 5 побудованих моделей нейронних мереж підтверджується також показником помилки в межах навчальної, контрольної та тестової вибірки, яка приймає близькі до нульового рівня значення.

Для проведення більш ґрунтовного аналізу якості побудованих нейромережевих моделей розглянемо статистики передбачених значень ризику кібершахрайств та факторів-складових (рисунок 1.14).

	Data statistics (Spreadsheet1.sta)							
Samples	cc_num Input	amt Input	birth Input	time Input	gender2 Input	category2 Input	Week_date Input	is_fraud Target
Minimum (Train)	6,041621E+1	1,1(	16,0000	0,0000(	0,00000	1,0000(	1,00000	0,00000
Maximum (Train)	4,992346E+1	12882,7	97,0000	23,0000	1,00000	16,0000	7,00000	1,00000
Mean (Train)	4,230247E+1	90,21	48,5640	13,2904	0,40280	7,8983	3,78247	0,01768
Standard deviation (Train)	1,319230E+1	171,9	17,7160	6,7401	0,49046	4,5225	2,18718	0,13180
Minimum (Test)	6,041621E+1	1,1(	16,0000	0,0000(	0,00000	1,0000(	1,00000	0,00000
Maximum (Test)	4,992346E+1	13149,1	97,0000	23,0000	1,00000	16,0000	7,00000	1,00000
Mean (Test)	4,505042E+1	91,78	48,4880	13,2678	0,40651	7,8998	3,81784	0,01705
Standard deviation (Test)	1,356057E+1	198,2	17,6696	6,7477	0,49120	4,5268	2,20587	0,12947
Minimum (Overall)	6,041621E+1	1,1(	16,0000	0,0000(	0,00000	1,0000(	1,00000	0,00000
Maximum (Overall)	4,992346E+1	13149,1	97,0000	23,0000	1,00000	16,0000	7,00000	1,00000
Mean (Overall)	4,285208E+1	90,52	48,5488	13,2859	0,40354	7,8986	3,78954	0,01755
Standard deviation (Overall)	1,326712E+1	177,48	17,7066	6,7416	0,49061	4,5233	2,19096	0,13133

Рисунок 1.14 – Описові статистики значень ризику кібершахрайств та факторів-складових

Дані рисунку 1.14 надають узагальнену характеристику фінансових транзакцій, у т.ч. шахрайського характеру, що власників рахунків у фінансовій установі. Зокрема, середньостатистична фінансова транзакція проводилася жінкою у віці 48,5 років у середу або четверг з 13.00 до 14.00 для оплати продуктів харчування.

Аналіз статистичних характеристик побудованих нейромережевих моделей, представлених на рисунку 1.15 та в додатку А, свідчить про високу якість моделей (незначну варіацію мінімальних та максимальних рівнів як в межах навчальної, так і контрольної та тестової вибірок) та незначний рівень чутливості моделей до зміни масштабу вхідних даних.

Network weights (Spreadsheet1.sta)

Weight ID	Connections 1.MLP 7-6-1	Weight values 1.MLP 7-6-1	Connections 2.MLP 7-10-1	Weight values 2.MLP 7-10-1	Connections 3.MLP 7-5-1	Weight values 3.MLP 7-5-1
1	cc_num --> hidden neuron 1	-0,2613	cc_num --> hidden neuron 1	0,0525	cc_num --> hidden neuron 1	-4,0240
2	cc_num --> hidden neuron 2	24,2463	cc_num --> hidden neuron 2	25,3785	cc_num --> hidden neuron 2	-12,6913
3	cc_num --> hidden neuron 3	-0,4269	cc_num --> hidden neuron 3	-1,1746	cc_num --> hidden neuron 3	14,1261
4	cc_num --> hidden neuron 4	-5,9955	cc_num --> hidden neuron 4	-2,1610	cc_num --> hidden neuron 4	35,2826
5	cc_num --> hidden neuron 5	0,3327	cc_num --> hidden neuron 5	-0,3174	cc_num --> hidden neuron 5	27,9063
6	cc_num --> hidden neuron 6	0,4125	cc_num --> hidden neuron 6	-0,4648	amt --> hidden neuron 1	18,7772
7	amt --> hidden neuron 1	-0,4609	cc_num --> hidden neuron 7	-0,0748	amt --> hidden neuron 2	-23,2665
8	amt --> hidden neuron 2	5,8589	cc_num --> hidden neuron 8	-0,0484	amt --> hidden neuron 3	-0,1395
9	amt --> hidden neuron 3	4,8013	cc_num --> hidden neuron 9	-42,5145	amt --> hidden neuron 4	-70,3528
10	amt --> hidden neuron 4	0,4377	cc_num --> hidden neuron 10	0,8976	amt --> hidden neuron 5	0,5410
11	amt --> hidden neuron 5	-7,7284	amt --> hidden neuron 1	1,8963	birth --> hidden neuron 1	-2,6496
12	amt --> hidden neuron 6	-7,3084	amt --> hidden neuron 2	0,2291	birth --> hidden neuron 2	2,0735
13	birth --> hidden neuron 1	7,5904	amt --> hidden neuron 3	0,4390	birth --> hidden neuron 3	0,0485
14	birth --> hidden neuron 2	-0,3647	amt --> hidden neuron 4	0,0998	birth --> hidden neuron 4	-0,2636
15	birth --> hidden neuron 3	-0,5819	amt --> hidden neuron 5	-0,0434	birth --> hidden neuron 5	-0,7097
16	birth --> hidden neuron 4	0,5165	amt --> hidden neuron 6	-42,3234	time --> hidden neuron 1	33,6740
17	birth --> hidden neuron 5	0,1427	amt --> hidden neuron 7	1,2498	time --> hidden neuron 2	9,3340
18	birth --> hidden neuron 6	-6,3185	amt --> hidden neuron 8	2,7336	time --> hidden neuron 3	-16,2636
19	time --> hidden neuron 1	0,1784	amt --> hidden neuron 9	0,3439	time --> hidden neuron 4	-2,9899
20	time --> hidden neuron 2	1,2650	amt --> hidden neuron 10	0,5628	time --> hidden neuron 5	4,8023
21	time --> hidden neuron 3	-0,4903	birth --> hidden neuron 1	0,1272	gender2 --> hidden neuron 1	11,8304
22	time --> hidden neuron 4	-0,3112	birth --> hidden neuron 2	1,4357	gender2 --> hidden neuron 2	-29,0316
23	time --> hidden neuron 5	-24,0762	birth --> hidden neuron 3	9,3003	gender2 --> hidden neuron 3	127,4405
24	time --> hidden neuron 6	0,5436	birth --> hidden neuron 4	-2,6001	gender2 --> hidden neuron 4	-1,6147
25	gender2 --> hidden neuron 1	-6,6268	birth --> hidden neuron 5	6,8840	gender2 --> hidden neuron 5	-0,8162
26	gender2 --> hidden neuron 2	0,6188	birth --> hidden neuron 6	5,1097	category2 --> hidden neuron 1	-0,1927
27	gender2 --> hidden neuron 3	1,1960	birth --> hidden neuron 7	-2,6516	category2 --> hidden neuron 2	-4,1593
28	gender2 --> hidden neuron 4	-0,3847	birth --> hidden neuron 8	0,4990	category2 --> hidden neuron 3	-0,5874

Network weights (Spreadsheet1.sta)

Weight ID	Connections 1.MLP 7-6-1	Weight values 1.MLP 7-6-1	Connections 2.MLP 7-10-1	Weight values 2.MLP 7-10-1	Connections 3.MLP 7-5-1	Weight values 3.MLP 7-5-1
28	gender2 --> hidden neuron 4	-0,3847	birth --> hidden neuron 8	0,4990	category2 --> hidden neuron 3	-0,5874
29	gender2 --> hidden neuron 5	-1,2999	birth --> hidden neuron 9	-0,7694	category2 --> hidden neuron 4	7,7014
30	gender2 --> hidden neuron 6	-17,1868	birth --> hidden neuron 10	-62,6995	category2 --> hidden neuron 5	5,7137
31	category2 --> hidden neuron 1	0,5634	time --> hidden neuron 1	0,6689	Week_date --> hidden neuron 1	31,4874
32	category2 --> hidden neuron 2	3,6341	time --> hidden neuron 2	-2,0158	Week_date --> hidden neuron 2	-29,4272
33	category2 --> hidden neuron 3	0,5811	time --> hidden neuron 3	0,3150	Week_date --> hidden neuron 3	7,7142
34	category2 --> hidden neuron 4	-2,0556	time --> hidden neuron 4	7,5426	Week_date --> hidden neuron 4	-13,6799
35	category2 --> hidden neuron 5	0,1679	time --> hidden neuron 5	-0,0640	Week_date --> hidden neuron 5	2,8949
36	category2 --> hidden neuron 6	-0,0228	time --> hidden neuron 6	-0,4629	input bias --> hidden neuron 1	-20,0664
37	Week_date --> hidden neuron 1	0,0009	time --> hidden neuron 7	-6,3181	input bias --> hidden neuron 2	3,6992
38	Week_date --> hidden neuron 2	-0,0002	time --> hidden neuron 8	0,3152	input bias --> hidden neuron 3	24,3658
39	Week_date --> hidden neuron 3	-6,1817	time --> hidden neuron 9	0,0026	input bias --> hidden neuron 4	-8,9063
40	Week_date --> hidden neuron 4	1,2350	time --> hidden neuron 10	0,3332	input bias --> hidden neuron 5	-9,8802
41	Week_date --> hidden neuron 5	0,5424	gender2 --> hidden neuron 1	0,9557	hidden neuron 1 --> is_fraud	0,1254
42	Week_date --> hidden neuron 6	-0,3088	gender2 --> hidden neuron 2	-0,1579	hidden neuron 2 --> is_fraud	-2,3985
43	input bias --> hidden neuron 1	3,3479	gender2 --> hidden neuron 3	-0,0946	hidden neuron 3 --> is_fraud	-4,6354
44	input bias --> hidden neuron 2	-3,3351	gender2 --> hidden neuron 4	23,6766	hidden neuron 4 --> is_fraud	-3,2223
45	input bias --> hidden neuron 3	5,9892	gender2 --> hidden neuron 5	-0,7207	hidden neuron 5 --> is_fraud	-3,4289
46	input bias --> hidden neuron 4	6,6156	gender2 --> hidden neuron 6	-1,0377	hidden bias --> is_fraud	-4,5542
47	input bias --> hidden neuron 5	-2,2966	gender2 --> hidden neuron 7	-0,1759		
48	input bias --> hidden neuron 6	3,7980	gender2 --> hidden neuron 8	-5,2899		
49	hidden neuron 1 --> is_fraud	-2,8213	gender2 --> hidden neuron 9	0,1286		
50	hidden neuron 2 --> is_fraud	-3,2199	gender2 --> hidden neuron 10	0,0173		
51	hidden neuron 3 --> is_fraud	1,1678	category2 --> hidden neuron 1	0,8043		
52	hidden neuron 4 --> is_fraud	-2,8156	category2 --> hidden neuron 2	-0,8911		
53	hidden neuron 5 --> is_fraud	-0,1654	category2 --> hidden neuron 3	-1,7476		
54	hidden neuron 6 --> is_fraud	3,6940	category2 --> hidden neuron 4	-0,2712		
55	hidden bias --> is_fraud	0,0774	category2 --> hidden neuron 5	-0,2949		

Network weights (Spreadsheet1.sta)

Weight ID	Connections 1.MLP 7-6-1	Weight values 1.MLP 7-6-1	Connections 2.MLP 7-10-1	Weight values 2.MLP 7-10-1	Connections 3.MLP 7-5-1	Weight values 3.MLP 7-5-1
55	hidden bias --> is_fraud	0,0774	category2 --> hidden neuron 5	-0,2949		
56			category2 --> hidden neuron 6	-0,0408		
57			category2 --> hidden neuron 7	-0,3754		
58			category2 --> hidden neuron 8	7,7285		
59			category2 --> hidden neuron 9	0,5150		
60			category2 --> hidden neuron 10	-3,0563		
61			Week_date --> hidden neuron 1	0,3169		
62			Week_date --> hidden neuron 2	1,2680		
63			Week_date --> hidden neuron 3	-0,1926		
64			Week_date --> hidden neuron 4	0,1670		
65			Week_date --> hidden neuron 5	111,1298		
66			Week_date --> hidden neuron 6	-0,1436		
67			Week_date --> hidden neuron 7	1,7150		
68			Week_date --> hidden neuron 8	-0,0355		
69			Week_date --> hidden neuron 9	-17,9089		
70			Week_date --> hidden neuron 10	-0,0090		
71			input bias --> hidden neuron 1	1,2301		
72			input bias --> hidden neuron 2	0,2855		
73			input bias --> hidden neuron 3	-0,0982		
74			input bias --> hidden neuron 4	-12,2102		
75			input bias --> hidden neuron 5	2,9202		
76			input bias --> hidden neuron 6	-4,8767		
77			input bias --> hidden neuron 7	9,3502		
78			input bias --> hidden neuron 8	0,0288		
79			input bias --> hidden neuron 9	4,5908		
80			input bias --> hidden neuron 10	18,4531		
81			hidden neuron 1 --> is_fraud	-0,4461		
82			hidden neuron 2 --> is_fraud	-2,7718		

Network weights (Spreadsheet1.sta)

Weight ID	Connections 1.MLP 7-6-1	Weight values 1.MLP 7-6-1	Connections 2.MLP 7-10-1	Weight values 2.MLP 7-10-1	Connections 3.MLP 7-5-1	Weight values 3.MLP 7-5-1
70			Week_date --> hidden neuron 10	-0,0090		
71			input bias --> hidden neuron 1	1,2301		
72			input bias --> hidden neuron 2	0,2855		
73			input bias --> hidden neuron 3	-0,0982		
74			input bias --> hidden neuron 4	-12,2102		
75			input bias --> hidden neuron 5	2,9202		
76			input bias --> hidden neuron 6	-4,8767		
77			input bias --> hidden neuron 7	9,3502		
78			input bias --> hidden neuron 8	0,0288		
79			input bias --> hidden neuron 9	4,5908		
80			input bias --> hidden neuron 10	18,4531		
81			hidden neuron 1 --> is_fraud	-0,4461		
82			hidden neuron 2 --> is_fraud	-2,7718		
83			hidden neuron 3 --> is_fraud	2,3205		
84			hidden neuron 4 --> is_fraud	-0,0568		
85			hidden neuron 5 --> is_fraud	0,1228		
86			hidden neuron 6 --> is_fraud	6,2373		
87			hidden neuron 7 --> is_fraud	14,6218		
88			hidden neuron 8 --> is_fraud	1,4856		
89			hidden neuron 9 --> is_fraud	-2,3082		
90			hidden neuron 10 --> is_fraud	-2,4977		
91			hidden bias --> is_fraud	-2,3051		

Рисунок 1.15 – Фрагмент нейронних мереж з архітектурою MLP 7-6-1 (загальна кількість шарів 7, кількість прихованих шарів 6), MLP 7-10-1 (загальна кількість шарів 7, кількість прихованих шарів 10), MLP 7-5-1 (загальна кількість шарів 7, кількість прихованих шарів 5) ризику кібершахрайств

Математичну модель другої нейронної мережі з найбільшою продуктивністю з архітектурою MLP 7-10-1 (загальна кількість шарів 7, кількість прихованих шарів 10) ризику кібершахрайств у загальному вигляді можна представити в наступному вигляді (враховуючи представлені вище ваги прихованих нейронів):

$$sn_1^{(2)} = f(v_{11}^{(1)}p_1 + v_{12}^{(1)}p_2 + \cdots + v_{16}^{(1)}p_6 + v_{17}^{(1)}p_7 + s_1^{(1)}) \quad (1.4)$$

$$sn_2^{(2)} = f(v_{21}^{(1)}p_1 + v_{22}^{(1)}p_2 + \cdots + v_{26}^{(1)}p_6 + v_{27}^{(1)}p_7 + s_2^{(1)})$$

$$sn_3^{(2)} = f(v_{31}^{(1)}p_1 + v_{32}^{(1)}p_2 + \cdots + v_{36}^{(1)}p_6 + v_{37}^{(1)}p_7 + s_3^{(1)})$$

$$sn_4^{(2)} = f(v_{41}^{(1)}p_1 + v_{42}^{(1)}p_2 + \cdots + v_{46}^{(1)}p_{16} + v_{47}^{(1)}p_7 + s_4^{(1)})$$

$$sn_5^{(2)} = f(v_{51}^{(1)}p_1 + v_{52}^{(1)}p_2 + \cdots + v_{56}^{(1)}p_6 + v_{57}^{(1)}p_7 + s_5^{(1)})$$

$$sn_6^{(2)} = f(v_{61}^{(1)}p_1 + v_{62}^{(1)}p_2 + \cdots + v_{66}^{(1)}p_6 + v_{67}^{(1)}p_7 + s_6^{(1)})$$

$$sn_7^{(2)} = f(v_{71}^{(1)}p_1 + v_{72}^{(1)}p_2 + \cdots + v_{76}^{(1)}p_6 + v_{77}^{(1)}p_7 + s_7^{(1)})$$

$$sn_8^{(2)} = f(v_{81}^{(1)}p_1 + v_{82}^{(1)}p_2 + \cdots + v_{86}^{(1)}p_6 + v_{87}^{(1)}p_7 + s_8^{(1)})$$

$$sn_9^{(2)} = f(v_{91}^{(1)}p_1 + v_{92}^{(1)}p_2 + \cdots + v_{96}^{(1)}p_6 + v_{97}^{(1)}p_7 + s_9^{(1)})$$

$$sn_{10}^{(2)} = f(v_{101}^{(1)}p_1 + v_{102}^{(1)}p_2 + \cdots + v_{106}^{(1)}p_6 + v_{107}^{(1)}p_7 + s_{10}^{(1)})$$

$$\tilde{R} = h^{(3)} = f(v_1^{(2)}sn_1^{(2)} + v_2^{(2)}sn_2^{(2)} + v_3^{(2)}sn_3^{(2)} + v_4^{(2)}sn_4^{(2)} + v_5^{(2)}sn_5^{(2)} + v_6^{(2)}sn_6^{(2)} + v_7^{(2)}sn_7^{(2)} + v_8^{(2)}sn_8^{(2)} + v_9^{(2)}sn_9^{(2)} + v_{10}^{(2)}sn_{10}^{(2)} + s^{(2)})$$

де f(-) – специфікація функції активації прихованих нейронів, в нашому випадку логістична функція;

$sn_1^{(2)}$ – вихід першого прихованого нейрону в розрізі другого шару нейронної мережі, входи якого є приховані нейрони першого шару $v_{11}^{(1)}p_1, v_{12}^{(1)}p_2, \ldots, v_{16}^{(1)}p_6, v_{17}^{(1)}p_7$ та $s_1^{(1)}$. Інші $sn_1^{(2)}$, $sn_2^{(2)}$, $sn_3^{(2)}$, $sn_4^{(2)}$, $sn_5^{(2)}$, $sn_6^{(2)}$, $sn_7^{(2)}$, $sn_8^{(2)}$, $sn_9^{(2)}$, $sn_{10}^{(2)}$ – аналогічно;

$h^{(3)}$ - вихід прихованих нейронів в розрізі третього шару нейронної мережі; входами для даних виходів є зважені виходи прихованих нейронів другого шару нейронної мережі $sn_1^{(2)}$, $sn_2^{(2)}$, $sn_3^{(2)}$, $sn_4^{(2)}$, $sn_5^{(2)}$, $sn_6^{(2)}$, $sn_7^{(2)}, sn_8^{(2)}, sn_9^{(2)}, sn_{10}^{(2)}$.

В якості специфікації функції активації виходу нейронної мережі в нашому випадку є функція тангенса:

$$OUT = \tanh(net) \tag{1.5}$$

де OUT – виходи прихованих нейронів нейронної мережі в розрізі третього шару $\mathrm{h}^{(3)}$;

net – сума вхідних сигналів, зважених на відповідні вагові коефіцієнти для другого шаре, наприклад $sn_1^{(2)} = f(v_{11}^{(1)}p_1 + v_{12}^{(1)}p_2 + \cdots + v_{16}^{(1)}p_6 + v_{17}^{(1)}p_7 + s_1^{(1)}$ для $\mathrm{h}_1^{(2)}$.

Переходячи до опису моделі (1.4) на основі реальних даних отримаємо:

$$\begin{aligned} sn_1^{(2)} &= f(0.0525p_1 + 1.8963p_2 + 0.1272p_3 + 0.6689p_4 + 0.9557p_5 \\ &\quad + 0.8043p_6 + 0.3169p_7 + 1.2301) \end{aligned} \tag{1.6}$$

$$\begin{aligned} sn_2^{(2)} &= f(25.3785p_1 + 0.2291p_2 + 1.4357p_3 - 2.0158p_4 - 0.1579p_5 \\ &\quad - 0.8911p_6 + 1.2680p_7 + 0.2855) \end{aligned}$$

$$\begin{aligned} sn_3^{(2)} &= f(-1.1746p_1 + 0.4390p_2 + 9.3003p_3 + 0.3150p_4 - 0.0946p_5 \\ &\quad - 1.7476p_6 - 0.1926p_7 - 0.0982) \end{aligned}$$

$$\begin{aligned} sn_4^{(2)} &= f(-2.1610p_1 + 0.0998p_2 - 2.6001p_3 + 7.5426p_4 \\ &\quad + 23.6766p_5 - 0.2712p_{16} + 0.1670p_7 - 12.2102) \end{aligned}$$

$$sn_5^{(2)} = f(-0.3174p_1 - 0.0434p_2 + 6.8840p_3 - 0.0640p_4 - 0.7207p_5 - 0.2949p_6 + 111.1298p_7 + 2.9202)$$

$$sn_6^{(2)} = f(-0.4648p_1 - 42.3234p_2 + 5.1097p_3 - 0.4629p_4 - 1.0377p_5 - 0.0408p_6 - 0.1436p_7 - 4{,}8767)$$

$$sn_7^{(2)} = f(-0.0748p_1 + 1.2498p_2 - 2.6516p_3 - 6.3181p_4 - 0.1759p_5 - 0.3754p_6 + 1.7150p_7 + 9{,}3502)$$

$$sn_8^{(2)} = f(-0.0484p_1 + 2.7336p_2 + 0.4990p_3 + 0.3152p_4 - 5.2899p_5 + 7.7285p_6 - 0.0355p_7 + 0{,}0288)$$

$$sn_9^{(2)} = f(-42.5145p_1 + 0.3439p_2 - 0.7694p_3 + 0.0026p_4 + 0.1286p_5 + 0.5150p_6 - 17.9089p_7 + 4{,}5908)$$

$$sn_{10}^{(2)} = f(0.8976p_1 + 0.5628p_2 - 62.6995p_3 + 0.3332p_4 + 0.0173p_5 - 3.0563p_6 - 0.0090p_7 + 18{,}4531)$$

$$\tilde{R} = h^{(3)}$$

$$= f(-0{,}4461sn_1^{(2)} - 2{,}7718sn_2^{(2)} + 2{,}3205sn_3^{(2)} - 0{,}0568sn_4^{(2)} + 0{,}1228sn_5^{(}$$

$$+ 6{,}2373sn_6^{(2)} + 14{,}6218sn_7^{(2)} + 1{,}4856sn_8^{(2)} - 2{,}3082sn_9^{(2)}$$

$$- 2{,}4977sn_{10}^{(2)} - 2{,}3051$$

Заключним етапом розробленого науковметодичного підходу є прогнозування ризику кібершахрайств на основі побудованої нейромережевої моделі для заданого набору факторів. Прогнозні значення факторних ознак представлені у графах cc_num, amt, bith, time, gender2, category2, week_date рисунку 6. Графи 1.is_fra, 2.is_fra, 3.is_fra, 4.is_fra, 5.is_fra відповідно відображують розрахункові прогнозні значення ризику кібершахрайств, обчислені за допомогою 5 згенерованих моделей багатошарового перспептрону MLP. Найкращою за показниками ефективності виявлено другу модель, тому і отримані на основі її використання прогнозні значення було обрано для проведення подальшого аналізу. Таким чином, для усіх

розглянутих 10 випадків, ризик кібершахрайств коливається в межах від 0,75 до 0,94 частки одиниці.

	Custom predictions spreadsheet (Spreadsheet1.sta)											
Cases	1.is_fra	2.is_fra	3.is_fra	4.is_fra	5.is_fra	cc_num	amt	birth	time	gender2	category2	Week_date
1	0,96168	0,94320	0,88327	0,98393	0,95380	2,242177E+1	981,22	62,0000	23,0000	1,00000	11,0000	1,00000
2	0,00000	0,75258	0,00512	0,00000	0,42858	2,242177E+1	6,600	62,0000	3,0000	1,00000	16,0000	2,00000
3	0,83955	0,85077	0,75037	0,93907	0,86899	6,390464E+1	835,25	35,0000	23,0000	1,00000	11,0000	4,00000
4	0,36367	0,85875	0,43613	0,59975	0,85652	3,741252E+1	837,53	51,0000	18,0000	1,00000	6,0000	5,00000
5	0,85933	0,76831	0,97557	0,68492	0,75416	1,800400E+1	806,56	64,0000	23,0000	0,00000	12,0000	3,00000
6	0,84744	0,89788	0,82565	0,85672	0,88906	6,390464E+1	1158,64	35,0000	23,0000	1,00000	11,0000	3,00000
7	0,68508	0,90323	0,75006	1,01049	0,95427	4,423489E+1	916,68	64,0000	22,0000	1,00000	6,0000	1,00000
8	0,99750	0,93088	0,89713	1,00583	0,90602	6,011493E+1	991,10	35,0000	22,0000	1,00000	11,0000	1,00000
9	0,00000	0,76872	0,13999	0,00000	0,66164	3,596217E+1	716,96	33,0000	0,0000	0,00000	6,0000	6,00000
10	0,00000	0,67645	0,35472	0,00000	0,54593	3,051820E+1	855,54	46,0000	1,0000	0,00000	6,0000	1,00000

Рисунок 1.16 – Прогнозні значення ризику кібершахрайств

Отже, запропонований науково-методичний підхід до оцінювання ризику фінансових кібершахрайств може використовуватися для привентивних заходів попередження незаконних транзакцій за посередництва фінансової устанвои та підвищити рівень внутрішнього фінансового моніторингу.

Для удосконалення існуючої системи протидії шахрайству з платіжними картками доцільно реалізувати наступний комплекс заходів:

– 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;

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

1.4. **Науково-методологічне підґрунтя визначення фінансових шахрайств у соціальних мережах**

Популярність соціальних медіа до сьогодні зростає дуже високими темпами, більше половини населення планети є активними користувачами соціальних мереж. Так, за даними аналітичного ресурсу Datareportal, станом на жовтень 2022 року кількість їх активних користувачів становить 4.74 млрд, що складає 59,3% відносно населення Землі. Варто зазначити, що показник темпу приросту визначено на рівні +4,2% щороку [53, 54].

Такі успіхи цих соціальних структур є цілком виправданими: Facebook, Instagram, Twitter тощо охоплюють різні сторони інтересів окремо взятого індивіда, оскільки дають великий перелік інструментів для віртуальної взаємодії одного користувача з усією спільнотою мережі. Наприклад, найвідоміший Facebook досяг такої величини різновікової аудиторії за рахунок широкого спектру контенту, який дозволяє розміщувати; Instagram, переважним чином – мережа яскравого фото- та відеоконтенту, тому найбільше приваблює молодих людей; Twitter, більшою мірою, покликаний для дещо локалізованого обговорення суспільних подій у вигляді невеликих реплік різних користувачів, що формують так звані треди (англ. thread – нитка). Інших сервісів існує дуже багато, але можна констатувати: кожен, хто має доступ до мережі Інтернет, може знайти соціальний медіаресурс, що відповідатиме індивідуальним потребам.

Така масова залученість користувачів Інтернет до соціальних взаємодій у віртуальному середовищі посприяла розвитку різних злочинних схем, які сьогодні широко використовуються шахраями. У даній статті шахрайство розглядаємо у розрізі соціальної інженерії, яка простежується в україно- та російськомовному сегменті соціальних мереж, оскільки громадяни України,

які стають жертвами шахраїв, втрачають свою купівельну спроможність, що, у свою чергу, набуваючи масового характеру, негативно впливає на розвиток економіки у цілому.

Соціальна інженерія як наука вивчає способи впливу на діяльність груп або окремих людей, досліджуючи причини різної поведінки, а також середовища та обставини, у яких вона проявляється [55, 56, 57]. Власне, наша сконцентрованість саме на цій науці продиктована частою застосовуваністю її прийомів зловмисниками, які жадають отримати ту чи іншу вигоду зі своїх жертв у соціальних медіа. Поширеність її пояснюється відносною легкістю опановування технік шахраєм, оскільки для роботи з ними, здебільшого, не потребується потужна обчислювальна техніка чи спеціальні знання. В Інтернеті існують форуми, присвячені даній тематиці, де соціальні інженери анонімно обговорюють ситуації, у яких їм доводилося діяти тощо, тому базовим навичкам маніпуляцій може навчитися будь-який потенційний злочинець, хоч і багато контенту на таких веб-сайтах знаходиться в обмеженому доступі.

Задача злочинця, який займається соціальною інженерією полягає у знаходженні найбільш гострих потреб, які психологічно тиснуть на особу. Факторами такого роду можуть бути дешеві речі в онлайн-магазині; високооплачувана робота; дуже цінні призи; емпатія до людей, які потрапили у надзвичайно скрутне становище тощо [58]. Багато з подібних прийомів, внаслідок складного фінансового становища громадян України через війну з Росією, нині можуть мати особливо великий вплив на них. Вразливість українців сьогодні пов’язана також із безпековою ситуацією у країні, тож шахраї можуть користуватися необхідністю громадян виїхати з небезпечних територій або бажанням долучитися до волонтерського руху.

Усе вищезазначене підтверджує актуальність глибокого аналізу соціальних мереж для протидії кібершахрайству та легалізації кримінальних доходів в умовах цифровізації економіки України та суспільного життя в усіх його аспектах.

Отже, мета даного дослідження полягає в аналізі коментарів соціальної мережі для виявлення певних текстових шаблонів, використовуваних членами спільноти, які можуть вказувати на спроби маніпуляцій читачами та подальше шахрайство. За наявності великого обсягу даних, досягнення вказаної цілі обумовлює необхідність використання парсера загальнодоступного контенту, а також програмного забезпечення для data-mining, щоб виконати задачу кластеризації сукупності отриманих записів та виокремити найбільш цікаві, з точки зору знаходження потенційно шахрайських умислів.

Сучасна інтеграція соціальних мереж у суспільне життя спонукає членів світової наукової спільноти займатися їх дослідженнями у багатьох аспектах, аби детально вивчити вплив, який вони мають у різних площинах людської діяльності.

З моменту свого виникнення соціальні мережі постійно підтримуються та оновлюються розробниками, їх можливості стають ширшими, у тому числі, для підприємців різної величини, тож Д. Еппел, Л. Греваль, Р. Хаді та А. Т. Стефен [59] намагалися спрогнозувати майбутнє соціальних медіа у маркетингових дослідженнях; загалом, проаналізувавши наукометричну базу Scopus, нами було встановлено, що ролі соціальних мереж у маркетингу науковцями присвячується велика кількість наукових робіт. М. Сінеллі, Г. Ф. Моралес, А. Галеаззі, В. Кватросіоччі, М. Старніні [60] займалися дослідженням ефекту ехокамер у середовищі віртуальних соціальних зв’язків, бо актуальність проблеми неможливо переоцінити: сформувавши коло однодумців, яке, під впливом певних факторів, опинилося у стані ізоляції від зовнішнього інформаційного середовища, конкретно взята людина може несвідомо потрапити в оману через відсутність поглядів, відмінних від розглядуваної. Соціальна мережа як явище – це, без перебільшення, один з центрів діяльності глобального суспільства; цифровий хаб, у якому генерується історія інформаційної ери, тому абсолютно обґрунтованою є увага, яка приділяється науковцями зі сфери суспільних наук.

Іншою складовою нашого дослідження, у нерозривному зв’язку з медіа, є соціальна інженерія. Так, Ф. Саладін та Н. Каабоуч [61] досліджували методи мануальних чи комп’ютерних атак шахраїв з умінням використовувати людську схильність до довіри у мережі Інтернет. Варто зазначити, що, судячи з кількісних результатів пошукової видачі бібліографічної бази даних Scopus, даній тематиці приділяється значно менше уваги, порівняно з соціальними мережами (станом на 7 листопада 2022 року – 403806 згадок ключа «social media» проти 23365 згадок ключа «social engineering»).

Представниками вітчизняного наукового товариства питання соціальних мереж також розглядається, хоч і не так глибоко, порівняно з іноземними колегами. Провівши пошукову роботу за відповідними ключовими словами, нами було виявлено дослідження, що охоплювали аспекти, відповідні проблемам сучасності щодо розглядуваних соціальних утворень. Наприклад, Штонда Р. М., Паламарчук Н. А. та Островський С. М. [62] розглядали соціальні медіа з точки зору загроз національній системі кібербезпеки України: тема є особливо актуальною в умовах нинішньої війни в Україні, коли супротивник намагається підірвати безпекове становище всередині країни, у тому числі, інформаційно-цифрове. Василик А. В., Іщенко О. В. [63] вивчали використання соціальних мереж комерційними організаціями для залучення персоналу, з позиції оформлення профілів компаній в сенсі естетики, наповнення контентом, бажаності бути причетним до розбудови того чи іншого бренду тощо.

На даному етапі, у площині української науки соціальна інженерія, здебільшого, розглядається на засадах, ідентичних з іноземними дослідженнями.

Феномен того рівня суспільної значимості соціальних мереж, якого вони набули, а також супроводжуюче їх кібершахрайство потребують сьогодні більш ґрунтовного вивчення, важливість якого ніколи не буде перебільшено як у майбутньому, так і нині.

Перш за все, необхідно позначити, що для аналізу було обрано таку соціальну мережу як Instagram. Цей вибір є цілком своєчасним: за результатами дослідження IT-компанії GlobalLogic, станом на липень 2022 року зазначений ресурс соціального медіа в Україні налічував понад 16,1 млн зареєстрованих користувачів. Для порівняння: найпопулярніша соціальна мережа у світі, Facebook, мала 15,45 млн українських користувачів в аналогічний період [64].

Як уже зазначалося, Instagram, переважним чином – мережа яскравого фото- та відеоконтенту, часто він генерується інфлюенсерами, які показують своє яскраве та успішне життя. Тому, почасти, їх цільовою аудиторією є амбітна верства населення – молодь, на потребах якої можуть спекулювати злочинці, що володіють навичками соціальної інженерії. З описаними знаннями про зазначену соціальну мережу, було почато процес дослідження для досягнення поставленої мети.

Конкретною складовою Instagram для аналізу було обрано коментарі під публікаціями популярних блогерів, бо, з точки зору зловмисника, правильно написаний маніпулятивний коментар може стати відправною точкою для вдалого вчинення злочину: зацікавлений читач може написати соціальному інженеру в особисті повідомлення.

Для масового збору коментарів було використано інструмент Instaloader, який призначено для завантаження публікацій з соціальної мережі Instagram повністю або частково [65]. Він працює на мові програмування Python; з усім набором функцій, необхідним для парсингу вищезазначеного контенту, робота відбувалася через консоль редактора коду Visual Studio Code. Набір параметрів, що задавався для парсингу: instaloader --user-agent Mediapartners-Google --login commente88 --comments --no-pictures --no-videos --no-captions --no-metadata-json --no-profile-pic profile *profile name*. Для потреб дослідження жодного коду додатково не потребувалося.

Результатом збору коментарів з-під публікацій стали JSON-файли, які мали наступні пари назва\значення, що цікавили нас:

– “text” : “”,
– “owner-id” : “”,
– “username” : “”

Зазначених даних достатньо для ідентифікації конкретного користувача, що опублікував коментар, у разі потреби. Варто зазначити, що під час проведення описаної операції, ми керувалися концепцією розвідки на основі відкритих джерел. У даному випадку, це означає, що дані збиралися виключно з тих публікацій, що містилися у загальнодоступних профілях, тобто автор не потребував ставати його підписником, щоб отримати доступ до вмісту сторінки.

Для виявлення схожих ознак у текстах з метою їх кластеризації найкраще використовувати бази даних з великою кількістю спостережень, тому після отримання великої кількості даних (762 JSON-файли з коментарями) було вирішено об’єднати їх в колекції, які формувалися за критерієм характеру контенту, який публікував той чи інший блогер. Для цього розроблено програмне рішення мовою Python з використанням модуля glob для отримання доступу до директорії з усіма необхідними файлами, а також бібліотеки pandas для проведення об’єднання усіх вивантажених записів (рис. 1.17).

```
import pandas as pd
import glob

json = glob.glob("*.json")

unification = pd.DataFrame()

for file in json:
    data = pd.read_json(file)
    unification = pd.concat([unification, data], ignore_index=True)
print (unification)

unification.to_json('All_comments.json', indent=10, orient='index')
```

Рисунок 1.17 – Код програми для об’єднання файлів

Для вирішення задачі кластеризації було обрано програмне забезпечення «Orange Data Mining», що надає широкий спектр засобів для візуалізованого аналізу даних та машинного навчання [66]. За замовчуванням, вказане програмне рішення не має інструментарію для майнінгу тексту, але розробники передбачили можливість встановлення необхідної надбудови.

Аналіз такого роду потребує вихідних даних у вигляді колекцій текстових документів (Corpus). Формат електронних таблиць Excel є цілком прийнятним варіантом для завантаження, тому вміст сформованих, відповідно до характеру контенту, файлів формату .json, що містить зібрані коментарі, нами було імпортовано у створений файл формату .xlsx за допомогою Excel Power Querry.

Для потреб дослідження було побудовано модель, візуалізацію якої представлено на рисунку нижче (рис. 1.18).

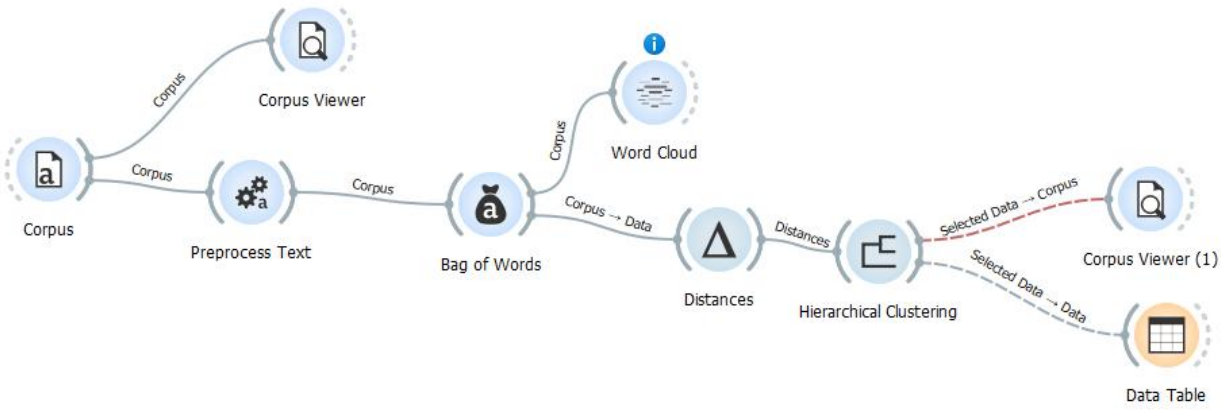


Рисунок 1.18 – Візуалізація моделі для кластеризації текстів

Вважаємо необхідним деталізувати будову даної моделі, тож розглянемо кожен з вузлів, що разом утворюють цілісну систему для розбиття спостережень таблиці на окремі кластери:

– за допомогою модуля Corpus у проєкт завантажується текстовий файл, що містить дані для аналізу.

– Corpus Viewer дозволяє переглядати вміст документа як одразу після його завантаження, так і на будь-якому етапі обробки інформації моделлю.

– задача вузла Preprocess Text полягає в розкладенні тексту на простіші складові (токени), скороченні слів до основи, нехтуючи суфіксами чи закінченнями (стемінг), а також приведенні схожих словоформ до їх основної словникової форми (лематизація). Цей інструмент дозволяє перевести увесь текст до літер нижнього регістру, прибирати знаки пунктуації та графічні елементи у вигляді смайлів, задати стоп-слова тощо. Таким чином, штучний інтелект зможе працювати з досліджуваним масивом даних.

– Bag of Words дозволяє виражати слова, що містяться у спостереженні, у вигляді їх кількостей (числами). Таким чином, можна визначати схожість виразів, використавши наступним кроком вузол Distances.

– Робота інструмента Distances полягає в обчисленні відстаней між рядками або стовпцями у наборі даних. Відстань між підготованими до цього процесу записами обчислювалася за допомогою косинуса подібності (косинус кута між двома векторами простору завантаженого документа), що дає оцінку: наскільки два спостереження схожі між собою (де -1 – записи мають зовсім різну тематику; 1 – записи ідентичні).

– Word Cloud – інструмент, який дозволяє переглянути хмару найбільш уживаних, у сукупності тексту, слів, що допомогає визначити тематику текстів з файлу. Розміщення його після Preprocess Text говорить про те, що хмару очищено від усіх неінформативних елементів.

– Віджет Hierarchical Clustering, власне, проводить ієрархічну кластеризацію даних на основі матриці відстаней і створює відповідну дендрограму, з якою можна взаємодіяти. Підключений до розглянутого вузол Corpus Viewer дозволяє досліджувати конкретно обраний кластер.

Інструменти та методи, застосовувані у процесі дослідження, дозволили нам отримати результати, висвітлені далі.

У рамках дослідження нас цікавили блоги, які стосуються таких сегментів діяльності: букмекерські контори, розважальні або лайфстайл-блоги, а також контент про інвестиції та фінанси.

Ставки на спорт діють на емоційний стан деяких людей, викликаючи нервове збудження від передбачення виграшу тієї чи іншої команди. Після проведення пошукової роботи у цьому напрямку виявлено, що зареєстровані та відповідно оформлені акаунти в Instagram мають лише функцію арбітражу трафіку у Telegram-канали: немає спроб взаємодії з аудиторією; усі пости мають мітки з псевдонімами каналів зазначеного месенджера; у шапці профілю прописані ключові слова для кращого ранжування у пошуковій видачі соціальної мережі та посилання, на якому акцентується увага (рис. 1.18).

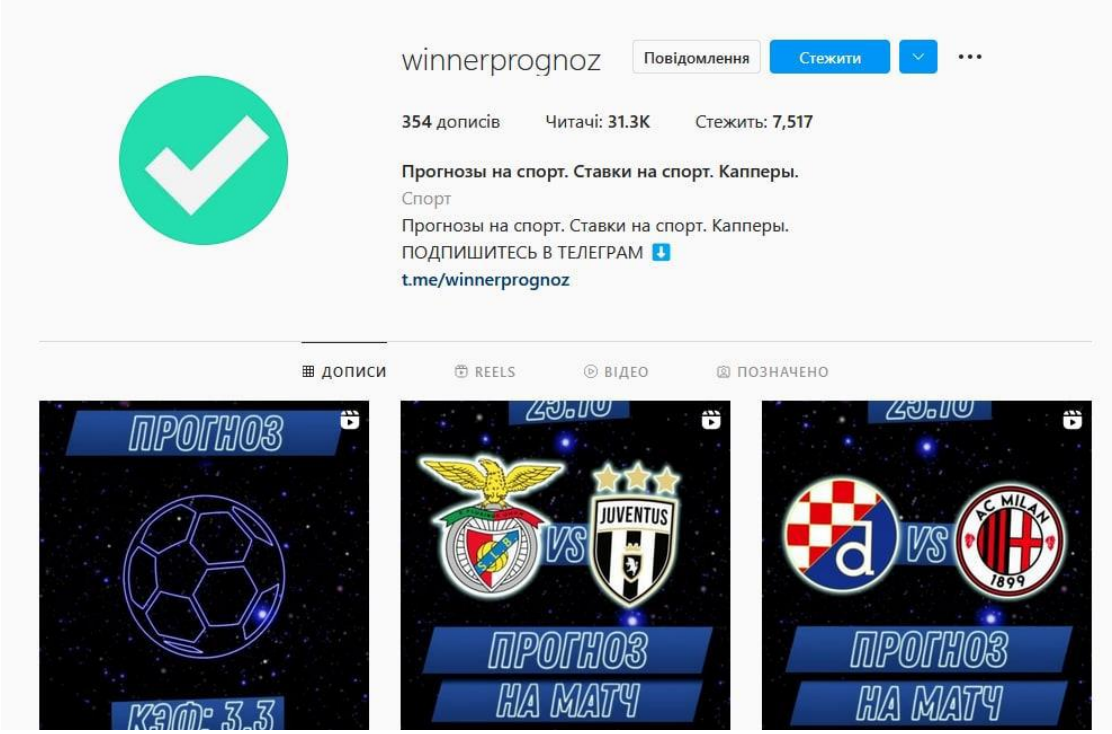


Рисунок 1.18 – Приклад арбітражної прокладки в Instagram

Користувацької активності у таких профілях майже не спостерігається (дані для подальшого аналізу відсутні), бо велика частка підписників нарощується штучно – за допомогою ботів. Результат дослідження цієї категорії блогів такий: можливі шахрайські маніпуляції, пов’язані з азартом громадян щодо спортивних подій, не розповсюджені у розглядуваній соціальній мережі; ресурси, що використовуються у злочинних цілях,

переважним чином, знаходяться у месенджері Telegram, який не лежить у площині інтересів даної роботи.

У блогерів, які розповідають про своє яскраве життя, часто формується аудиторія, яка бажає почати заробляти теж великі гроші за прикладом інфлюенсера, при цьому, не докладаючи багато зусиль для досягнення цієї мети.

Серед коментарів, зібраних під постами таких блогерів, вдалося відокремити кластер, який містить у собі дуже сконцентровану кількість спаму, порівняно з іншими групами. Його відображення представлено на рисунку нижче (рис. 1.19).

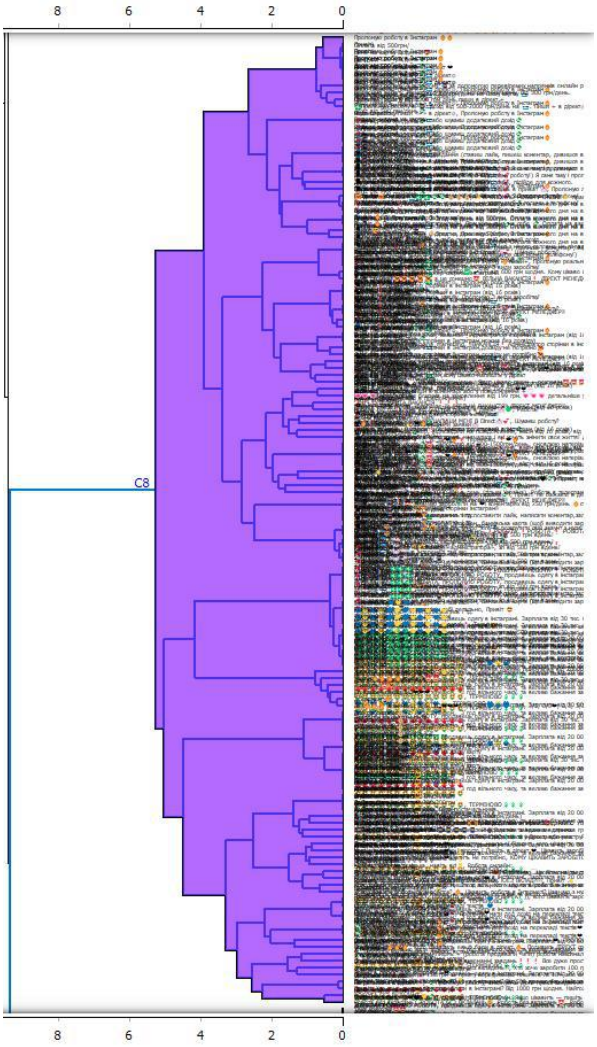


Рисунок 1.19 – Кластер зі спам-контентом

Безумовно, є багато однакових або схожих коментарів під постами, але часто вони мають на меті просто привернути увагу свого кумира. Тому варто обрати цей кластер у модулі Hierarchical Clustering та переглянути його вміст за допомогою інструмента Corpus Viewer (рис. 1.20).

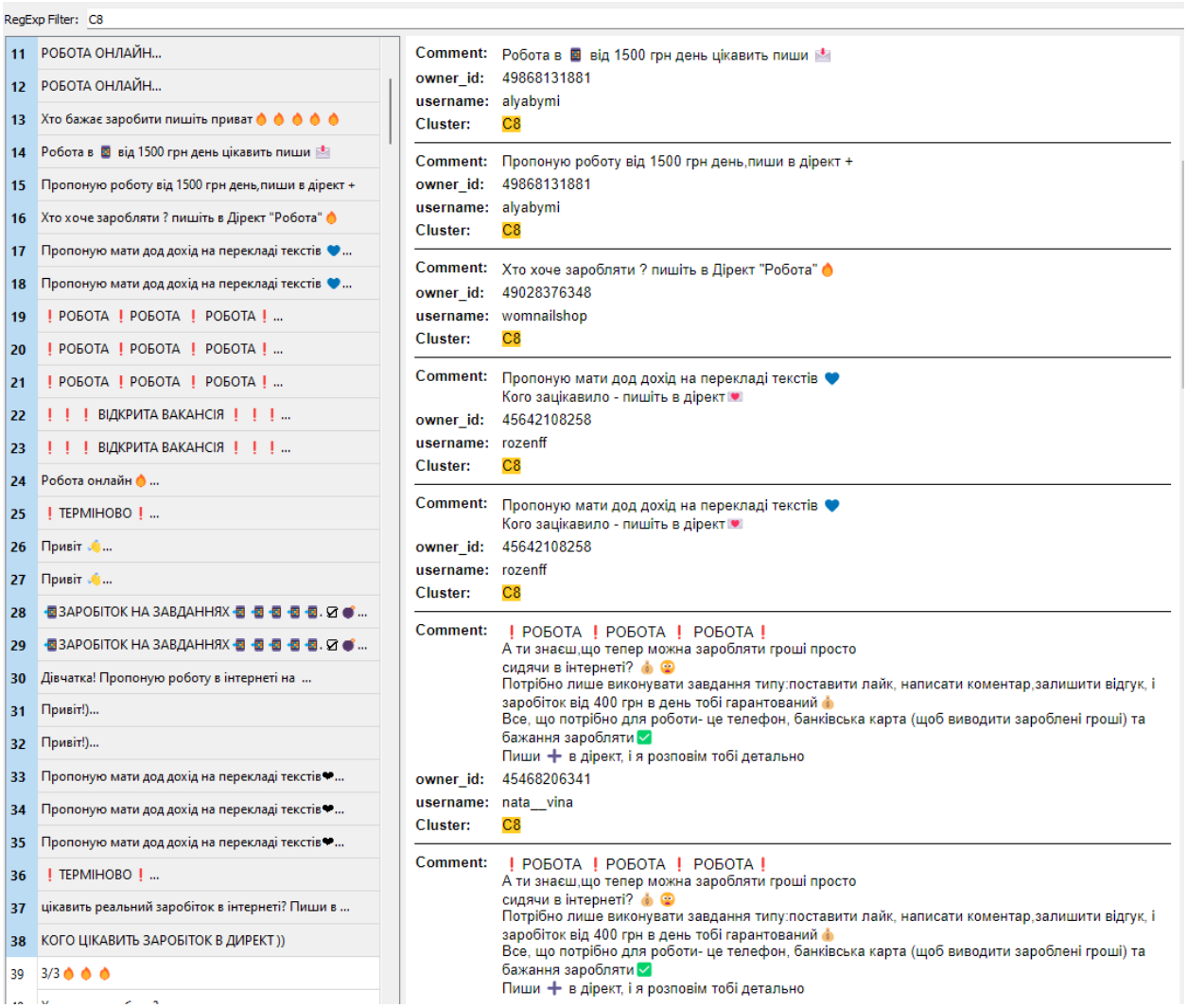


Рисунок 1.20 – Частина вмісту кластера C8

У лівій частині рисунка можна побачити велику кількість однотипних коментарів, що мають ознаки пропозиції роботи. У правій частині наведено деталізацію вмісту, з якої можна побачити, що вакансії є високооплачуваними і робота не є складною. Крім того, додається велика кількість графічних об’єктів (смайлів) для привернення уваги читачів. Також можна помітити, що деякі з таких пропозицій є більш вузько націленими. Наприклад, робота

пропонується виключно для представників жіночої статі. Подібні прояви можуть свідчити про ризик стати жертвою неправомірних дій шахраїв у подальшому. Обґрунтування пропонуємо таке: компанія, яка шукає робітників на вільні вакансії купуватиме рекламу у блогера; отримуватиме верифікацію на сайтах з пошуку роботи та розміщуватиме вакансії там. Якщо ж компанія не ризикує публікувати свої оголошення сторінках офіційних ресурсів, то це слід кваліфікувати як спроби маніпуляцій для реалізації злочинних умислів.

У ході дослідження категорії фінансових блогерів було виявлено, що їх цільовою аудиторією часто є матері у декретній відпустці, які шукають методи пасивного заробітку. Користувачі з цієї когорти вже є більш свідомими; помітно, що свої думки викладають одним закінченим коментарем. Відзначаємо, що кількість коментарів під постами популярних авторів з цього напряму, здебільшого, є не такою великою, порівняно з попередньою розглянутою категорією, спам майже відсутній. Припускаємо, що такі блогери мають модераторів, які займаються очищенням спаму та, у цілому, підозрілих текстів.

Через те, що коментарі, залишені під публікаціями, які присвячені темі фінансів та інвестицій, є унікальними, не вдалося чітко виокремити кластери через відсутність патернів. Пропонуємо переглянути приклади вмісту проаналізованого масиву даних (рис. 1.21).

З рисунка 1.21 видно, що за ключовим словом «успех» не слідує пропозицій написати в особисті повідомлення (хоча й може бути тригером для деяких читачів), думки є закінченими, майже відсутні графічні значки тощо.

Результат аналізу можна формалізувати так: піклуючись, у тому числі про свою репутацію, фінансові блогери займаються модерацією коментарів, не допускаючи шахрайських маніпулювань, спаму тощо.

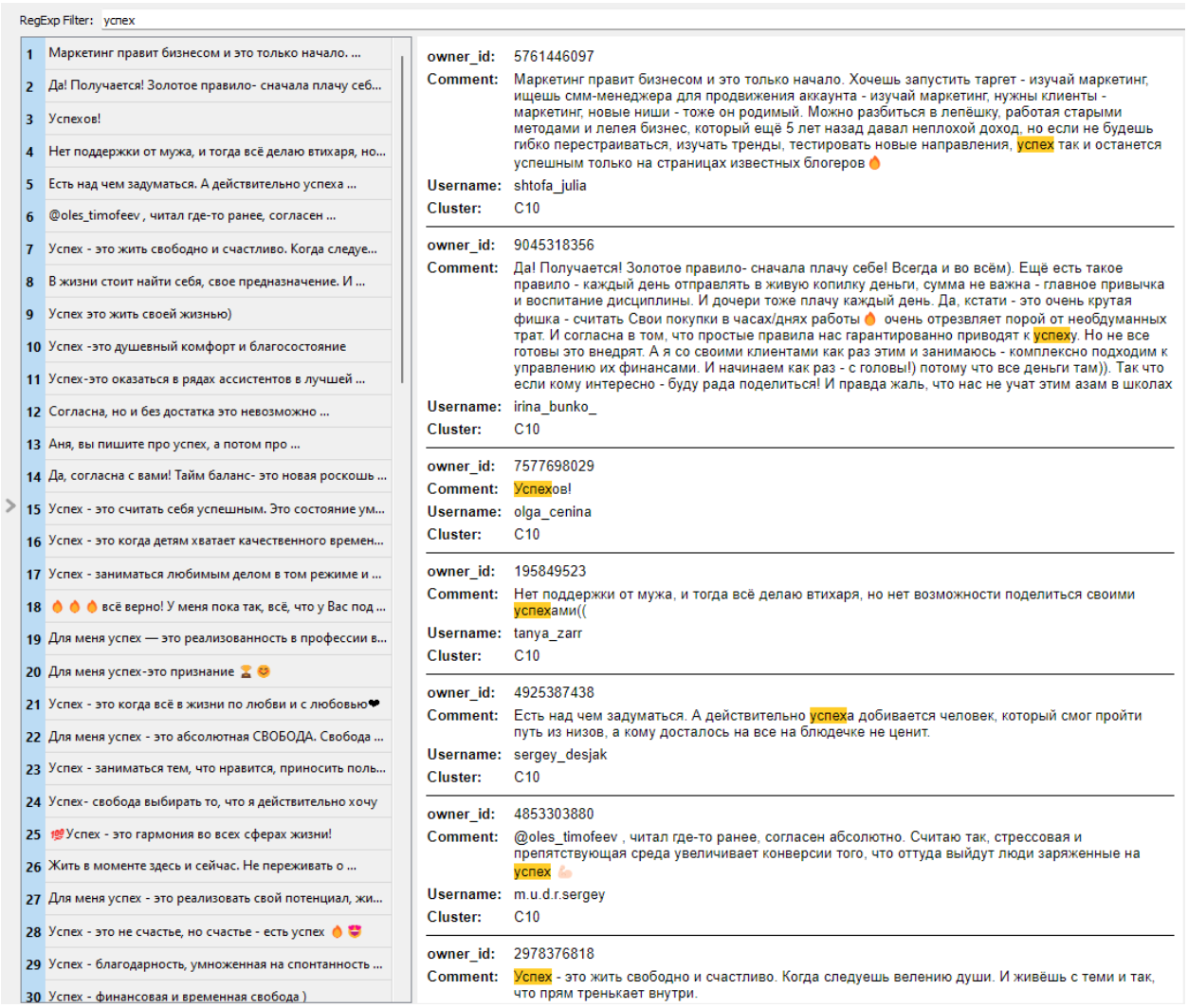


Рисунок 1.21 – Контент з ключовим словом «успех»

На даному етапі, досягши мети дослідження, необхідно зробити висновки та запропонувати рекомендації зацікавленим сторонам.

Висновки та рекомендації для стейкхолдерів. Проведений аналіз коментарів соціальної мережі Instagram з метою виявлення текстових шаблонів, використовуваних членами спільноти, які можуть вказувати на спроби маніпуляцій читачами та подальше шахрайство, показав:

Не в усіх нішах діяльності соціального інженера можуть бути реалізовані злочини в межах соцмережі, оскільки у деяких інформаційних напрямках в Instagram просто немає взаємодій з потенційною ЦА.

Ті пропозиції та заклики, які видаються дуже цікавими як для конкретних груп людей, так і загалу, і просуваються в коментарях за допомогою спаму, є небезпечними.

Деякі групи блогерів, які навчають свою аудиторію складним речам і мають високий рівень відповідальності, займаються перевіркою, у тому числі, коментарів на наявність підозрілих текстів, опублікованих іншими користувачами, спаму тощо.

Відповідно, читачам Instagram та інших соціальних мереж варто намагатися критично оцінювати заклики та пропозиції, що можуть здатися легким шляхом вирішити свої власні актуальні проблеми, оскільки шахраї експлуатують дуже бажане людиною з метою отримання вигоди за рахунок інших. Блогерам важливо піклуватися про довіру до своїх публікацій та свою репутацію, в цілому, тому необхідно забезпечувати максимальну безпеку своїх підписників. Для цього, у першу чергу, необхідно контролювати обговорення своєї спільноти. Державній службі спеціального зв'язку та захисту інформації України необхідно надалі покращувати громадський контроль у мережі Інтернет, зокрема, у соціальних мережах, аби не давати окремим інцидентам кібершахрайства розповсюджуватися, набираючи масового явища, що може негативно вплинути на суспільне становище всередині країни. Компанії Meta потрібно покращувати систему безпеки на технічному рівні, розробляючи та покращуючи нейронні мережі, здатні виявляти спроби скоєння неправомірних дій з подальшим накладенням санкцій на таких користувачів Instagram.

2 ІДЕНТИФІКАЦІЯ ІНФОРМАЦІЙНИХ ОЗНАК, ЯКІ ЗАСВІДЧУЮТЬ ЗДІЙСНЕННЯ НЕЗАКОННИХ ОПЕРАЦІЙ З КРИПТОВАЛЮТОЮ

2.1. Дослідження можливостей та загроз, які спричиняє криптовалюта для національної економіки

Світова цифрова трансформація сприяє появі нових інноваційних технологій для швидкого та надійного здійснення грошових переказів та передачі даних. Протягом осіннього десятиліття технології радикально змінили траєкторію розвитку світової фінансової системи. Поступово світ централізованих фінансів прокладає шлях до повної децентралізації. Одним з феноменів цифрової ери є поява віртуальних активів, для обліку яких використовується технологія блокчейн. Блокчейн є системою обліку, в основі якої знаходяться об’єкти у вигляді токенів – записів у системі обліку цифрових даних на основі технології розподіленого реєстру, що є ідентифікатором інформації, яка може бути, але не виключно, похідною від первинного активу [67, 68].

Одним із ключових структурних зрушень у розвитку фінансової екосистеми є розвиток децентралізованих фінансів (DeFi). Ключовими елементами цієї екосистеми є нові автоматизовані протоколи на блокчейнах – для підтримки торгівлі, кредитування та інвестування криптоактивів – і стейблкоіни, які полегшують переказ коштів. У системі децентралізованих фінансів існує «ілюзія децентралізації», оскільки необхідність управління робить певний рівень централізації неминучим, а структурні аспекти системи призводять до концентрації влади. У системі децентралізованих фінансів фінансові послуги надаються без централізованих посередників, функціонуючи виключно через автоматизовані протоколи на блокчейнах. На рисунку 2.1 представлено динаміку розвитку ринку криптовалют та DeFi за період з 3 кварталу 2020 року по 1 квартал 2022 року.

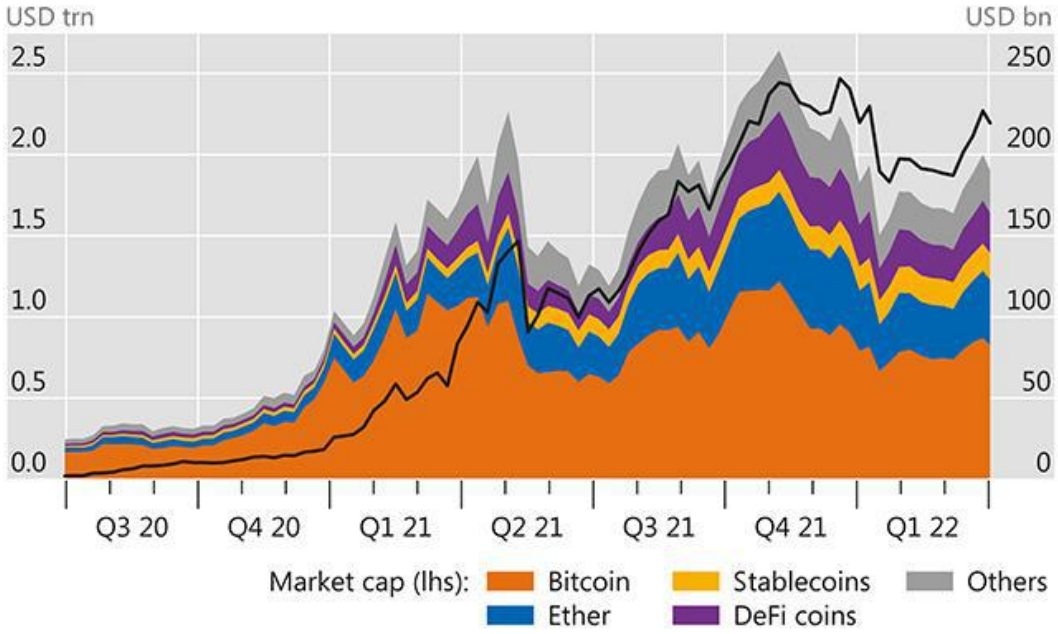


Рисунок 2.1 – Обсяг ринку криптовалют та DeFi у період 3 квартал 2020 – 1 квартал 2022

Джерело: Банк міжнародних розрахунків [69]

Хоча децентралізовані фінанси перебувають на початковій стадії свого розвитку, його суб'єкти пропонують фінансові послуги, подібні до тих, що надаються традиційними фінансовими установами, і мають подібні ризики та загрози в своїй діяльності. Оскільки екосистема цифрових активів стрімко зростає, вона стає більш взаємопов'язаним із традиційною фінансовою системою та імітує продукти та структури традиційних фінансів, створює нові потенційні проблеми для фінансової стабільності. До основних ризиків, які стосуються сфери обігу цифрових фінансових активів відносять невисокий рівень ліквідності цифрових активів та волатильність цін на цифрові активи [70].

Основними особливостями функціонування традиційних фінансів є: кошти клієнтів знаходяться у володінні компаній; клієнти довіряють компаніям свої гроші, сподіваючись, що їх кошти не будуть використані в незаконних цілях або віддані ненадійним позичальникам; транзакції можуть тривати до декількох днів, оскільки вони часто включають ручні процедури; персональні дані розкриваються фінансовим установам; оформлення

фінансових послуг підтверджується в паперовому вигляді; фінансові ринки недоступні цілодобово, існують вихідні та святкові дні.

На основі системного аналізу фахової літератури зауважимо, що система децентралізованих фінансів має наступні переваги порівняно з централізованими фінансами: швидкість транзакції; наявність коштів у кожного учасника; легкий доступ з будь-якої точки світу без налаштування банківського рахунку.

Використання смарт-контрактів на платформах DeFi потенційно усуває потребу в таких традиційних фінансових установах, що сприяє скороченню операційних витрат. Крім цього, переказ токенів може бути набагато швидшим і легшим за допомогою DeFi, ніж традиційні фінансові транзакції на внутрішньому та міжнародному рівнях.

Існують численні відмінності між традиційними та децентралізованими фінансами, такі як швидкість, вартість, доступ та інші. Основні відмінності між цими двома видами фінансів полягають в наступному:

– у DeFi всі операції проводяться у відкритому блокчейні. Отже, це основне джерело довіри. Щодо традиційних фінансів, то вони регулюються нормативно-правовими актами та ліцензіями на проведення окремих видів фінансових послуг;

– немає кордонів, які потрібно подолати користувачам DeFi. Їм потрібно зробити кілька простих дій, таких як налаштування електронного гаманця, пошук надійної платформи, вибір проекту і додавання своїх коштів;

– швидке впровадження нових продуктів. Існуючі технології дозволяють створювати різні фінансові продукти і їх миттєву реалізацію. Такі процедури забирають набагато більше часу і сил в рамках традиційної фінансової системи.

Сьогодні термін «цифровий актив» не має єдиного вичерпного визначення, яке б повною мірою розкривало суть і зміст терміну. Одна група вчених використовує термін «цифровий актив»; друга група використовує термін «криптовалюта»; третя група використовує термін «токен»; у четвертій

групі використовується термін «віртуальний актив»; п’ята група вчених використовує одночасно кілька термінів як синоніми, тобто спостерігається тісне переплетення термінів. Цей факт значно ускладнює розуміння багатьох процесів, пов’язаних з використанням цифрових активів, і досить часто впливає на спотворення та неправильне тлумачення інформації, закладеної в основу існування цифрових активів. Така термінологічна плутанина створює стійкі умови для подальшого встановлення неузгодженості та неоднозначності не лише самого терміну «цифровий актив», а й перспектив його використання. Тому актуальним є уточнення визначення терміну «цифровий актив».

Терміни «цифровий актив», «віртуальні валюти», «цифрові валюти», «криптовалюта» не мають чітко визначеного поняття в науковому просторі. Найчастіше ці поняття ототожнюються, що суперечить змісту вище наведених термінів. Адже цифровий (віртуальний) актив включає в себе глибшу суть, як інформаційний ресурс, що обертається в розподіленому реєстрі у вигляді унікального ідентифікатора [71].

Наразі існує безліч цифрових валют, в основі яких різні алгоритми їх майнігу: proof-of-work, proof-of-space й time. Цифрові валюти поділяються на централізовані та нецентралізовані цифрові валюти. Курсова вартість децентралізованої валюти безпосередньо визначається колом осіб, які її використовують. У міру того, як децентралізовані валюти стали більш популярними, також почала з'являтися концепція централізованих цифрових валют. Визнаючи потенційні переваги цифрових грошей, центральні банки та уряди почали вивчати використання форми технології блокчейн для створення цифрових валют центрального банку, також відомих як CBDC.

Централізовані цифрові валюти використовують ті ж види базової технології блокчейн, що і їх децентралізовані аналоги, але з вирішальною відмінністю: вони випускаються і контролюються централізованими установами. Таким чином, централізовані цифрові валюти не отримують вартість від своїх користувачів.

Мілош Д.В. та Герасенко В.П. [72] визначають цифрові фінансові активи як цифровий еквівалент майна, що існує в грошовій формі чи в формі різних фінансових інструментів, що використовується в якості засобу платежу чи в інвестиційних цілях. Крім того, автори пропонують розширити класифікацію цифрових фінансових активів (рис. 2.2).

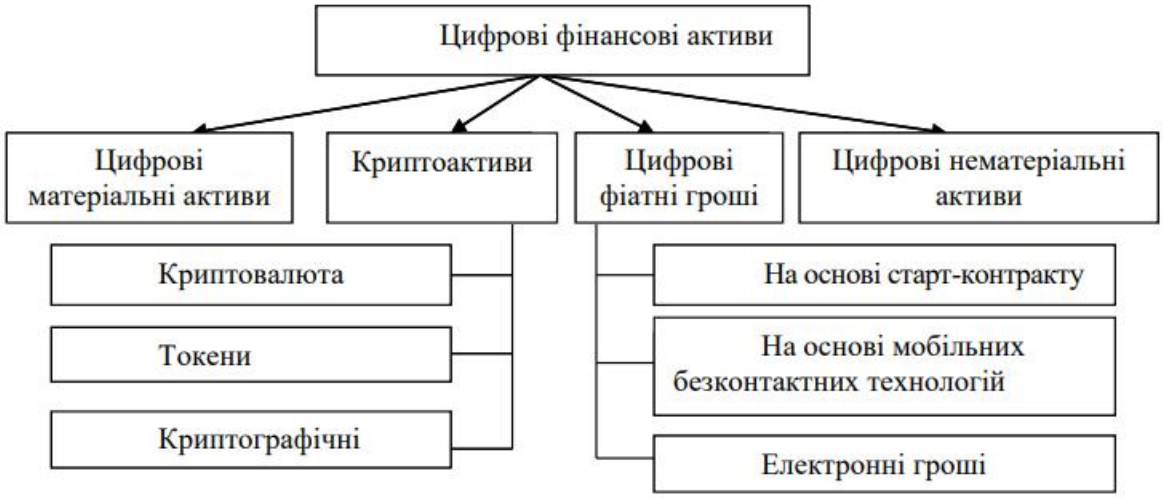


Рисунок 2.2 – Класифікація цифрових фінансових активів

Джерело: Мілош Д.В. та Герасенко В.П. [72]

Сьогодні ряд фахівців визначають криптовалюти як різновид цифрових активів. Так, провідний фахівець фінтех-компанії Ціннобер Волл визначає Ethereum як цифровий актив. Подібний підхід застосовується й до визначення біткоіна. Генеральний директор Ripple, також вважає біткойн цифровим активом, стверджуючи, що біткойн надає користувачеві можливість вирішувати конкретні реальні проблеми, що підтверджує його цінність.

Buntinx вважає, що цифровий актив існує в двійковій формі, і цифровим активом може служити будь-який тип цифрових даних: від плівки до папки на робочому столі. На думку Buntinx основною відмінністю між цифровими активами та криптовалютами є формат збережених даних. Більшість криптовалют мають ліміт пропозиції, тоді як цифрові активи, за необхідності, можна створювати (теоретично) необмежену кількість разів.

Відповідно до Закону України «Про віртуальні активи» [73], віртуальні активи – це нематеріальне благо, що є об'єктом цивільних прав, має вартість та виражену сукупністю даних в електронній формі. Існування та оборотоздатність віртуального активу забезпечується системою забезпечення обороту віртуальних активів. Віртуальний актив може посвідчувати майнові права, зокрема права вимоги на інші об'єкти цивільних прав. За класифікацією, встановленою Законом України «Про віртуальні активи», пропонується розділення цифрових активів на забезпечені та незабезпечені. Окремо у забезпечених віртуальних активах виокремлюється окремий різновид – цифрова валюта України.

Більшість країн та організацій тлумачить та класифікує цифрові активи по-різному. На рисунку 2.3 представлена систематизація сутності віртуальних активів у Франції, Великій Британії та на рівні Європарламенту.

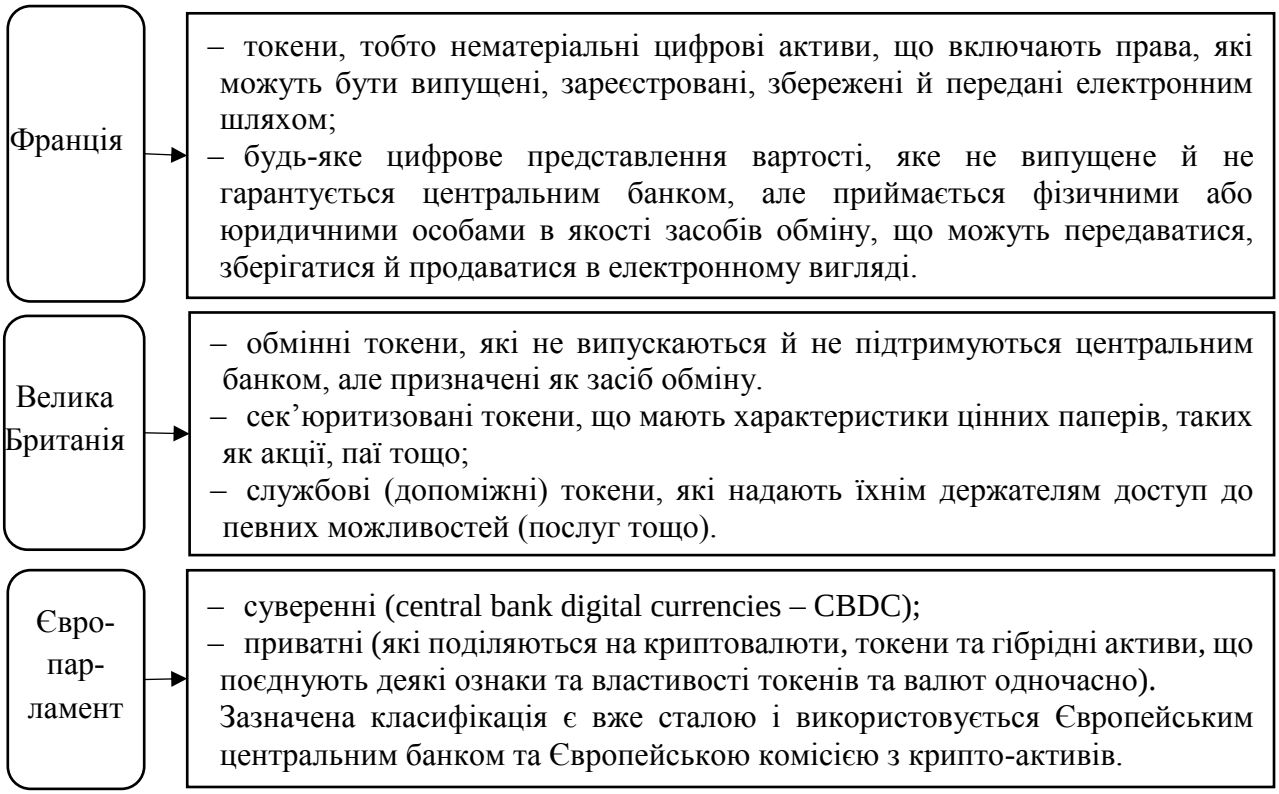


Рисунок 2.3 – Підходи до визначення цифрових активів за законодавством Франції, Великої Британії та Європарламентом

Джерело: [74]

За даними Міжнародного фінансового фонду, більше 100 країн активно розглядають шляхи створення цифрових валют центрального банку, а деякі вже почали їх використовувати (таблиця 2.4) [75]. Цифрова валюта центального банку це фактично електронна готівка. Як традиційні фіатні валюти, вона дає власникам (юридичним та фізичним особам) проводити електронні платежі та перекази.

Таблиця 2.4 – Характеристика цифрових валют країн, де CBDC запущено, знаходяться в тестуванні або в розробці

Назва валюти	Країна	Опис
Країни, де запущено CBDC		
Sand dollar (жовтень 2020)	Багамські острови	На Багамах 20% населення не мають банківського рахунку. Прогнозується, що Sand dollar може допомогти поліпшити фінансову інклюзію і зміцнити систему протидії відмивання грошей і незаконної економічної діяльності.
eNaira (жовтень 2021)	Нігерія	eNaira зберігається в цифровому гаманці і може використовуватися для безконтактних платежів в магазині, а також для переказу коштів.
DCash	Східнокарибський валютний союз	Система дозволяє користувачам навіть без банківських рахунків користуватися завантаженим застосунком і здійснювати платежі через QR-код зі смартфону
Країни, де CBDC знаходяться в тестуванні		
Електронна крона	Швеція	Шведський Ріксбанк вивчає технологічні та політичні наслідки CBDC. Однією з ключових цілей проекту є забезпечення широкого доступу до електронної крони в майбутньому. На меті є захистити людей похилого віку та людей з певними вадами, щоб переконатися, що вони не зазнали негативного впливу в безготівковому суспільстві.
e-CNY (цифровий юань, квітень 2020)	Китай	e-CNY має понад сто мільйонів індивідуальних користувачів і мільярди юанів в угодах. Країна надавала цифрові платіжні послуги юаня відвідувачам зимових Олімпійських ігор у Пекіні. Відвідувачі могли завантажити додаток цифрового гаманця юаня або зберігати гроші на фізичній картці.
Цифровий ямайський долар	Ямайка	Впровадження цифрового ямайського долару стане основою для архітектури цифрових платежів Ямайки та сприятиме більшій фінансовій інклюзії. У рамках тестового проекту було емітовано цифрової валюти на суму 230 мільйонів доларів (1,28 мільйона євро).
e-Hryvnia	Україна	e-Hryvnia може в перспективі розглядатися як альтернатива наявним методам роздрібних платежів – готівці, платіжним дорученням, платіжним карткам та електронним грошам. Перевагами е-гривні є простота використання, доступність, безпечність та швидкість розрахунків

Продовження таблиці 2.4

Країни, де CBDC знаходяться в розробці		
Цифрова рупія	Індія	«Цифрова рупія» буде заснована на технології блокчейн і, як очікується, запрацює до кінця березня 2023 року.
Цифровий євро	Єврозона	Європейський центральний банк (ЄЦБ) оголосив в липні 2021 року, що активно розглядає можливість створення цифрової версії євро.
Цифровий долар	США	Президент Джо Байден 9 березня 2022 року підписав розпорядження про підготовку до створення цифрового долара. Одним із заходів наказу є оцінка технологічної інфраструктури, необхідної для потенційного американського CBDC.

Джерело: [75]

CBDC не потребує посередників у фінансових операція і дозволяє транзакціям успішно проходити безпосередньо від однієї особи до іншої або від клієнта до постачальника. Це допомагає запобігти виникненню ризиків як для клієнта, так і для комерційного банку, оскільки створює прямий зв’язок між споживачами та центральним банком. Дана особливість, хоч і не повністю, але споріднює криптовалюти та цифрові валюти.

Ідея CBDC походить від криптовалют, таких як Bitcoin або Ethereum. Однак є і відмінності. Криптовалюти нерегульовані та децентралізовані. Вони нестабільні, оскільки їх вартість базується на інвесторах, використанні та спекуляціях. Цю волатильність можна побачити в коливаннях вартості Bitcoin за останні 12 місяців (рис. 2.4). Вартість CBDC прив'язана до валюти країни, і вони розроблені так, щоб бути більш стабільними та безпечними.

Наразі постає питання – яка різниця між CBDC та стейблкоїнами? Стейблкоіни виявилися корисними для збереження переваги долара США, оскільки оцифрування фіатної валюти або їх конвертація в токени сприяє укріпленню долара в цілому.

Більшість стейблкоїнів прив'язані до долара США, але існує попит на створення більшої кількості монет з альтернативними номіналами. Тим не менш, кілька стейблкоїнів прив'язані до таких валют, як сінгапурський долар, індонезійська рупія або євро.

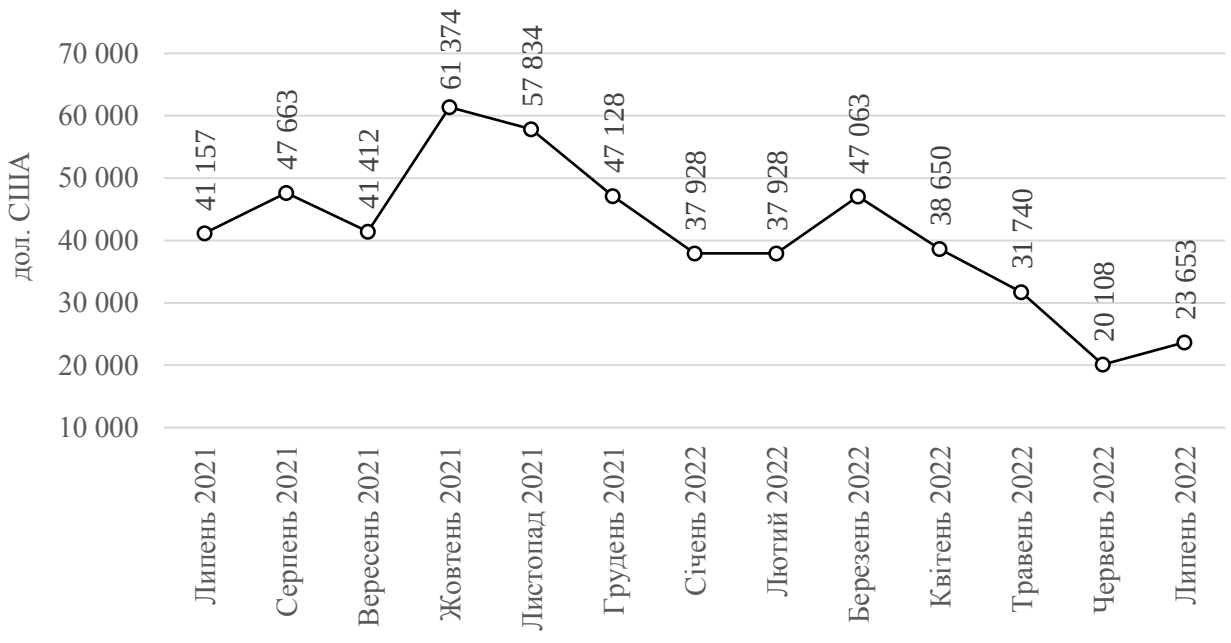


Рисунок 2.4 – Вартість Bitcoin протягом липня 2021 – липня 2022, дол. США

Джерело: [76]

Stablecoins – це приватні віртуальні цифрові активи (VDA), прив'язані до валюти, тоді як цифрова валюта Центрального банку (CBDC) має статус законного платіжного засобу, випущеного центральним монетарним органом, і є такою ж «хорошою», як і валюта країни [77].

Стейблкоїни забезпечують таку саму цінність для криптоінвесторів і трейдерів, як і фіатна валюта для учасників традиційних ринків – стабільність. Наприклад, якщо традиційні інвестори можуть вирішити розподілити частину свого портфеля на готівку або казначейські облігації, коли волатильність зростає, а криптоінвестори можуть перейти на стейблкоїни. Тобто стейблкоїни є надійним активом на нестабільному ринку, поєднуючи стабільність традиційних активів із гнучкістю цифрових. Найпопулярніші з них: Binance, Tether, USD Coin, TerraUSD, Dai, TrueUSD.

Проаналізуємо більш детальніше можливості та загрози використання цифрових активів для економіки. Цінність цифрових валют залежить тільки від віри користувачів в те, що через певний час вони зможуть їх обміняти на товари, послуги або фіатні валюти. Крім того, з розвитком ринку криптовалют

зароджуються відносини, в яких довіра між суб'єктами реалізується через технологічні інструменти (криптографічний код).

У свою чергу, на сьогодні можна виокремити 5 основних потенційних загроз, пов'язаних із функціонуванням ринку криптовалюти:

1. Анархічність системи.

Цифрові криптографічні валюти регулюються тільки закладеним в їх основу математичним алгоритмом. Таким чином, нова система позбавляє регулюючі органи виняткового права на емісію та контроль обороту грошових коштів, що призводить до соціальних змін у суспільстві, глибина яких безпосередньо залежить від масштабів цього ринку.

2. Проблема довіри

У цифрових валютах немає вартості. Це просто дані, якими ведеться обмін між покупцем, який використовує ці валюти для придбання товару за власною шкалою оцінки вартості, і продавцем, у якого є своя градація вартості. У такому випадку, при відсутності системи регулювання та контролю, їм необхідна якась ціна, щоб встановити довіру, без якої на сьогоднішній день валюта просто не може існувати.

3. Схожість з фінансовою пірамідою

Ряд дослідників порівнюють цифрову валюту з фінансовою пірамідою, яка в певний день може зникнути і призвести до втрат великої кількості грошей, і як наслідок, до зростання недовіри населення до державних структур, як би це не було парадоксально.

4. Анонімність

Існує ймовірність, що легалізація зазначених валют у найближчій перспективі призведе до зростання тіньової економіки. Транзакції з цифровими активами зазвичай пов'язані з високим ризиком незаконної діяльності (фінансові злочини, шахрайство та маніпулювання ринком) через деякі їх особливості, такі як анонімності та швидкість здійснення фінансових транзакцій. За даними Банку міжнародних розрахунків у 2019 році близько

1,1% усіх криптовалютних транзакцій (на суму близько 11 мільярдів доларів) були незаконними.

5. Обмеженість розрахунків

Зазначена проблема нерозривно пов’язана з неоднозначним ставленням регуляторів до цифрових валют, відсутністю регламентів їх обліку, а також високою вартістю захисту. Утім, у разі розвитку регулюючої бази кількість розрахунків із зазначеною валютою може значно зрости.

До вищезаначених загроз, можна додати загрозу сталому розвитку. Загалом платежі впливають на навколишнє середовище, тому важливо розуміти, як цифрові валюти може вплинути на це. Відомо, що існуючі платіжні системи, такі як готівка та кредитні картки, споживають незначну кількість енергії. Для цифрових валют велике коливання у вартості енергії пов’язане з використанням різних технологій (типів) блокчейну.

Більшість публічних мереж блокчейнів сьогодні використовують алгоритми, які називаються Proof of Work (PoW) або Proof of Stake (PoS), щоб забезпечити консенсус, тоді як приватні – або «дозволені» – блокчейни та технології розподіленого реєстру (DLTs) можна структурувати різними способами, щоб визначити пріоритет швидкості, безпеки та масштабованості [78].

Потреба у високій обчислювальній потужності є частиною дизайну систем PoW, включаючи ту, що використовує Bitcoin, перший і найвідоміший криптоактив. Відсутність централізованого органу влади означає, що рішення щодо дійсності транзакцій делегуються мережі користувачів-учасників. Для Bitcoin це досягається за допомогою механізму консенсусу Накамото PoW.8 Кожен може завантажити безкоштовне програмне забезпечення для Bitcoin, щоб зробити комп’ютер біткойн-вузлом, який може перевіряти операції. Імовірність того, що вузол додає наступну групу транзакцій до книги (шляхом формування «блок») залежить від обчислювальної потужності, витраченої на вирішення алгоритмічної задачі.

З екологічної точки зору механізми PoW мають два важливі негативні наслідки: споживання енергії та електронні відходи. Система DLT, заснована на PoW, споживає багато електроенергії під час обчислень, які виконуються вузлами, що конкурують за підтвердження транзакцій. Наприклад, станом на 25 квітня 2022 р. річне споживання електроенергії мережею Bitcoin оцінюється в 144 терават-годин (ТВт-год) на рік згідно Кембриджського індексу споживання електроенергії Bitcoin (рис. 2.5). Це становить приблизно 0,6 відсотка загального світового споживання електроенергії. Другою екологічною проблемою є електронні відходи, які стосуються електроніки, яку викидають наприкінці терміну служби [79].

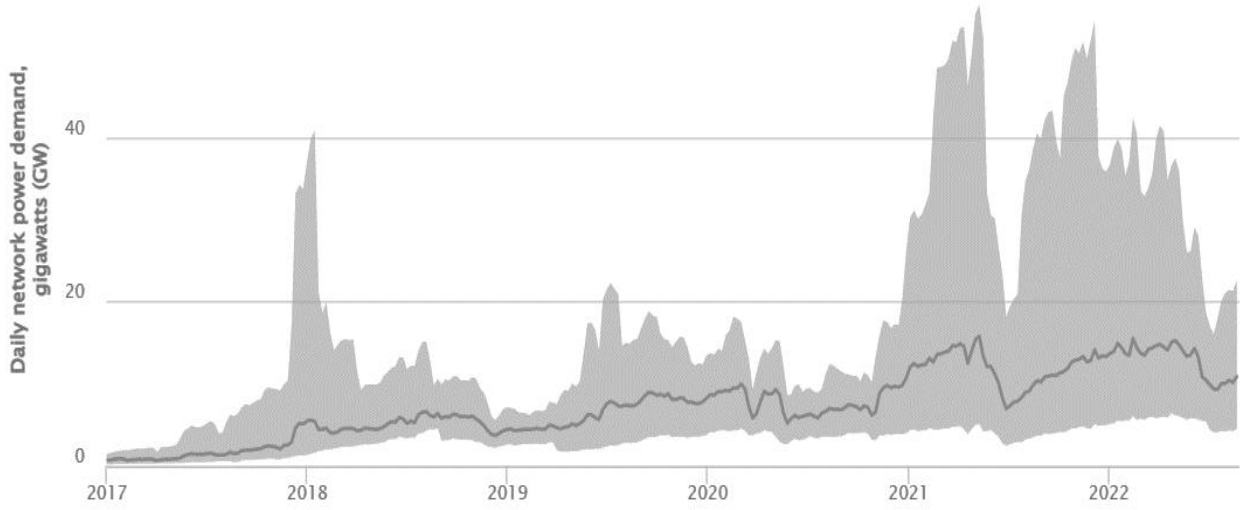


Рисунок 2.5 – Динаміка споживання електроенергії мережею Bitcoin у період 2017-2022

Джерело: Cambrige Bitcoin Electricity Consumption Index [80]

На думку Джага К. та Бача К. [81] для досягнення стабільного рівня цін на криптовалюту необхідна наявність нормативної бази та політична підтримка. Тоді як стабільний рівень цін є необхідною умовою для масового впровадження криптовалют. Лише тоді, коли всі ці вимоги виконуються, криптовалюти можуть розкрити свій повний потенціал та покращити фінансову інклюзію, зробити закордонні платежі дешевшими та більш

швидкими, розширити доступ для торгівлі для бізнесу, а також підвищити рівень соціальної довіри та зменшення корупції [82].

Отже, розвиток криптовалют та його майбутні наслідки не є однозначно зрозумілі та здатні як посилити крихкість, так і підвищити рівень фінансової безпеки країни. Багато людей все ще вибирають звичайний спосіб проведення розрахунків. Однак кількість користувачів цифрових активів швидко збільшується. Враховуючи велику кількість переваг цієї системи, вона має всі шанси в майбутньому замінити традиційну фінансову систему. У той же час, цифрові активи створюють можливості для використання криптовалют з метою провадження незаконних операцій, тому їх розвиток та поширення повинно відбуватись під контролем національних та міжнародних органів нагляду.

2.2. **Аналіз особливостей та методів використання криптовалюти з метою реалізації протиправної діяльності**

На сьогоднішній день фінансові технології щільно інтегровані у всі аспекти суспільного життя різних рівнів. Це ще більше спонукає до пошуку актуальних інструментів реалізації все зростаючих потреб ринку фінансових послуг.

Останнім часом особливого поширення на ринку фінансових послуг набуває новітня фінансова технологія криптовалюта як важливий напрям у фінансових дослідженнях. Використання криптовалюти сприяє реформуванню та трансформації фінансового рикну, зростанню цифрової економіки, збільшенню ефективності розподілу фінансових ресурсів. Ринок криптовалюти швидко набирає оберти та постає альтернативною фінансовою платформою до традиційного ринку фінансових послуг.

У той же час стрімкий розвиток криптовалютного ринку має і свої суттєві недоліки: нормативно-правова, законодавча база криптовалюти ще не достатньо сформована, що викликає особливу зацікавленість у представників злочинної сфери з метою отримання незаконного прибутку, тобто

використання криптовалюти в якості інструменту реалізації фінансових злочинів, таких як відмивання нелегальних доходів, фінансування тероризму, фінансування розповсюдження зброї масового знищення, корупція. В результаті, актуальності набуває пошук нових методик протидії та боротьби з проведенням шахрайських операцій відмивання нелегальних коштів з криптовалютою, які ґрунтуються на ідентифікації, досконалому аналізі та прогнозуванні ознак незаконних транзакцій та схем з використанням криптовалюти.

Поняття, особливості, функції, фактори, чинники, ознаки, проблеми, учасників операцій з криптовалютою розкривають у своїх роботах ряд вчених, а саме: Чжао Л. [83] опиує функції, вплив та проблеми криптовалюти у контексті фінансових технологій; Лю РХ.Ф., Рен Х., Лю С., Цзян Х. [84] охарактеризовують ключових агентів у криптовалютній економіці; Бейлі А. М., Реттлер Б., і Вармке К. [85] визначають філософію, політику та економік криптовалюти; Лопес-Мартін К., Беніто Муела С. і Аргедас Р [86] розкривають ефективність криптовалютних ринків; Хак І. У., Манінгам А., Чупрадіт С., Суксатан В. і Хуо К. [87] досліджують управління ризиками на ринку криптовалют; Махдаві-Дамгані Б., Фрейзер Р., Хауелл,Дж., і Халдорссон Дж.С. [88] описують особливості секторизації криптовалюти за допомогою кластеризації та веб-скрейпінгу; Фанг Ф., Вентре К., Басиос М., Кантан Л., Мартинес-Рего Д., Ву Ф., Ли Л. [89] висвітлюють новітні тенденції з питання торгівлі криптовалютою; та ін.

Економічно-правовий характер роботи з криптовалютою у різних країнах має суттєві відмінності, про які у своїх матеріалах пишуть сучасні наукові діячі: Бзікер З. [90] щодо статусу криптовалюти в Марокко; Віджая Г. [91] стосовно ролі криптовалюти в Індонезійському центральному банку; Райлі Дж. [92] про сучасний стан регулювання криптовалюти в Китаї та його вплив у всьому світі; Уквуезе Ф. О. [93] щодо специфіки роботи з криптовалютою у Нігерії та Південній Африці; Дельва Бенавідес Дж. Е., і

Торрес Амайя Ф. Е. [94] про юридичну, податкову та бухгалтерську обробку криптовалют в Мексиці; та ін.

Важливим питанням, яке почали порушувати сучасні економісти, стосується проблеми здійснення незаконних операцій з криптовалютою. Так, Нгієм Х., Мурік Г., Морстаттер Ф. і Феррара Е. [95] описують виявлення шахрайства криптовалютних операцій на базі використанням ринкових і соціальних сигналів; Тайхманн Ф. М. Дж., Фалькер М. [96] досліджують використання криптовалюти як засобу для фінансових злочинів; Хуанг С. [97] висвітлює зв'язок криптовалюти зі злочинністю; Колеснікова К., Мезенцева О., Мукатаєв Т. [98] аналізують транзакції з криптовалютою для виявлення незаконних операцій; Дюпюї Д. та Глісон К. [99] вивчають проблему відмивання грошей за допомогою криптовалюти; Троцце А., Кампс Дж., Акартуна Е.А., Хетцель Ф.Дж., Клейнберг Б., Девис Т., Джонсон С.Д. [100] досліджують зв'язок криптовалюти та майбутніх фінансових злочинів; Рен Б. і Люсі Б. [101] показують різницю між чистими та брудними криптовалютними ринками; Акартуна Е. А., Джонсон С. Д., і Торнтон А. [102] розкривають особливості запобігання ризикам відмивання грошей та фінансування тероризму через криптоактиви; Люсі Б. М., Вінь С. А., Яровая Л., і Ван Ю. [103] пропонують для аналізу новий показник індекс невизначеності криптовалюти; та ін.

В сучасному світовому фінансовому середовищі щодня з'являються все нові види незаконних операцій з криптовалютою. До найпоширеніших трендів використання криптовалюти з метою протиправної діяльності належать наступні: використання криптовалют без наявності правового статусу таких фінансових операцій; розширення видів використовуваних криптовалют при здійснення незаконних фінансових транзакцій; покращення наявних технологічних характеристик та специфікації окремих, успішно використовуваних злочинцями дистанційних інтернет-сервісів фінансового ринку психотропних, наркотичних засобів, продуктів іншої незаконної діяльності; розвиток сервісів конвертації криптовалюти, а також готівкове

виведення фіатних коштів; розширення використання анонімних фінансових транзакцій через криптомати; збільшення обсягів відмивання нелегальних коштів через фінансові операції за допомогою програм-змішувачів; проведення фінансових криптотранзакцій через слабо контрольовані офшори; нелегальних видів професійної діяльності – адміністрування та координування однією особою одночасно декількох не пов'язаних сервісів, гарантування крипто-угод, посередництво з переміщення товарів та обігу криптовалюти, вирощування та продаж за криптовалюту нарковмістких рослин, розміщення на асфальтованих дорогах оголошень про незаконні криптоопераціі, та ін.; купівля-продаж за криптовалюту обладнання та хімічних конструкторів по виготовленню наркотичних засобів; здійснення віртуальних фінансових транзакцій на сайтах азартних ігор; злочини з посягання на право власності криптовалютою через використання підроблених електронних криптогаманців, сайти-копії, сайти двійники, шахрайські інвестиційні онлайн проекти.

В сучасному електронному світі існує цілий ряд механізмів обертання криптовалюти, за допомогою яких криптовалюта конвертується в інші форми електронних коштів. Це такі механізми як:

– Monero (являє собою приватну децентралізовану криптовалюту на базі протоколу CryptoNote; має підвищену конфіденційність фінансових операцій; використовується через гаманець; може застосовуватись на різних платформах; цю криптовалюту можна майнити, обмінювати на товари, послуги, іншу валюту з низькою комісією, конвертувати),

– Dash (це криптовалютна готівка; являє собою також відкриту децентралізовану платіжну систему; базується на блокчейні; працює за принципом зростання конфіденційності фінансових операцій; емісія такої криптовалюти відбувається при майнингу);

– Ripple (це цифрова криптовалюта; глобальна криптовалютна платформа, блокчейн-компанія, з децентралізованою інфраструктурою для роботи платіжних систем; базується на фінансових операціях переміщення та

обміну валюти без проведення поворотних платежів; створює інклюзивну фінансову систему; представник новітньої цифрової економіки; має відкритий цифровий код, на якому може працювати будь-хто; має відкритий протокол Інтерледжер для з'єднання різних платіжних систем з метою безперешкодного обміну даними);

– Zcash (є цифрова криптовалюта, що має відкритий вихідний код, забезпечує конфіденційність фінансових операцій, високу швидкість, має низькі комісії, передбачає вибіркову прозорість транзакцій, тобто самі платежі є відомими, але анонімними залишаються відправник, отримувач фінансової операції та сума такої операції; найкраще підходить для здійснення мобільних платежів;);

– Capfolio (є сучасною платіжною системою, технологічною, професійною платформою для операцій торгівлі криптовалютою, де можна протестувати існуючі криптовалютні ринки, клонувати актуальних високоефективних лідерів, створити новий складний торговий алгоритм роботи з криптовалютою);

– 3Commas (є автоматизованою, безпечною, аналітичною системою крипто-трейдинга, платформою для операцій торгівлі криптовалютою, де наявна можливість відслідковування обраної криптовалюти в одному портфелі з різних криптовалютних бірж; використовуються різні стратегії для отримання прибутку: ведмежий ринок, воловий ринок, боковий рух; застосовуються розумні торгові термінали, які містять широкий перелік функцій; наявні готові боти для дублювання та копіювання; можливість підключення сигналів до торгових ботів);

– CCXT (є професійною платформою для торгівлі криптовалитою, реалізації алгоритмічного криптотрейдингу, з відкритим вхідним кодом для проведення криптофінансування; підтримує декілька ринків продажу криптовалют, багато криптовалютних бірж та продавців, містить стандартну бібліотеку з новітніми, уніфікованими функціями з легкою інтеграцією);

– Freqtrade (є безкоштовним ботом для проведення торгівельних операцій з криптовалютою; має відкритий вихідний код, що створений мовою Python; підтримує основні криптовалютні біржі; містить функціонали побудови ефективної стратегії, керування капіталом, завантаження історії ринку, тестування обраної стратегії, оптимізації процесів, побудови графіків, послідуючий аналіз; система керування здійснюється за допомогою Telegram чи WebUI);

– CryptoSignal (висококваліфікована платформа торгівлі криптовалютою; цілодобово сканує криптовалютні ринки; передбачає глубокий технічний аналіз криптовалют; використання алгоритму штучного інтелекту);

– Ctubio (платіжна система криптовалютної торгівлі на базі C++; висока швидкість операцій; містить систему графічної візуалізації стану торгового рахунку, цільову позицію криптовалюти);

– Blackbird Bitcoin Arbitrage (криптовалютна платіжна система на базі C++, що виконує арбітраж короткострокового чи довгострокового типу між криптовалютними біржами; генерує ринково-нейтральні торгівельні стратегії, має незалежні від ринкових коливань стратегії; здійснює фактичний продаж криптовалюти на короткій біржі; реалізація операцій на паралельних біржах);

– StockSharp (є торгівельною платформою для криптовалют; безкоштовна програма торгівлі криптовалютою на багатьох ринках; має відкритий вихідний код для торгівельних операцій; містить значну широкий перелік криптовалютних бірж; має автоматичний та ручний спосіб проведення операцій; містить безкоштовну бібліотеку та історію даних; включає безкоштовний додаток-термінал побудови графічної візуалізації; підтримує багато джерел; зручний додаток побудови стратегій; містить готову оболочку, що легко підлаштовується під конкретну стратегію);

– Catalyst (платформа роботи з криптовалютою; здійснення аналізу криптовалютного ринку; побудови, тестування та аналізу криптовалютних стратегій; графічна візуалізація криптовалютних торгових операцій;

тестування криптовалютних стратегій; зберігання, обмін, систематизація інформації; візуалізація новітніх ссхем торгівлі криптовалютою);

– Golang Crypto Trading Bot (платіжна система торгівлі криптовалютою на базі програмного забезпечення Go; наявна можливість тестування стратегії торгівлі криптовалютою); та ін.

В свою чергу, окремо виділяють ключових агентів у криптовалютній економіці: централізовані біржі криптовалют (біржі криптовалют без безпосередньої участі біржі, де користувачі системи можуть здійснювати купівлю-продаж різних криптовалют за фіатні кошти, інші види криптовалют; при чому адреса обміну виступає умовним депонуванням між покупцем та продавцем), децентралізовані біржі криптовалют (біржі криптовалют з безпосередньою участю біржі, де користувачі системи можуть здійснювати купівлю-продаж різних криптовалют за фіатні кошти, інші види криптовалют), криптовалютні гаманці (передбачає онлайн-банкінг криптовалюти, куди користувачами системи вносяться криптовалютні кошти), емітенти токенів (передбачають початкові адреси вихідних пропозицій), сервіси роздачі (визначають адреси, що сприяють вільному обігу токенів серед користувачів криптовалюти у якості реклами), ігрові сервіси (передбачають адреси, що використовуються для організації азартних ігор), та ін.

Незаконним операціям з криптовалютою характерні певні інформаційні ознаки, які класифікують у залежності від типів таких ознак.

Залежно від характеру операцій, ознаками незаконних операцій з криптовалютою є:

– непрозорі криптовалютні контракти;

– зашифровані криптовалютні угоди;

– неперсоніфіковані транзакції;

– роздроблені систематичні операції на граничні, лімітовані суми для уникнення ідентифікації;

– операції, що не відповідають затвердженим протоколам транзакцій;

– операції обміну валюти неідентифікованими трейдерами;

– проведення заплутаного обміну криптовалюти в інші форми електронних коштів з метою виведення таких кошів у готівку тощо.

Залежно від способів проведення, ознаками незаконних операцій з криптовалютою можуть бути: використання та комбінація офшорних акаунтів; операції через гібридні біржі; транзакції з електронним гаманцем з прямим посиланням на ринок, з правом власності первісній особі; підзвітні вузлові гаманці у разі циклічного та частого перетинання чи сходження їх транзакцій; «смурфінг», тобто створення другого додаткового облікового запису для проведення транзакцій; фальшиві платформи для торгівлі; скам-біржі криптовалют; хмарний майнінг; фішинг; віруси-здирники; клони криптовалютних гаманців; інвестиційні схеми; шахрайство із додатковим залученням обмінників; фейкові роздачі; схеми з пожертвуваннями; фінансові піраміди; підроблена криптовалюта; шахрайські фонди; шантаж та вимагання; та ін.

Залежно від інструментів реалізації відмивання коштів, ознаками незаконних операцій з криптовалютою є наступні:

– використання тамблерів (інструмент відмивання криптовалюти переважно у криптовалютах біткойн, лайткойн, ефіриум, що передбачає змішування сервісів різних вебсайтів (чистих, прозорих та даркнетівських), тим самим порушуючи транзакційний зв’язок між гаманцями, змішуючи законний обіг криптовають з незаконним, з послідуючим виведення готівкових коштів через перекази міжнародних платіжних систем);

– операції на позабіржовому ринку (проведення угод через брокера (Bitstocks, Kraken, Genesis Trading та ін.) – зі значно обмеженою можливістю відмивання коштів, тому що в цьому випадку присутні банківські відносини, а відмивання могло бути до угоди з брокером; проведення угод особисто між двома особами з участю готівки невідомого походження, або яка буде використана на незаконні цілі;

– застосування конфіденційних монет (анонімні монети з прихованим джерелом, сумою та призначенням, такі як Monero, Dash, Zcash та ін.);

– транзакції на децентралізованих біржах (анонімні ринки, представлені розподіленим реєстром програм, що дозволяють користувачам проводити транзакції з використанням криптовалют без участі централізованих організацій-посередників при торгівлі чи зберіганні криптовалюти);

– проведення прямих роздрібних покупок за допомогою криптовалюти (придбання за криптовалюту великовартісних активів, таких як нерухомість, автомобіль, дорогоцінні метали, ювелірні вироби та ін.);

– майнинг як прикриття (спрямування незаконних коштів у легальний прибутковий бізнес, сплата необхідних для ведення бізнесу податків, з наступною витратою очищених коштів; тобто змішування нелегальних коштів із законними); та ін.

До попереджувальних ознак незаконних операцій з криптовалютою варто віднести: пропонування безкоштовних грошей; обіцянка необгрунтовано великих високоризикованих доходів; відсутність опису та деталей запропонованої угоди.

У відповідності до секторів кібершахрайств, ознаками незаконних операцій з криптовалютою є: використання нових видів цифрових валют для відмивання нелегальних коштів; незаконні шляхи реалізації психоактивних речовин, заборонених засобів, наркотичних препаратів; незаконний продаж заборонених контентів; нелегальна реалізація незаконних та злочинних послуг; посягання на право власності криптовалютою.

В залежності від типів товарів та послуг, що придбаються чи продаються за криптовалюту, ознаками незаконних операцій з криптовалютою виділяють: операції, пов’язані з злочинним використанням особистої інформації; операції торгівлі підробленими паперами та документами; операції торгівлі нелегальними лікарськими препаратами; операції з торгівлі товарами та послугами заборонених галузей, в тому числі наркотичних та психотропних засобів; та ін.

Окремі ознаки мають незаконні операції щодо сервісів тіньової мережі Internet:

– Abraxas (сервіс інтернет-операцій);

– Agora (інтернет-послуги електронної пошти та веб-хостинга);

– Darknet (анонімні мережі, підпільні інтернет-комунікації та технології, приховані мережі, зашифровані, нейронні мережі з відкритим початковим кодом, що реалізуються для незаконної діяльності);

– Evolution (один напрям – послуги онлайн-ігор, онлайн-казино; інший напрям – програма для роботи з електронною поштою, для керування та формування адресної книги);

– Nuklias (облачна платформа інтернет-послуг у сфері бізнес-послуг, мультимедіа, графічного дизайну на основі технологій Modernizr, Font Awesome, Wordpress 4.5, PHP);

– Ship Marketplace (операції з купівлі-продажу товарів на загальнодоступному торговому інтернет-майданчику Marketplace на Facebook з доставкою);

– Silk Road (операції на анонімному торговому інтернет-майданчику анонімної мережі, більшість реалізуємих товарів та послуг на якому є нелегальними, в тому числі заборонені психоактивні речовини) та ін.

В сучасному електронному світі використовують певні програмні комплекси для ідентифікації незаконних операцій з криптовалютою. Ці програми ґрунтуються на використанні розширеної кластеризації та власних алгоритмів для встановлення зв’язків між електронним гаманцями, транзакціями, переказами. Серед таких програмних продуктів варто виділити наступні:

– Chainanalysis (це платформа бази даних блокчейну; це сервісна компанія, що допомагає укріпляти довіру до блокчейнів; працювати з криптовалютою; вона спеціалізується на відслідковуванні біткойнів; допомагає державним установам, регулюючим органам, банківським та іншим фінансовим установам, криптовалютним компаніям, відслідковувати джерела походження коштів із анонімних гаманців, незважаючи на заплутаний та множинний характер угоди; створює прозорість для глобальної світової

економічної системи, що має в основі структуру з блокчейнів; надає можливість банківським та іншим фінансовим установам, уряду, представникам бізнесу, сформувати уяву використання криптовалюти; надає програмне забезпечення, відомості, послуги, дослідження, державним органам, фінансовим установам, що займаються кібербезпекою; розробляє чіткі стандарти, правила, методики, засоби контролю за криптовалютою);

– CypherTrace (представляє собою першу у світі команду судової експертизи блокчейну; це інтернет платформа, що забезпечує контроль криптовалютних ризиків відмивання віртуальних інтернет-активів, загроз, злочинів, для фінансових установ, банків; використовується для зниження фінансових ризиків щодо виконання та дотримання вимог до криптовалюти; допомагає банківським установам, платіжним системам, регулюючим органам, ідентифікувати операції з криптовалютою та встановлювати їх взаємозв’язок з ризикованими партнерами та контрагентами; дозволяє встановити підозрілу та потребуючу додаткової уваги фінансову активність з криптогрошима, оперативно повідомити таку інформацію відповідним структурам; забезпечує опис критичного уявлення про ризиковані сліпі зони роботи з криптокоштами; працює за принципом «знай свого клієнта», і, відповідно, забезпечує реалізацію комплексної перевірки клієнтів з метою встановлення підозрілих, недобросовісних, достовірно незареєстрованих клієнтів, які приховують свої наміри роботи з криптовалютою; реалізує блокчейн-аналітику; здійснює поглиблений аналіз постачальників послуг віртуальної фінансової активності; забезпечує індивідуальне надання інформації та даних по крипто-ризикам);

– Elliptic AML (програмне забезпечення, що реалізує рішення по організації та дотримання відповідності криптографічним нормативним вимогам при використанні криптоактивів; проводить блокчейн-аналітику; здійснює сертифікацію криптобізнесу; забезпечує управління фінансовими ризиками роботи з криптоактивами; здійснення скринінгу крипто гаманця, встановлення ризиків криптовалютних гаманців; реалізація моніторингу

криптовалютних фінансових операцій на дотримання вимог фінансового моніторингу, протидії вдмивання нелегальних коштів, фінансування тероризму, санкційній приналежності; скринінг портфеля ризиків постачальників послуг віртуальних активів; здійснення криптовалютних розслідувань через докладну мережеву візуалізацію електронних гаманців, а також фінансових транзакцій між ними);

– Orbit (хмарна сервісна платформа, що являє собою практичного помічника, що відслідковує, автоматизує, контролює операції користувачів; передбачає віртуалізацію робочої станції, віртуалізацію кінчевих точок, 3 D Workplace, безечну доставку додатків, віртуальний робочий стіл; використовує стратегію хмарних сервісів, хмарного управління; включає IT консолідацію); та ін.

Методики та моделі виявлення, контролю та перешкоджання здійсненню незаконних операцій з криптовалютою:

– Регулююча діалектика (модель боротьби з відмиванням коштів за допомогою криптовалюти шляхом безперервного контролю та взаємодії між банківськими спеціалістами та державними органами банківського нагляду за наступною схемою: фінансові установи та баки запроваджують нововведення, що не достатньо законодавчо врегульовані, на що контролюючі державні органи у правовому порядку вводять нові укази та регулюючі заходи, що підривають шахрайську діяльність, а фінансові установи та банки відповідно запроваджують нові методики та моделі, тобто починається новий цикл заходів);

– Транзакційна модель ідентифікації, класифікації та вивчення блокчейн-адрес ключових агентів (модель передбачає проведення ряду етапів: визначення даних блокчейну щодо криптовалютних транзакцій; визначення ключових індикаторів економічних агентів фінансових транзакцій; ідентифікація ознак та характеристик фінансових транзакцій, що виражаються в певних змінних, при чому мережева структура вузла фінансових транзакцій виражається формулою 2.1-2.4 [104]:

$$S_v = \frac{|(u,v)|(u,v)\in C_v^{size} and\ (v,u)\in C_v^{size}|}{|(u,v)|(u,v)\in C_v^{size} or\ (v,u)\in C_v^{size}|}, \quad (2.1)$$

при чому коефіцієнт кластеризації виражається формулою 2:

$$K_v = \frac{1}{\sum N_{inout}(v)(\sum N_{inout}(v)-1)-2\sum N^*_{inout}(v)}\mathrm{T(v)}, \quad (2.2)$$

щільність мережі транзакцій зображується формулою 3:

$$D_v^{size} = \frac{m}{n(n-1)}, \quad (2.3)$$

$$S_v^{size} = \frac{|(u,w)|(u,w)\in C_v^{size} and\ (w,u)\in C_v^{size}|}{m}, \quad (2.4)$$

де $G = (V, C)$ – обрана мережа фінансових транзакцій,

V – вузли адрес блокчейна,

$C = \{e|(V_s, V_t, t), V_s, V_t \in V\}$ – набір обраних харакетристик,

T_{in} та T_{out} – кількість вхідних та вихідних транзакцій,

N_{in} та N_{out} – ступінь вхідних та вихідних транзакцій,

N_{size} – обсяг мережі транзакцій;

$T(v)$ - кількість маркерів, що мають харакеристику (v),

$\sum N_{inout}(v)$ – сума вхідного та вихідного ступенів транзакцій,

$\sum N^*_{inout}(v)$ – зворотня ступінь,

m – кількість вузлів у мережі,

n – кількість характеристик;

процес підготовки моделі на базі перехресної перевірки шляхом алгоритмів логістичної регресії, методики опорних векторів, багатошарових перцептронів, дерева рішень.

– Модель зв’язку криптовалют та управління ризиками в умовах невизначеності економічної політики (Показником ризику криптовалют виступає:

1) індекс невизначеності економічної політики (UEP) – обумовлюється залежність UEP, а також економічної політики, управлінських рішень регулюючих державних органів для подальшого керування протоколами та валютами на крипторинку, боротьби з волатильністю фондового криптовалютного ринку, невизначеністю в економічній державній політиці; передбачає стандартне відхилення ціни актива, його доходності, включає ряд економічних показників, долю невизначеності настроїв і новинних характеристик; успішна стратегія хеджування ризиків передбачає врахування структури кореляції;

2) глобальний індекс економічної невизначенності (GUEP) – охоплює показники країн, що мають суттєвий вклад до загального світового виробничого обсягу, що коригується на ринковий обмінний курс, згідно показників ВВП, ППС; базується на середньозваженому значенні показника розвинених країн світу, корелює з фінансово-економічними кризами, політичними подіями, соціальними процесами, іншими нетиповими явищами; відзначається емпірична цінність криптовалют; включає хеджування та безпечне збереження криптовалюти; встановлюється зв’язок з глобальним бізнес-циклом.

– Економетрика криптовалюти (передбачає комбінацію статистичних та економічних моделей для оцінювання та прогнозування криптовалютних економічних характеристик, таких як: кластеризація та лінійна класифікація, лінійні регресійні методи, дерево рішень, часові ряди, ймовірнісні класифікатори, теорії портфелів, - що формуються в комплексні моделі:

1) гібридна модель вибору (на основі методів моделювання дискретного вибору, використовує різні типи даних, припускає гнучкі порушення, моделювання латентних змінних);

2) прогнозування волатильності криптовалюти (модель GARCH – статистичний метод багатомірного моделювання прогнозування волатильності дохідності криптовалюти, VECH - модель Боллерслева, Енгела, Вулдриджа, багатомірна модель умовної гетероскедастичності, BEKK – модель Баба, Енгела, Кронера, Крафта, для оцінки коливань криптовалют; CGCD – модель Copula-Granger-Causality in Distribution, передбачає аналіз причинно-наслідкового зв'язку на фінансовому криптовалютному ринку, дослідження потенціалу покращення прогнозованої економічної ситуації, за копула-квантильним аналізом, аналізом по Грейнджеру; GAS – це модель узагальненої авторегресійної оцінки для моделювання, прогнозування ризиків та дохідності криптовалюти);

3) лінійна статистична модель (модель оцінки лінійної залежності незалежних та залежних змінних; модель ARMA – при аналізі часових рядів залежності ціни та незалежних змінних криптовалют, використання авторегресійного ковзного середнього);

4) при чому репрезентативні набори показників, що використовуються в економетричних моделях вивчення криптовалютних операцій, їх ризикованості, легальності транзакцій, наступні: ринкові показники (ціна, обсяг торгівельних операцій, рівень ордерів, волатильність криптовалюти, часові мітки); показники настроїв учасників ринку криптовалюти (відомості мережі Інтернет, онлайн-спільнот, ЗМІ, ринкові дані, інформація соцмереж, пошукові запити, новинні дані, повідомлення, коментарі, в тому числі метадані статистично-емоційного характеру); інші показники (попередня, необроблена інформація, відомості диверсифікованих портфелей, крос-валюта);

– модель оцінки індексу невизначеності криптовалюти (CrUI (cryptocurrency uncertainty index) – індекс невизначеності криптовалюти, що відображає перебіг основних процесів у криптовалютному просторі, в тому числі визначає і дохідність, волатильність криптовалюти. Індекс невизначеності криптовалюти включає два типи невизначеності:

невизначеність криптовалютної ціни, невизначеність криптовалютної політики. Модель оцінки індексу невизначеності криптовалюти передбачає ряд етапів:

1) етап 1 – збір відомостей з відкритих баз даних, інформаційних джерел, засобів масової інформації, розгляд соціального інформаційного аспекту щодо криптовалют;

2) етап 2 – побудова індексів невизначеності криптовалютної ціни (cryptocurrency price uncertainty index – CrPrUI, формула 2.5) та невизначеності криптовалютної політики (cryptocurrency policy uncertainty index – CrPolUI, формула 2.6) [103]:

$$CrPrUI = \frac{(Vpr_t - \mu pr)}{\delta pr} + 100 \quad (2.5)$$

Vpr_t – цінність інформації про криптовалюту щодо їх цін за період t;

μpr – середнє значення показників цінності інформації про криптовалюту щодо їх цін;

δpr – стандартне відхилення цінності інформації про криптовалюту щодо їх цін.

$$CrPolUI = \frac{(Vpol_t - \mu pol)}{\delta pol} + 100 \quad (2.6)$$

$Vpol_t$ – цінність інформації про криптовалюту щодо політики за період t;

μpol – середнє значення показників цінності інформації про криптовалюту щодо політики;

δpol – стандартне відхилення цінності інформації про криптовалюту щодо політики.

При розрахунках індексу невизначеності криптовалюти за системні змінні було взято індекс невизначеності криптовалютної ціни, індекс невизначеності криптовалютної політики, індекс невизначеності економічної політики, глобальний індекс економічної невизначеності, обсяг криптовалюти, ціна криптовалюти, індекс стресу фінансової системи, індекс золота;

3) етап 3 – побудова економетричної моделі:

– проведення тесту Augment Dickey-Fuller на стаціонартність;

– доведення коінтегрованості змінних, проведення тесту Johansen: для проведення структурного аналізу та прогнозування використовується модель векторної авторегресії, модель структурної векторної авторегресії, модель векторної коректировки помилок, модель структурної векторної авторегресії з коінтегрованими змінними. Так, для визначення кількісного виразу впливу криптовалютної ціни та криптовалютної політики на динаміку системних змінних, можна модель векторної коректировки помилок виразити рівнянням 2.7:

$$\Delta y_t = \varepsilon \epsilon_{y_{t-1}} + \omega_1 \Delta y_{t-1} + \ldots + \omega_{p-1} \Delta y_{t-p+1} + \psi^+ d_t + \varphi_t \qquad (2.7)$$

y_t – вектор змінних у часі *t;*

ε – матриця з коефіцієнтами навантаження;

ϵ - матриця з коінтегрованими векторами;

ω - матриця короткостровкових коефіцієнтів;

d_t- вектор детермінованих членів;

ψ^+- матриця коефіцієнтфів, що відповідають d_t;

φ_t- аналізований векторний процес з коваріаційною матрицею, показує порушення форми, помилки прогнозу.

Модель адаптується для криптовалютної ціни та криптовалютної політики.

Підводячи підсумки зазначимо, що криптовалюта доволі часто використовується при скоєнні фінансових злочинів, що стає суттєвою проблемою розвитку економіки. Це пов’язано з тим, що існуючі заходи фінансового моніторингу в секторі криптовалюти наразі є недостатньо ефективними. Результати проведеного дослідження шляхом ідентифікації інформаційних ознак, які засвідчують здійснення незаконних операцій з криптовалютою, допоможуть отримати розуміння про методи та шляхи відмивання незаконних коштів, фінансування тероризму, фінансування розповсюдження зброї масового знищення, реалізації корумпованих дій. Отже для більш ефективної боротьби з фінансовою злочинністю на основі використання криптовалюти, потрібно створити певну модель та єдині стандарти роботи з криптовалютою, регулювання та контролю таких операцій. Запропоновані автором методики моніторингу за криптовалютою можуть стати основою для формування таких стандартів. Все це дозолить фахівцям на практиці спрогнозувати можливі загальнодоступні фінансові шахрайства, для подальшого правового регулювання, внутрішнього та зовнішнього нагляду, контролю за законністю обігу коштів з використанням криптовалюти.

2.3. Визначення закономірностей здійснення фінансових кібершахрайств з використанням криптовалюти

Акумулювання великого масиву неструктурованих даних про фінансові транзакції дозволяє виявляти приховані закономірності між ними та отримувати нові знання. Одним із популярних методів виявлення знань стали алгоритми пошуку асоціативних правил. Асоціативні правила дозволяють знаходити закономірності між пов'язаними подіями. Проблема пошуку асоціативних правил може бути в загальному вигляді спрямована на вирішення двох основних задач: пошук найбільш поширених наборів елементів, і генерація правил на основі аналізу існуючої бази даних.

Асоціативні правила – це дуже сучасна та складна технологія, що дозволяє ідентифікувати взаємозв'язки між пов'язаними подіями або елементами. Будь-яке асоціативне правило складається із двох наборів елементів, що мають умову (antecedent) та наслідок (consequent), й записуються у вигляді $X \to Y, X \cap Y \to \emptyset$.

При чому, будь-яке асоціативне правило можна представити двома основними характеристиками [105, 106]:

- підтримка (опора) $supp(X \to Y)$ асоціативного правила $X \to Y$ виступає значенням, що дорівнює відношенню кількості записів $X \cup Y$ в базі даних D, до загальної кількості записів у базі даних. Іншими словами, підтримка вказує на загальну кількість транзакцій, яке містить як умову та і наслідок. Загальний вигляд пітримки асоціативного праивла можно представити наступним чином [107]:

$$supp(X \to Y) = P\ (X \cap Y) = \frac{n(\{X; Y\} \in d_i}{N} \tag{2.8}$$

- довіра $conf(X \to Y)$ до асоціативного правила $X \to Y$ виступає. значенням, що дорівнює відношенню її опори $supp(X \to Y)$ до опори

$supp(X \to Y)$ набору X. Довіра до асоціативного правила відображає міру точності правила [107]:

$$conf(X \to Y) = P\ (X|Y) = \frac{n1(\{X;Y\} \in d_i}{n1(\{X\} \in d_i} \quad (2.9)$$

Побудова асоціативних правил передбачає розгляд всіх можливих комбінації умов і наслідків, з відповіним рівнем підтримки й довіри. Важливим етапом побудови асоціативних правил є оптимізація їх кількості та виключення тих, які не задовольняють порогу мінімальної підтримки.

У межах даного дослідження застосовано алгоритми асоціативних правил для визначення ймовірних умов, які будуть вказувати на можливість проведення шахрайської операції з криптовалютою. Об'єктом дослідження обрано Ethereum. За даними BanklessTimes, Ethereum (ETH) зараз використовується для незаконної діяльності більше порівняно з Bitcoin. Згідно з аналізом, частка незаконних транзакцій у загальному відомому потоці Ethereum зросла до 0,33 відсотка проти 0,04 відсотка для Bitcoin. Експерти наголошують, що криптовалюта Ethereum є популярним фінансовим інструментом серед учасників на ринку даркнету, які використовуються для торгівлі незаконними товарами та послугами. Це повязано з цим, що Ethereum пропонує більшу конфіденційність, ніж Bitcoin. Ці ринки часто розміщені в «темній мережі», доступ до якої можливий лише за допомогою спеціального програмного забезпечення. Крім цього, зростання незаконної діяльності з викоритсанням Ethereum, ймовірно, пов'язано з його популярністю як платформи для смарт-контрактів. Розумні контракти дозволяють розробляти децентралізовані програми (dApps), які часто використовуються злочинцями для сприяння незаконній діяльності, такій як відмивання грошей і торгівля наркотиками. Крім того, збільшення частки незаконної діяльності Ethereum може бути пов'язане з його популярністю серед операторів програм-вимагачів та інших злочинців. Атаки програм-вимагачів останнім часом стали більш

поширеними, і злочинці часто вимагають оплату в криптовалюті [108]. Таким чином, розробка методичних засад для ідентифікації незаконних фінансових операцій з використанням Ethereum є вкрай актуальним.

Розроблений науково-методичний підіхд до визначення закономірностей здійснення фінансових кібершахрайств з використанням Ефіріум на основі використання асоціативних правил полягає в реалізації наступної послідовності етапів:

1 етап. Формування вхідної структури даних здійснення фінансових кібершахрайств з використанням Ефіріум.

На даному етапі проводиться збір та систематизація даних щодо переліку наступних показників:

– загальна кількість унікальних адрес, з яких обліковий запис отримував транзакції (URFA);

– загальна кількість унікальних адрес, з яких обліковий запис надсилає транзакції (USTA);

– середній розмір Ефіріуму, який отримується (AVR);

– середній розмір Ефіріуму, який надсилається (AVS);

– загальний обсяг Ефіріуму, надісланий на адресу облікового запису (TES);

– загальний обсяг Ефіріуму, отриманий на адресу облікового запису (TER);

– індикатор шахрайства (0 – відсутнє шахарайство, 1 – присутнє шахрайство) (FRAUD).

Джерелом статистичних даних слугувала база Kaggle [109], тоді як фрагмент сформованої статистичної бази подано в таблиці 2.5.

Таблиця 2.5 – Фрагмент вхідної структури даних здійснення фінансових кібершахрайств з використанням Ефіріум

	FRAUD	URFA	USTA	AVR	AVS	TES	TER
0	0	40	118	6.589513	1.200681	865.6910932	586.4666748
1	0	5	14	0.385685	0.032844	3.08729702	3.085478209
2	0	10	2	0.358906	1.794308	3.58861565	3.58905665
3	0	7	13	99.48884	70.001834	1750.045862	895.399559
4	0	7	19	2.671095	0.022688	104.3188828	53.4218965
5	0	2	1	3.234908	4.851858	9.70371586	9.70472386
6	0	9	20	1.098115	0.482496	12.0623941	12.079266
7	0	3	3	0.891098	0.040861	8.703392156	4.45548974
8	0	1	1	2	1.99938	1.99938	2
9	0	2	4	16.07	18.634625	149.077	50.1
10	0	2	1	1.004819	1.004055	10.04055439	10.04819041
…	…	…	…	…	…	…	…
9831	1	3	6	2.598288	1.731872	10.39123372	10.39315016
9832	1	0	0	0	0	0	0
9833	1	0	0	0	0	0	0
9834	1	15	1	1.02508	15.375782	15.37578207	15.37620207
9835	1	1	0	0	0	0	0
9836	1	11	4	2.82106	9.166365	36.66546146	36.67377746
9837	1	0	0	0	0	0	0
9838	1	31	44	1.234192	0.922179	61.78599493	53.07025157
9839	1	1	0	0.5	0	0	0.5
9840	1	1	5	6333.26508	644.427778	11599.7	18999.79523

Серед 9841 випадків 7662 випадки, тобто 77,86% класифіковані як факт відсутності фінансових кібершахрайств з використанням Ефіріум. Лише для 2179 випадків, тобто 22,14% було виявлено ознаки шахрайства з використанням Ефіріум.

Наступним етапом розробленого науково-методичного підходу є визначення закономірностей між характеристиками фінансових транзакцій з використанням Ефіріум. Для реалізації даного етапу використано програмний продукт STATISTICA 10: команду Data Mining/Sequence, Association and Link Analysis. Фрагмент отриманих результатів представимо в таблиці 2.6.

Таблиця 2.6 – Результати побудови асоціативних правил для визначення закономірностей зійснення незаконних операцій з Ефіріум

Body	==>	Head	Support (%)	Confidence (%)
-39,576163<URFA<=100,277515, -73745,232761<TES<=94068,968712	==>	-0,070274<FRAUD<=0,124189	75,96789	77,7212
-73745,232761<TES<=94068,968712, -73645,038405<TER<=96923,921976	==>	-0,070274<FRAUD<=0,124189	77,18728	77,7164
-39,576163<URFA<=100,277515, -73645,038405<TER<=96923,921976	==>	-0,070274<FRAUD<=0,124189	75,87644	77,7003
-39,576163<URFA<=100,277515, -73745,232761<TES<=94068,968712, -73645,038405<TER<=96923,921976	==>	-0,070274<FRAUD<=0,124189	75,8053	77,6841
-73645,038405<TER<=96923,921976	==>	-0,070274<FRAUD<=0,124189, -73745,232761<TES<=94068,968712	77,18728	77,6608
-39,576163<URFA<=100,277515, -73645,038405<TER<=96923,921976	==>	-0,070274<FRAUD<=0,124189, -73745,232761<TES<=94068,968712	75,8053	77,6275
-73745,232761<TES<=94068,968712	==>	-0,070274<FRAUD<=0,124189, -73645,038405<TER<=96923,921976	77,18728	77,5815
-39,576163<URFA<=100,277515, -73745,232761<TES<=94068,968712	==>	-0,070274<FRAUD<=0,124189, -73645,038405<TER<=96923,921976	75,8053	77,5548
-39,576163<URFA<=100,277515, -35,997920<USTA<=87,555079	==>	-0,070274<FRAUD<=0,124189	75,0127	77,5176
-39,576163<URFA<=100,277515, -73745,232761<TES<=94068,968712, -35,997920<USTA<=87,555079	==>	-0,070274<FRAUD<=0,124189	74,53511	77,4142
-39,576163<URFA<=100,277515, -73645,038405<TER<=96923,921976, -35,997920<USTA<=87,555079	==>	-0,070274<FRAUD<=0,124189	74,44365	77,3928
-73745,232761<TES<=94068,968712, -35,997920<USTA<=87,555079	==>	-0,070274<FRAUD<=0,124189	75,34803	77,3524
-73645,038405<TER<=96923,921976, -35,997920<USTA<=87,555079	==>	-0,070274<FRAUD<=0,124189	75,25658	77,3311
-73745,232761<TES<=94068,968712, -73645,038405<TER<=96923,921976, -35,997920<USTA<=87,555079	==>	-0,070274<FRAUD<=0,124189	75,18545	77,3145
-574,848976<AVR<=776,291550, -73645,038405<TER<=96923,921976	==>	-0,070274<FRAUD<=0,124189	73,56976	76,9558
-39,576163<URFA<=100,277515, -574,848976<AVR<=776,291550, -73745,232761<TES<=94068,968712	==>	-0,070274<FRAUD<=0,124189	72,34021	76,9455
-574,848976<AVR<=776,291550, -73745,232761<TES<=94068,968712, -73645,038405<TER<=96923,921976	==>	-0,070274<FRAUD<=0,124189	73,51895	76,9435
-39,576163<URFA<=100,277515, -574,848976<AVR<=776,291550, -73645,038405<TER<=96923,921976	==>	-0,070274<FRAUD<=0,124189	72,24876	76,9231
-39,576163<URFA<=100,277515, -574,848976<AVR<=776,291550, -73745,232761<TES<=94068,968712, -73645,038405<TER<=96923,921976	==>	-0,070274<FRAUD<=0,124189	72,19795	76,9106
-11,224277<AVS<=100,744593, -73645,038405<TER<=96923,921976	==>	-0,070274<FRAUD<=0,124189	72,33005	76,7191
-39,576163<URFA<=100,277515, -574,848976<AVR<=776,291550, -35,997920<USTA<=87,555079	==>	-0,070274<FRAUD<=0,124189	71,31389	76,7162

Обмеживши рівень довіри до асоціативних правил на рівні не менше 69% отримано 665 правил, де індикатор «FRAUD» розглянуто в контексті «наслідку». На основі даних отриманих асоціативних правил, представлених в таблиці 2.6, можна зробити наступні висновки:

– за умови загальної кількості унікальних адрес, з яких обліковий запис отримував транзакції (URFA) до 100,28, а також загального обсягу Ефіріуму, надісланий на адресу облікового запису (TES) на суму до 94068,97 у 77,72% випадків виникає ймовірність фінансових кібершахрайств з криптовалютою на рівні до 0,12 частки одиниці;

– використання Ефіріуму для незаконної діяльності становить лише невелику частину обігу криптовалюти, і це порівняно менше, ніж обсяг незаконні транзакцій з використанням традиційних фінансових інструментів;

– якщо загальна кількість унікальних адрес, з яких обліковий запис надсилає транзакції (USTA) становить не більше 87,56, та середній розмір Ефіріуму, який надходить на рахунок (AVR) не перевищує 776,29, то тоді існує ризик шахрайських транзакцій з даною криптовалютою. Підтвердженість такого асоціативного правила становить 76,65%;

– у 77,72% випадків при значеннях TES від 73745,23 до 94068,97 та значення TER у межах від 73645,04 до 96923,92 може призвести до здійснення шахрайських операцій з Ефіріумом тощо.

Переходячи до аналізу частоти виявлених випадків здійснення фінансових кібершахрайств з використанням Ефіріум, що є суттєвим доповненням до наведених вище асоціативних правил (рисунок 2.6).

Аналіз рисунку 2.6 дозволяє констатувати, що найбільша частка фінансових кібершахрайств з використанням Ефіріум відбувається призначеннях TES не менше 94068 та TER не менше 96923 і складає 99,49% та 99,39% відповідно. Найменші частки фінансових кібершахрайств з використанням Ефіріум відбувається для випадків високого ризику не менше 0,90 та становить лише 22,14%.

Frequent itemsets computed (Spreadsheet5_(Recovered)2.sta)
Min: support = 20,0%, confidence = 10,0%
Max. size of an itemset = 10

	Frequent itemsets	Number of items	Frequency	Support(%)
1	(-0,070274<FRAUD<=0,124189	1,00000	7662,00	77,8579
2	(-39,576163<URFA<=100,27751	1,00000	9669,00	98,2522
3	(-574,848976<AVR<=776,29155	1,00000	9456,00	96,0878
4	(-11,224277<AVS<=100,74459	1,00000	9309,00	94,5940
5	(-73745,232761<TES<=94068,96871	1,00000	9791,00	99,4919
6	(-73645,038405<TER<=96923,92197	1,00000	9781,00	99,3903
7	(-35,997920<USTA<=87,55507	1,00000	9634,00	97,8965
8	(FRAUD>0,902041	1,00000	2179,00	22,1420
9	(-0,070274<FRAUD<=0,124189, -35,997920<USTA<=87,555	2,00000	7462,00	75,8256
10	(-0,070274<FRAUD<=0,124189, -73645,038405<TER<=96923,921976, -35,997920<USTA<=87,	3,00000	7406,00	75,2565
11	(-0,070274<FRAUD<=0,124189, -73745,232761<TES<=94068,968712, -35,997920<USTA<=87,	3,00000	7415,00	75,3480
12	(-0,070274<FRAUD<=0,124189, -11,224277<AVS<=100,744593, -35,997920<USTA<=87,5	3,00000	6961,00	70,7346
13	(-0,070274<FRAUD<=0,124189, -574,848976<AVR<=776,291550, -35,997920<USTA<=87,5	3,00000	7094,00	72,0861
14	(-0,070274<FRAUD<=0,124189, -39,576163<URFA<=100,277515, -35,997920<USTA<=87,5	3,00000	7382,00	75,0127
15	39, -73745,232761<TES<=94068,968712, -73645,038405<TER<=96923,921976, -35,997920<USTA<=	4,00000	7399,00	75,1854
16	4593, -73745,232761<TES<=94068,968712, -73645,038405<TER<=96923,921976, -35,997920<UST/	5,00000	6926,00	70,3790
17	1550, -73745,232761<TES<=94068,968712, -73645,038405<TER<=96923,921976, -35,997920<UST/	5,00000	7043,00	71,5679
18	7515, -73745,232761<TES<=94068,968712, -73645,038405<TER<=96923,921976, -35,997920<UST/	5,00000	7319,00	74,3725
19	744593, -73745,232761<TES<=94068,968712, -73645,038405<TER<=96923,921976, -35,997920<U	6,00000	6919,00	70,3079

Рисунок 2.6 – Частота виявлених випадків здійснення фінансових кібершахрайств з використанням Ефіріум

3 етап. Графічне представлення отриманих результатів побудови мережі асоціативних правил причинно-наслідковості зв’язків між досліджуваними явищами здійснення фінансових кібершахрайств з використанням Ефіріум на основі застосування методів візуалізації та графічного дизайну.

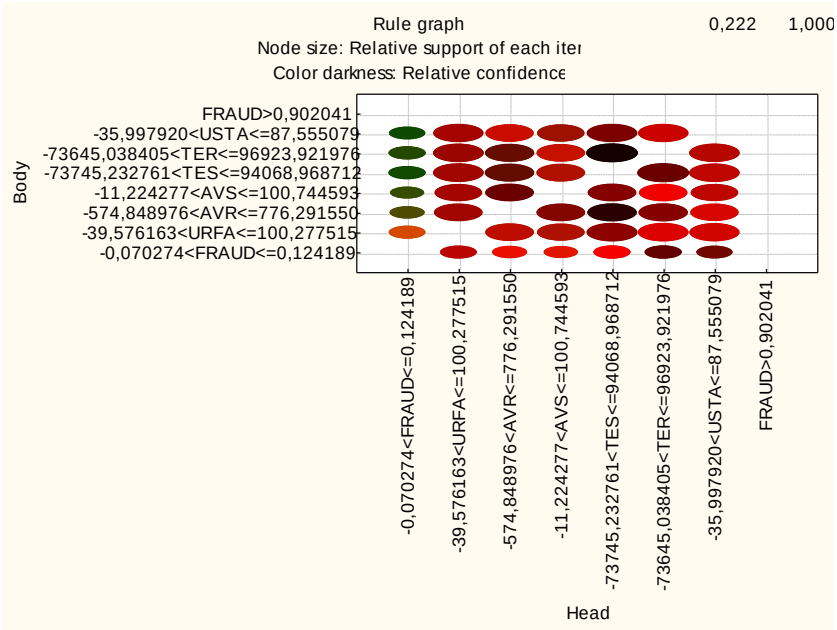


Рисунок 2.7 – Граф асоціативних правил

В рамках даного етапу побудовано граф виявлених на другому етапі асоціативних правил, представлений на рисунку 2.7, який дозволяє отримати візуальне представлення сутності (вісь Head означає причину, вісь Body – наслідок), ступеня підтвердженості виявлених зв'язків (колір відповідного еліпса), а також частки досліджуваної сукупності, для якої відповідне асоціативне правило характерне (величина еліпсу).

Переходячи до аналізу частоти виявлених випадків здійснення фінансових кібершахрайств з використанням Ефіріум (рисунок 2.8 та веб-граф 4) найбільшим даний показник є для низького рівня ризику, коли TER не перевищує 96923, AVR - 776, TES – 94.068 відповідно. Найманша частка випадків спостерігається для низького рівня ризику здійснення фінансових кібершахрайств з використанням Ефіріум в межах до 0,12 частки одиниці.

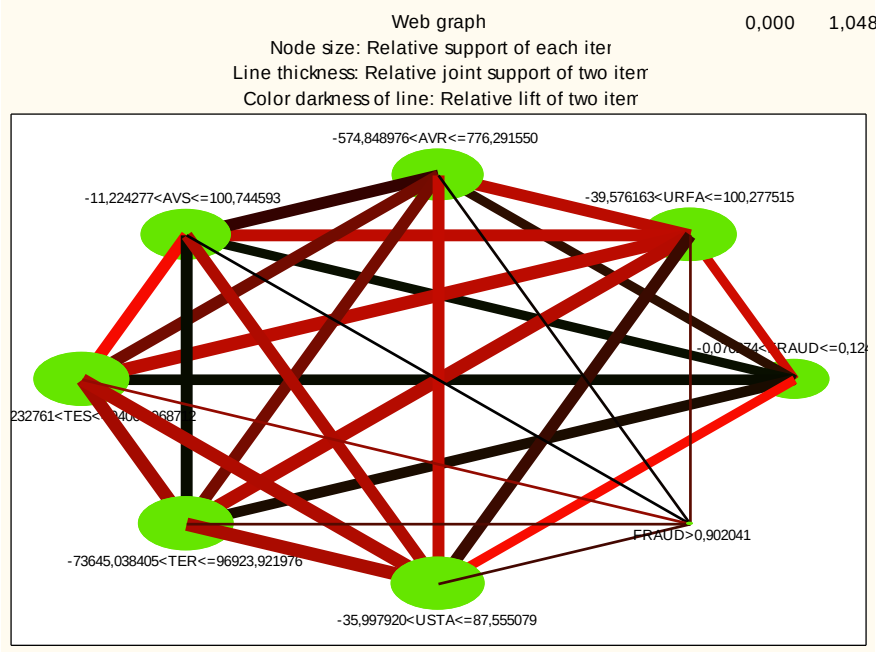


Рисунок 2.8 – Веб-граф підтримки виявлених асоціативних правил в розрізі здійснення фінансових кібершахрайств з використанням Ефіріум

Таким чином, обрана методологія дозволяє обробляти великі бази даних шляхом формування певних економічних алгоритмів, вирішення яких сприяє пошуку розв'язку поставленого завдання з незначними часовими витратами. Розроблений науково-методичний підхід дозволяє удосконалити

внутрішню систему фінансового моніторингу та підвищити рівень протидії фінансовим шахрайствам з використанням Ефіріуму.

2.4. **Методичні засади дослідження вплив криптовалюти на фінансову стабільність держави**

Провівши теоретичне дослідження особливостей розвитку криптовалюти та її значення на сучасному етапі розвитку національної економіки, актуальності набуває кількісна ідентифікація ступеня впливу криптовалюти на фінансову стабільність держави. Саме кількісна ідентифікація сили впливу зміни вартості та обсягу криптовалюти на складові фінансової стабільності держави дозволяє визначити її сучасну роль в суспільстві, встановити пріоритетність інструментів держаного регулювання та потенційні деструктивні наслідки.

Таким чином, запропоновано в якості об’єктів дослідження обрати чотири високо розвинуті Європейські країни (Німеччина, Фінляндія, Франція, Великобританія) та Україну. Це дозволить визначити загальну тенденцію впливу криптовалюти на фінансову стійкість держав Європи, а також з’ясувати рівень відхилення отриманих результатів для України та інших країн.

Отже, на першому етапі дослідження сформуємо інформаційну базу аналізу закономірностей впливу криптовалют на фінансову стабільність держав (Німеччини, Фінляндії, Франції, Великобританії, України). Так, в якості результативних ознак для Німеччини, Фінляндії, Франції, Великобританії обрано індекс фінансової стабільності, а для України запропоновано розширити сферу дослідження та застосувати індекс фінансового стресу, субіндекс банківського сектору, субіндекс поведінки домогосподарств, субіндекс валютного ринку. В якості факторних ознак для всіх країн обрано – вартість та обсяг криптовалют Біткоїн (BTC) та Ефіріум (ETH).

Провівши експрес-аналіз динаміки варіації індексу фінансової стабільності для Німеччини, Фінляндії, Франції, Великобританії (рисунки 2.9-2.10) справедливо зауважити, що для Німеччини й Франції динаміка досліджуваного показника майже ідентична, так аномальні зазначення за всіма періодами співпадають. У свою чергу, фінансова стабільність Фінляндії має тільки дві аномально зростаючи тенденції, а тренд для Великобританії навпаки постійно зростає та спадає.

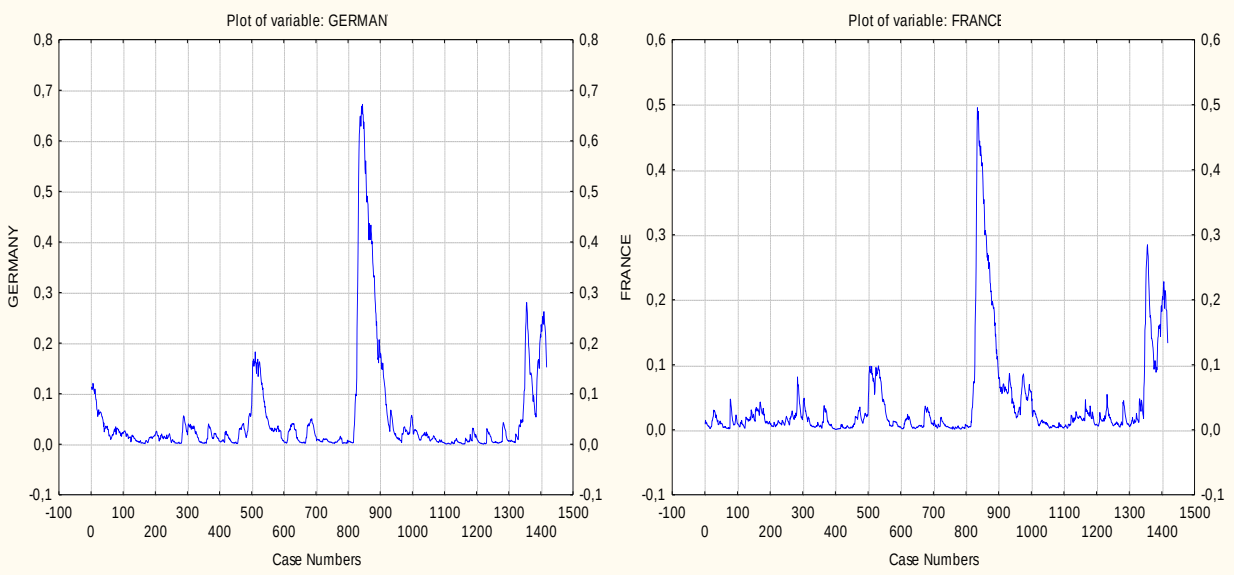


Рисунок 2.9 – Динаміка часового ряду індексу фінансової стабільності для Німеччини (лівий графік) та Франції (правий графік)

Переходячи до аналізу результативних показників характеристики фінансової стабільності України, зазначимо, що динаміка варіації індексів фінансового стресу, субіндексів банківського сектору, поведінки домогосподарств, валютного ринку (рисунок 2.11-2.12) носить хвилеподібний характер. Жодний з досліджуваних показників не розвивався поступово.

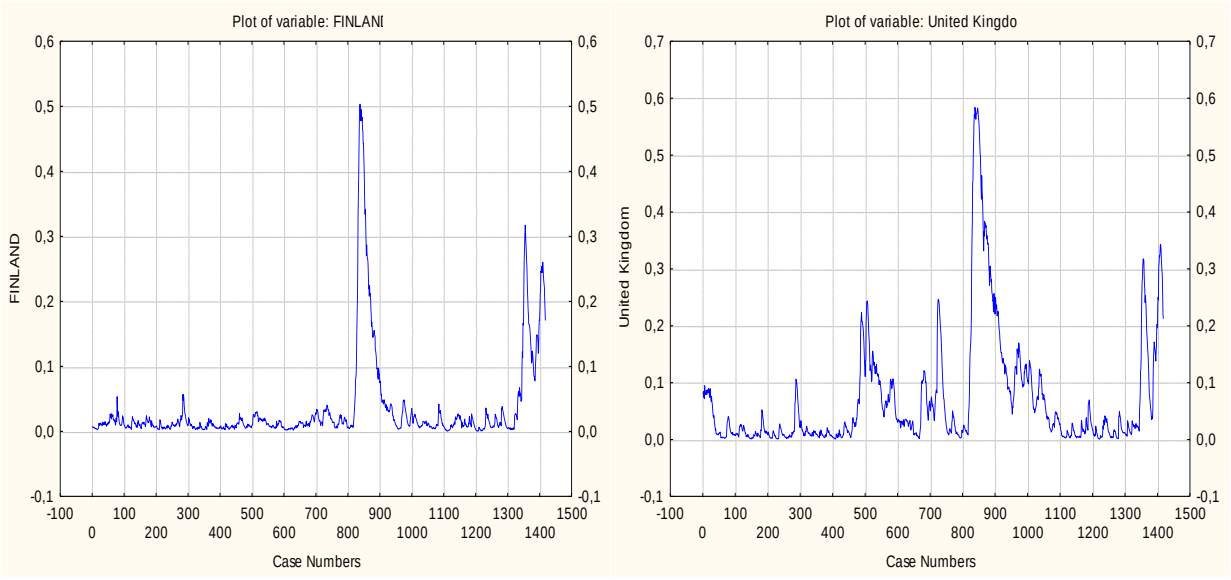


Рисунок 2.10 – Динаміка часового ряду індексу фінансової стабільності для Фінляндії (лівий графік) та Великобританії (правий графік)

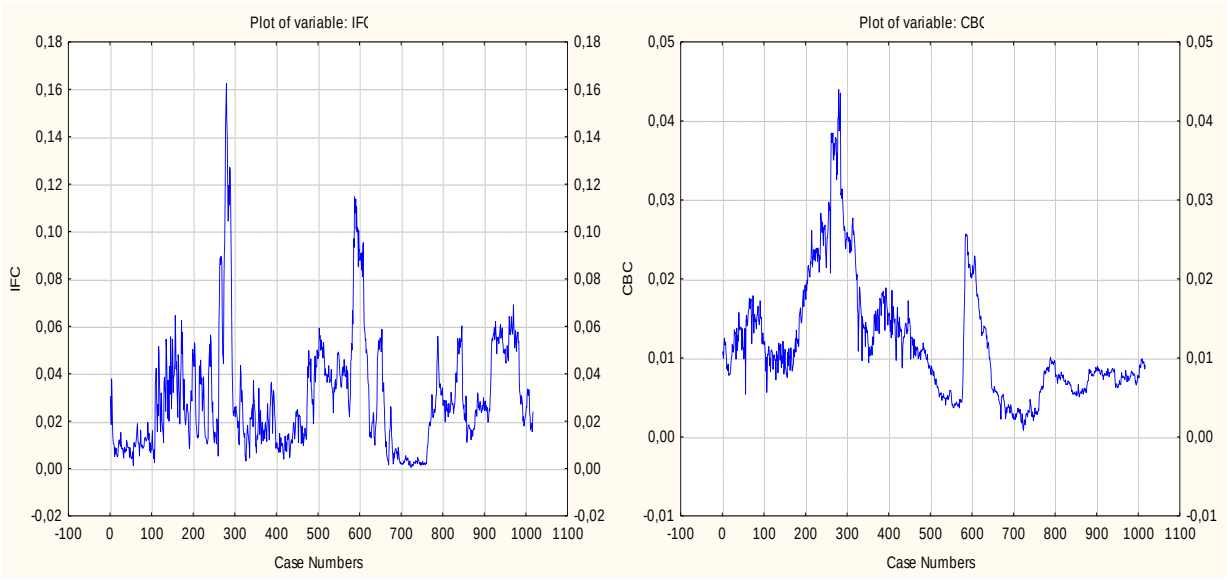


Рисунок 2.11 – Динаміка часового ряду індексу фінансового стресу (лівий графік) та субіндексу банківського сектору (правий графік) для України

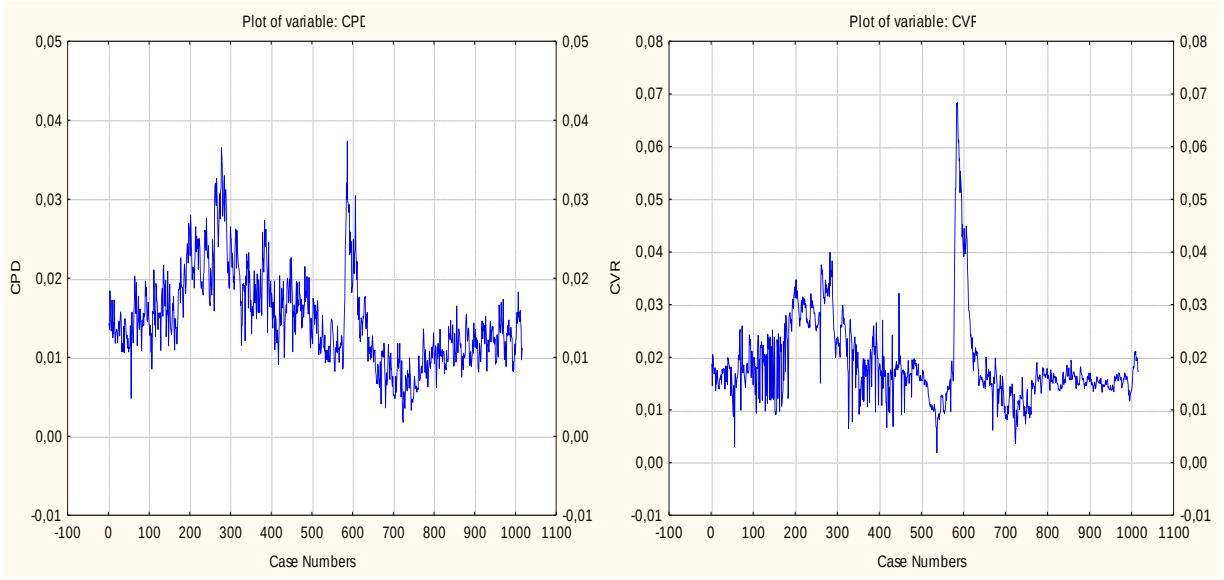


Рисунок 2.12 – Динаміка часового ряду субіндексу поведінки домогосподарств (лівий графік) та субіндексу валютного ринку (правий графік) для України

Переходячи до факторних ознак визначення впливу криптовалют на фінансову стабільність держави, представимо графічно динаміку варіації вартості та обсягів криптовалют BTC та ETH (рисунок 2.13-2.14).

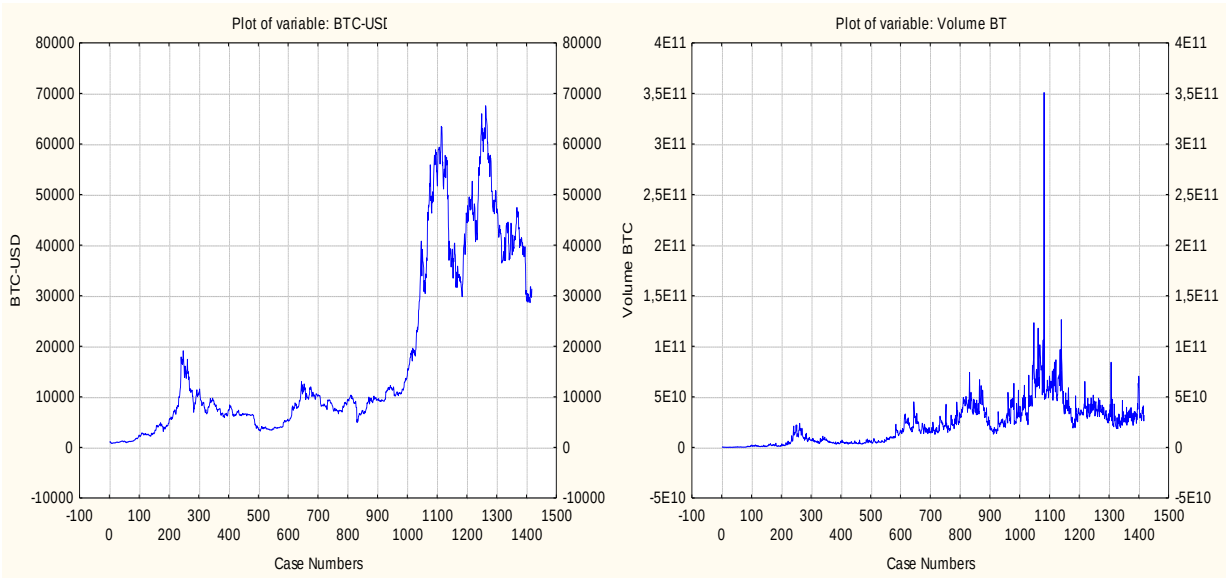


Рисунок 2.13 – Динаміка часового ряду вартості (лівий фрагмент) та обсягів криптовалют BTC (правий фрагмент)

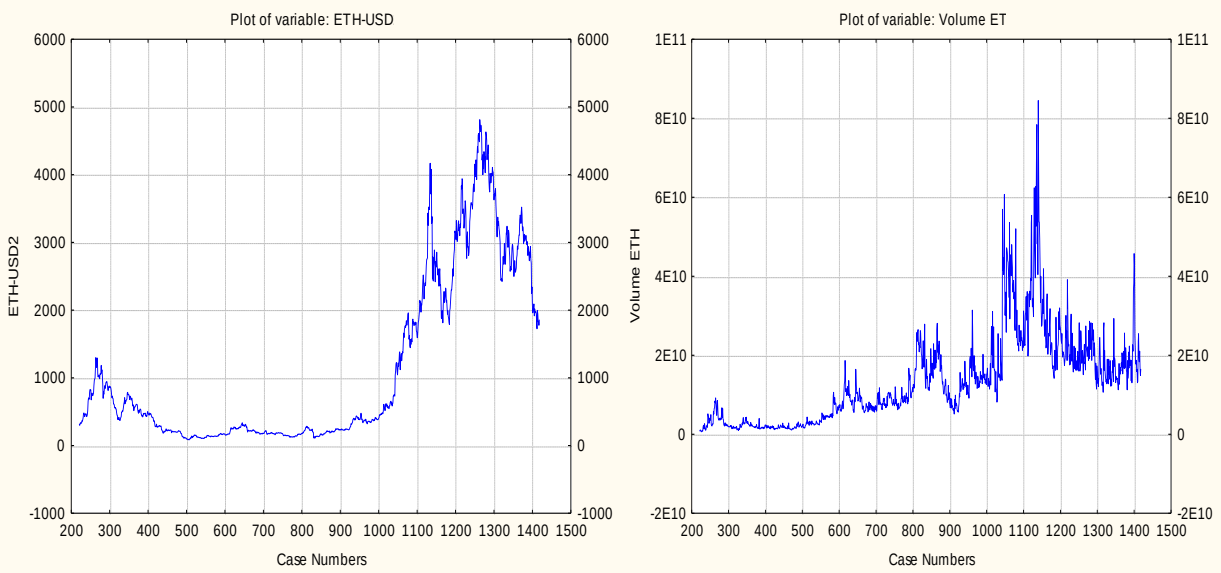


Рисунок 2.14 – Динаміка часового ряду вартості (лівий фрагмент) та обсягів криптовалют ETH (правий фрагмент)

На основі приведених вище рисунків, справедливо зауважити, що показники розвитку як Біткоїна, так й Ефіріума протягом досліджуваного періоду неодмінно змінювались. Досліджувані тренди результативних та факторних показників, зважаючи на їх постійні зміни, дозолять визначити необхідні взаємозв’язки, проте до цього завдання необхідно підходити комплексно, оскільки наявна щоденна динаміка усіх без виключення чинників може не дозолити ідентифікувати достовірні рівняння.

Таким чином, в першу чергу проведемо кореляційний аналізу залежності показників характеристики криптовалют та фінансової стабільності держави з метою підтвердження або спростування гіпотези наявності взаємозв’язків та необхідності виявлення закономірностей з урахуванням лагових затримок. Для реалізації даного етапу скористаємось програмою Statistica, інструментарієм Statistics/Multiple linear regression/Review descriptive statistics, correlation matrix. Отримані результаті представимо у вигляді таблиці 2.7.

Таблиця 2.7 – Кореляційна матриця залежності показників характеристики криптовалют (BTC та ETH) та фінансової стабільності Німеччини, Фінляндії, Франції, Великобританії

Показники	BTC	Volume BTC	ETH	Volume ETH	Німеччина	Фінляндія	Франція	Великобританія
BTC	1,0000	0,5896	0,9244	0,6997	-0,2266	-0,1277	-0,1798	-0,2910
Volume BTC	0,5896	1,0000	0,3972	0,8427	0,0916	0,1559	0,1240	0,0963
ETH	0,9244	0,3972	1,0000	0,5724	-0,2226	-0,1267	-0,1685	-0,3186
Volume ETH	0,6997	0,8427	0,5724	1,0000	-0,0049	0,0646	0,0353	-0,0182
Німеччина	-0,2266	0,0916	-0,2226	-0,0049	1,0000	0,9437	0,9746	0,9228
Фінляндія	-0,1277	0,1559	-0,1267	0,0646	0,9437	1,0000	0,9657	0,8725
Франція	-0,1798	0,1240	-0,1685	0,0353	0,9746	0,9657	1,0000	0,9132
Великобританія	-0,2910	0,0963	-0,3186	-0,0182	0,9228	0,8725	0,9132	1,0000

Аналіз кореляційної матриці (фрагмент перетину рядків Німеччина, Фінляндія, Франція, Великобританія та стовбців BTC, Volume BTC, ETH, Volume ETH) дозволяє стверджувати про відсутність підтвердженого зв’язку для всіх елементів матриці, окрім значення коефіцієнту кореляції на рівні «-0,31» в розрізі Великобританії для криптовалюти ETH. Підтвердженням відсутності зв’язку залежності показників характеристики криптовалют (криптовалют BTC та ETH) та фінансової стабільності держав виступають розраховані абсолютні значення коефіцієнтів кореляції на рівні не більше 0,3. Лише в розрізі Великобританії для криптовалюти ETH ідентифіковано слабкий обернений зв’язок. Виявлені закономірності дозволяють зробити висновок про доцільність врахування лагових затримок впливу криптовалют на фінансову стабільність держави.

Переходячи до проведення кореляційного аналізу залежності показників характеристики криптовалют та складових фінансової стабільності держави в розрізі України, розглянемо таблицю 2.8.

Таблиця 2.8 – Кореляційна матриця залежності показників характеристики криптовалют (криптовалют BTC та ETH) та індексів фінансового стресу (IFC), субіндексів банківського сектору (CBC), поведінки домогосподарств (CPD), валютного ринку (CVR) для України

Показники	BTC	Volume BTC	ETH	Volume ETH	IFC	CBC	CPD	CVR
BTC	1,0000	0,6096	0,8885	0,7133	0,0615	-0,4047	-0,3982	-0,2639
Volume BTC	0,6096	1,0000	0,3985	0,8438	0,0518	-0,4102	-0,4162	-0,1559
ETH	0,8885	0,3985	1,0000	0,5720	0,0652	-0,3211	-0,3051	-0,2179
Volume ETH	0,7133	0,8438	0,5720	1,0000	0,0446	-0,4317	-0,4395	-0,2020
IFC	0,0615	0,0518	0,0652	0,0446	1,0000	0,4162	0,5041	0,5617
CBC	-0,4047	-0,4102	-0,3211	-0,4317	0,4162	1,0000	0,8790	0,7404
CPD	-0,3982	-0,4162	-0,3051	-0,4395	0,5041	0,8790	1,0000	0,7849
CVR	-0,2639	-0,1559	-0,2179	-0,2020	0,5617	0,7404	0,7849	1,0000

Аналіз таблиці 2.8 (фрагменту перетину рядків IFC, CBC, CPD, CVR та стовбців BTC, Volume BTC, ETH2, Volume ETH) дозволяє стверджувати про наявність слабкого оберненого зв’язку для CBC, CPD в розрізі стовбців BTC, Volume BTC, ETH, Volume ETH та відсутність закономірностей для IFC та CVR. Зазначені факти виступають підтвердженням доцільності врахування лагових затримок при ідентифікації закономірностей впливу криптовалют на фінансову стабільність України.

Встановивши необхідність ідентифікації часових затримок проведемо автокореляційний аналіз за допомогою автокореляційних функцій та корелограм з метою вирішення поставленого завдання. Для реалізації даного етапу скористаємость програмою Statistica, інструментарієм Statistics/Advanced linear/nonlinear models/Times series and Forecasting/Autocorrelation та отримаємо наступні результати (рис. 2.15).

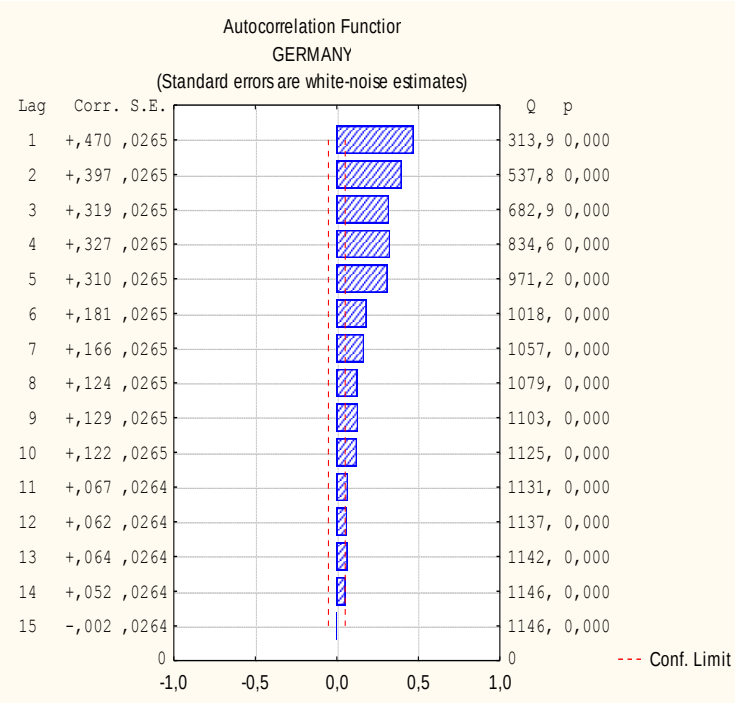


Рисунок 2.15 – Корелограми залежності значень автокореляційних функцій від часових лагів для Німеччини (лівий фрагмент) та Фінляндії (правий фрагмент)

Аналіз рисунку 2.15 (фрагменту в розрізі Німеччини) дозволяє констатувати варіацію значень автокореляційної функції різних рівнів часового ряду перших різниць фінансової стабільності в залежності від часового лагу та їх статистичну значущість до 11 рівня включно. Так, в розрізі значень автокореляційної функції спостерігається тенденція зменшення з першого до третього рівнів зі стрибкоподібним збільшенням значення автокореляційної функції четвертого рівня і подальшим поверненням до тенденції спадання рівнів. Даний факт свідчить про доцільність врахування лагових затримок впливу криптовалют на фінансову стабільність Німеччини на рівні 4.

Проведемо аналогічний аналіз корелограм впливу криптовалют на фінансову стабільність для Фінляндії, Франції, Великобританії, представлених на рисунках 2.15 (правий фрагмент), 2.16.

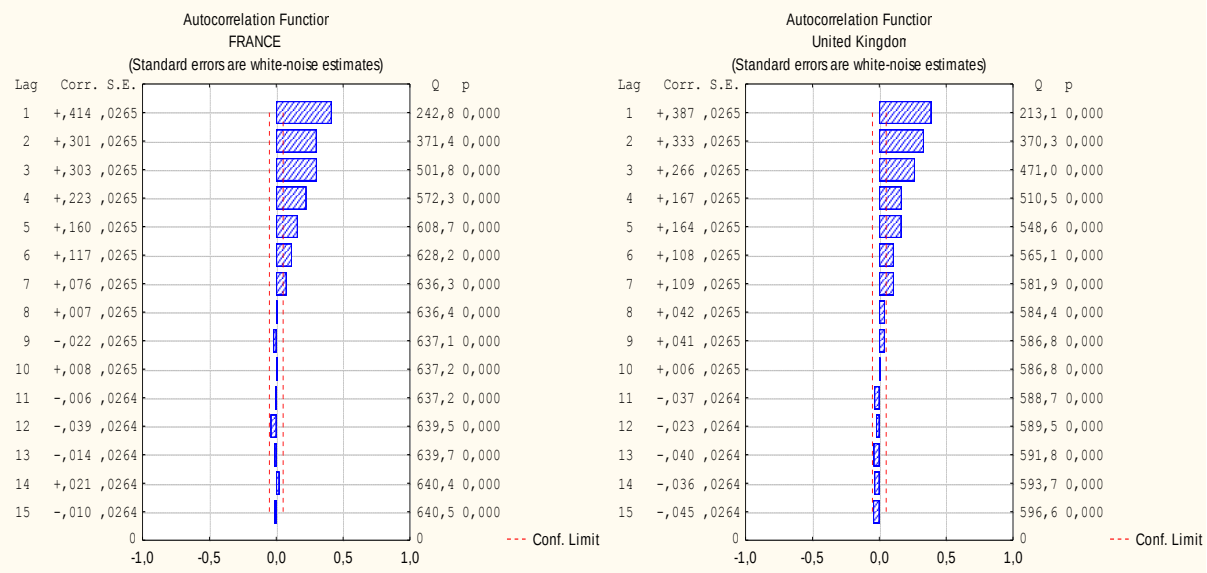


Рисунок 2.16 – Корелограми залежності значень автокореляційних функцій від часових лагів для Франції (лівий фрагмент) та Великобританії (правий фрагмент)

Таким чином, в розрізі розглянутих країн виявлена наступна закономірність лагової затримки впливу криптовалют на фінансову стабільність: Німеччина 4 дні, Фінляндія 4 дні, Франція 4 дні, Великобританія 5 днів.

Аналогічно проведеному і описаному вище автокореляційному аналізу, проведемо ідентифікацію лагових затримок впливу вартості та обсягів криптовалют BTC та ETH на індекс фінансового стресу, субіндекси банківського сектору, поведінки домогосподарств, валютного ринку для України. Для цього проаналізуємо корелограми, представлені на рисунках 2.17 і 2.18.

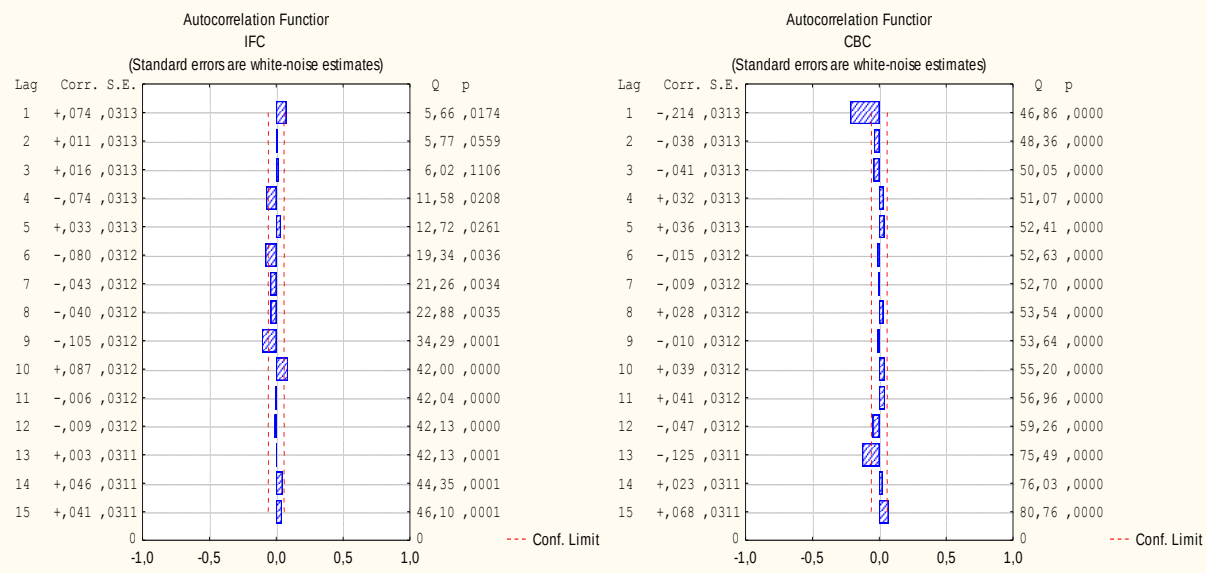


Рисунок 2.17 – Корелограми залежності значень автокореляційних функцій від часових лагів для України в розрізі індексу фінансового стресу (лівий фрагмент) та субіндексу банківського сектору (правий фрагмент)

Аналіз рисунку 2.17 (лівого фрагменту в розрізі показника фінансового стресу) дозволяє ідентифікувати статистично значуще пікове значення авкореляційної функції для часового лагу на рівні 6, який і пропонується розглянути в подальших дослідженнях сили на напрямку впливу криптовалют на фінансову стабільність держави. Аналогічно проведемо аналіз правого фрагменту рисунку 2.17 і рисунок 2.18.

Таким чином, на основі ґрунтового аналізу рисунків 2.17 і 2.18, було виявлено затримки впливу вартості та обсягів криптовалют BTC та ETH на індекс фінансового стресу на рівні 6 днів, субіндексу банківського сектору – 1 день, субіндексу поведінки домогосподарств – 5 днів, субіндексу валютного ринку – 1 день відповідно. Це цілком логічно, оскільки банківський і особливо валютний ринок реагують відразу на зміну вартості криптовалюти, домогосподарства ще певний час вижидають, оскільки розраховують, що ситуація повернеться до рівноважного стану, в свою чергу для індексу загального фінансового стресу зміни доходять найдовше, оскільки цей показник є комплексним та будь-який шок відчувається за кілька днів.

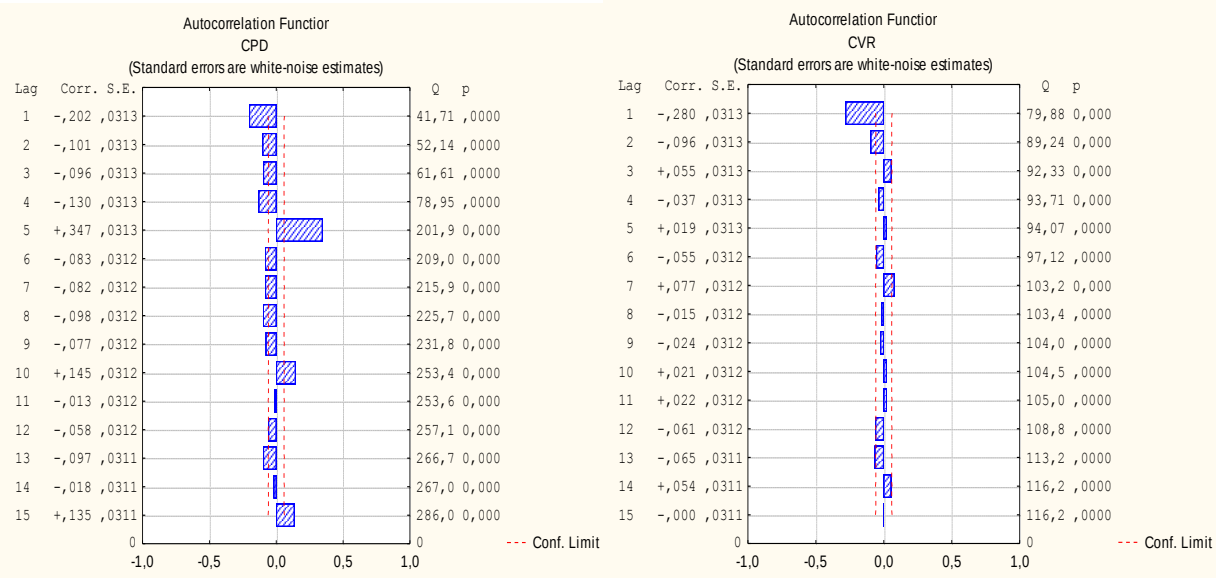


Рисунок 2.18 – Корелограми залежності значень автокореляційних функцій від часових лагів для України в розрізі субіндексу поведінки домогосподарств (лівий фрагмент) та субіндексу валютного ринку (правий фрагмент)

Встановивши час затримки впливу в подальшому актуальності набуває ідентифікація напрямку та кількісної його характеристики. Отже, побудуємо поліноміальні моделі розподіленого лагу Алмона впливу криптовалют на фінансову стабільність держави, параметри яких дозволили визначити напрямок та величину зазначеного впливу.

Аналіз розподіленого лагу – один із специфічних підходів до оцінювання затримки впливу одних рядів даних на інші, який дозволяє побудувати регресійну залежність з урахуванням лагових затримок значень одного часового ряду на основі іншого. Математично модель розподіленого лагу може бути записана у вигляді наступного співвідношення:

$$y_t = b_0 \cdot x_t + b_1 \cdot x_{t-1} + b_2 \cdot x_{t-2} + \cdots + b_k \cdot x_{t-k} \qquad (2.10)$$

де y_t – залежна змінна в момент часу t;

x_t – незалежна змінна в момент часу t;

x_{t-k} – незалежна змінна з лаговою затримкою $t-k$;

b_k – коефіцієнти лінійного регресійного рівняння.

У випадках наявної сильної кореляційної залежності в масиві незалежних змінних, тобто виявленому факті мультиколінеарності, для оцінювання параметрів лінійного регресійного рівняння b_k застосовується поліноміальний підхід Алмона, який формалізовано наступним чином:

$$b_k = a_0 + a_1 \cdot i + a_2 \cdot i^2 + \cdots + a_q \cdot i^q, q < k \qquad (2.11)$$

де a_q – поліноміальні коефіцієнти регресійної моделі.

Для реалізації даного етапу пропонується скористатись програмою Statistica, інструментарієм Statistics/Advanced linear/nonlinear models/Times series and Forecasting/Distributed lags analysis. Отримані результати представимо у вигляді таблиць 2.9-2.24.

Таблиця 2.9 – Фрагмент поліноміальної моделі розподіленого лагу Алмона в розрізі впливу вартості криптовалюти BTC на фінансову стабільність Німеччини

Lag	Almon Polyn. Distr.Lags; Regression Coefficients (Spreadsheet1.sta) Indep: BTC Dep: GERMANY Lag: 4 Polyn. order: 1 R=,2440 R-square=,0595 N: 1414			
	Regressn	Standard	t(1409)	P
0	-0,000000053632	0,000001071311	-0,050061847152	0,960080200017
1	0,000000089078	0,000000535793	0,166254240591	0,867980726201
2	0,000000231788	0,000000024518	9,453917109480	0,000000000000
3	0,000000374497	0,000000536924	0,697485837405	0,485613861406
4	0,000000517207	0,000001072443	0,482269702974	0,629689294333

Аналіз p-рівня (останній стовпчик таблиці 2.9) дозволяє стверджувати про статистичну значущість в розрізі впливу вартості криптовалюти BTC на фінансову стабільність Німеччини лише лагу на рівні 2 дні, оскільки відповідне значення ймовірності не перевищує 0,05. Відповідно, стандартна

похибка для 2-денної лагової затримки є найменшою, критерій Стьюдента статистичної значущості відповідного регресійного коефієнту моделі розподіленого лагу Алмона є найбільшим і перевищує критично допустимий рівень. Отже, на основі даних графи «Regressn Coeff» таблиці 3 закономірність впливу вартості криптовалюти BTC на фінансову стабільність Німеччини може бут формалізована у вигляді наступної моделі:

$$Germany(t) = 0.2318 \cdot 10^{-6} \cdot BTC\_USD(t-2) \qquad (2.12)$$

де $Germany(t)$ – індекс фінансової стабільності Німеччини в момент часу t; $BTC\_USD(t-2)$ – значення вартості крипто валюти BTC в момент часу $t-2$.

Аналіз регресійного коефіцієнту моделі Алмона (2.10) перед змінною $BTC\_USD(t-2)$ свідчить про те, що зі зростанням вартості криптовалюти BTC на 1 од., фінансова стабільність Німеччини зросте на $0.2318 \cdot 10^{-6}$ з затримкою у 2 дні.

Проведемо аналогічний аналіз та формалізацію поліноміальної моделі розподіленого лагу Алмона для інших країн та показників.

Таблиця 2.10 – Фрагмент поліноміальної моделі розподіленого лагу Алмона в розрізі впливу обсягів криптовалюти BTC на фінансову стабільність Німеччини

Lag	Almon Polyn. Distr.Lags; Regression Coefficients (Spreadsheet1.sta) Indep: Volume BTC Dep: GERMANY Lag: 4 Polyn. order: 1 R=,4299 R-square=,1848 N: 1414			
	Regressn Coeff.	StandardError	t(1409)	P
0	0,000000000000233	0,000000000000	1,29846618586	0,194339647967
1	0,000000000000283	0,000000000000	3,11114010202	0,001901078714
2	0,000000000000333	0,000000000000	17,88321681055	0,000000000000
3	0,000000000000384	0,000000000000	4,21403980534	0,000026678838
4	0,000000000000434	0,000000000000	2,42312839910	0,015512809203

На основі застосування статистично значущих лагів та регресійних коефіцієнтів (таблиця 2.10) поліноміальна моделі розподіленого лагу Алмона

в розрізі впливу обсягів криптовалюти BTC на фінансову стабільність Німеччини набуває вигляду:

$$Germany(t) = 0.333 \cdot 10^{-12} \cdot VBTC(t-2) + 0.384 \cdot 10^{-12} \cdot VBTC(t-3) + 0.283 \cdot 10^{-12} \cdot VBTC(t-1) + 0.434 \cdot 10^{-12} \cdot VBTC(t-4) \quad (2.13)$$

де $VBTC(t-m)$ – значення обсягів криптовалюти BTC в момент часу $t-m$.

Таблиця 2.11 – Фрагмент поліноміальної моделі розподіленого лагу Алмона в розрізі впливу вартості криптовалюти ETH на фінансову стабільність Німеччини

Lag	Almon Polyn. Distr.Lags; Regression Coefficients (Spreadsheet1.sta) Indep: ETH2 Dep: GERMANY Lag: 4 Polyn. order: 1 R=,2060 R-square=,0424 N: 1194			
	RegressnCoeff.	StandardError	t(1189)	p
0	-0,000010927384	0,000015635644	-0,698876517878	0,484765883570
1	-0,000003906621	0,000007822964	-0,499378644865	0,617605057008
2	0,000003114142	0,000000430918	7,226758469037	0,000000000001
3	0,000010134905	0,000007837992	1,293048626715	0,196245396356
4	0,000017155667	0,000015650688	1,096160571991	0,273230465984

На основі застосування статистично значущих лагів та регресійних коефіцієнтів (таблиця 2.11) поліноміальна моделі розподіленого лагу Алмона в розрізі впливу вартості криптовалюти ETH на фінансову стабільність Німеччини набуває вигляду:

$$Germany(t) = 0.3114 \cdot 10^{-5} \cdot ETH\_USD(t-2) \quad (2.14)$$

де $ETH\_USD(t-m)$ – значення вартості криптовалюти ETH в момент часу $t-m$.

На основі застосування статистично значущих лагів та регресійних коефіцієнтів (таблиця 2.12) поліноміальна моделі розподіленого лагу Алмона в розрізі впливу обсягів криптовалюти ETH на фінансову стабільність Німеччини набуває вигляду:

$$Germany(t) = 0.534 \cdot 10^{-12} \cdot VETH(t-2) + 0.707 \cdot 10^{-12} \cdot VETH(t-3) \quad (2.14)$$

де $VBTC(t-m)$ – значення обсягів криптовалюти ETH в момент часу $t-m$.

Таблиця 2.12 – Фрагмент поліноміальної моделі розподіленого лагу Алмона в розрізі впливу обсягів криптовалюти ETH на фінансову стабільність Німеччини

Lag	Almon Polyn. Distr.Lags; Regression Coefficients (Spreadsheet1.sta) Indep: Volume ETH Dep: GERMANY Lag: 4 Polyn. order: 1 R=,3651 R-square=,1333 N: 1194			
	RegressnCoeff.	StandardError	t(1189)	p
0	0,000000000000187	0,000000000000	0,39307121727	0,694337342826
1	0,000000000000360	0,000000000000	1,50001242057	0,133876696969
2	0,000000000000534	0,000000000000	13,52319126399	0,000000000000
3	0,000000000000707	0,000000000000	2,93846158797	0,003362109258
4	0,000000000000881	0,000000000000	1,84892168294	0,064717219110

Таблиця 2.13 – Фрагмент поліноміальної моделі розподіленого лагу Алмона в розрізі впливу вартості криптовалюти BTC на фінансову стабільність Франції

Lag	Almon Polyn. Distr.Lags; Regression Coefficients (Spreadsheet1.sta) Indep: BTC Dep: FRANCE Lag: 4 Polyn. order: 1 R=,3315 R-square=,1099 N: 1414			
	RegressnCoeff.	StandardError	T(1409)	p
0	-0,000000384366	0,000000743208	-0,51717242789	0,605116970978
1	-0,000000079974	0,000000371699	-0,21515816297	0,829675148764
2	0,000000224418	0,000000017009	13,19426571558	0,000000000000
3	0,000000528811	0,000000372484	1,41968612079	0,155920266719
4	0,000000833203	0,000000743993	1,11990676875	0,262944326734

На основі застосування статистично значущих лагів та регресійних коефіцієнтів (таблиця 2.13) поліноміальна моделі розподіленого лагу Алмона в розрізі впливу вартості криптовалюти BTC на фінансову стабільність Франції набуває вигляду:

$$France(t) = 0.2244 \cdot 10^{-6} \cdot BTC\_USD(t-2) \quad (2.16)$$

де $France(t)$ – індекс фінансової стабільності Франції в момент часу t;
$BTC\_USD(t-m)$ – значення вартості криптовалюти BTC в момент часу $t-m$.

Таблиця 2.14 – Фрагмент поліноміальної моделі розподіленого лагу Алмона в розрізі впливу обсягів криптовалюти BTC на фінансову стабільність Франції

Lag	Almon Polyn. Distr.Lags; Regression Coefficients (Spreadsheet1.sta) Indep: Volume BTC Dep: FRANCE Lag: 4 Polyn. order: 1 R=,4879 R-square=,2380 N: 1414			
	Regressn Coeff.	StandardError	T(1409)	p
0	0,000000000000191	0,000000000000	1,54355599463	0,122920494121
1	0,000000000000230	0,000000000000	3,67112182717	0,000250508848
2	0,000000000000270	0,000000000000	20,99278757891	0,000000000000
3	0,000000000000309	0,000000000000	4,92780298474	0,000000930010
4	0,000000000000349	0,000000000000	2,82517156441	0,004792159576

На основі застосування статистично значущих лагів та регресійних коефіцієнтів (таблиця 2.9) поліноміальна моделі розподіленого лагу Алмона в розрізі впливу обсягів криптовалюти BTC на фінансову стабільність Франції набуває вигляду:

$$France(t) = 0.270 \cdot 10^{-12} \cdot VBTC(t-2) + 0.309 \cdot 10^{-12} \cdot VBTC(t-3) + 0.230 \cdot 10^{-12} \cdot VBTC(t-1) + 0.349 \cdot 10^{-12} \cdot VBTC(t-4) \quad (2.17)$$

де $VBTC(t-m)$ – значення обсягів криптовалюти BTC в момент часу $t-m$.

Таблиця 2.15 – Фрагмент поліноміальної моделі розподіленого лагу Алмона в розрізі впливу вартості криптовалюти ETH на фінансову стабільність Франції

Lag	Almon Polyn. Distr.Lags; Regression Coefficients (Spreadsheet1.sta) Indep: ETH Dep: FRANCE Lag: 4 Polyn. order: 1 R=,3030 R-square=,0918 N: 1194			
	RegressnCoeff.	StandardError	T(1189)	p
0	-0,000010660193	0,000010901608	-0,97785511582	0,328344912999
1	-0,000003689425	0,000005454389	-0,67641403414	0,498909380784
2	0,000003281342	0,000000300448	10,92148978220	0,000000000000
3	0,000010252109	0,000005464867	1,87600347575	0,060899616624
4	0,000017222876	0,000010912097	1,57832874279	0,114756065828

На основі застосування статистично значущих лагів та регресійних коефіцієнтів (таблиця 2.10) поліноміальна моделі розподіленого лагу Алмона в розрізі впливу вартості криптовалюти ETH на фінансову стабільність Франції набуває вигляду:

$$France(t) = 0.3281 \cdot 10^{-5} \cdot ETH\_USD(t-2) \qquad (2.18)$$

де $ETH\_USD(t-m)$ – значення вартості криптовалюти ETH в момент часу $t-m$.

Таблиця 2.16 – Фрагмент поліноміальної моделі розподіленого лагу Алмона в розрізі впливу обсягів криптовалюти ETH на фінансову стабільність Франції

Lag	Almon Polyn. Distr.Lags; Regression Coefficients (Spreadsheet1.sta) Indep: Volume ETH Dep: FRANCE Lag: 4 Polyn. order: 1 R=,4315 R-square=,1862 N: 1194			
	RegressnCoeff.	StandardError	T(1189)	p
0	0,000000000000103	0,000000000000	0,31206285893	0,755047455984
1	0,000000000000277	0,000000000000	1,66319849330	0,096536259651
2	0,000000000000451	0,000000000000	16,48649347406	0,000000000000
3	0,000000000000626	0,000000000000	3,74760518266	0,000187101587
4	0,000000000000800	0,000000000000	2,42107724636	0,015623534221

На основі застосування статистично значущих лагів та регресійних коефіцієнтів (таблиця 2.16) поліноміальна моделі розподіленого лагу Алмона в розрізі впливу обсягів криптовалюти ETH на фінансову стабільність Франції набуває вигляду:

$$France(t) = 0.451 \cdot 10^{-12} \cdot VETH(t-2) + 0.626 \cdot 10^{-12} \cdot VETH(t-3) + 0.800 \cdot 10^{-12} \cdot VETH(t-4) \quad (2.19)$$

де $VETH(t-m)$ – значення обсягів криптовалюти ETH в момент часу $t-m$.

Таблиця 2.17 – Фрагмент поліноміальної моделі розподіленого лагу Алмона в розрізі впливу вартості криптовалюти BTC на фінансову стабільність Фінляндії

Lag	Almon Polyn. Distr.Lags; Regression Coefficients (Spreadsheet1.sta) Indep: BTC Dep: FINLAND Lag: 4 Polyn. order: 1 R=,3259 R-square=,1062 N: 1414			
	Regressn Coeff.	Standard Error	T(1409)	p
0	-0,000000191675	0,000000723237	-0,26502326335	0,791030304169
1	0,000000011349	0,000000361711	0,03137531500	0,974974671120
2	0,000000214372	0,000000016552	12,95165208778	0,000000000000
3	0,000000417396	0,000000362475	1,15151517470	0,249715724529
4	0,000000620419	0,000000724002	0,85693082267	0,391628817679

На основі застосування статистично значущих лагів та регресійних коефіцієнтів (таблиця 2.12) поліноміальна моделі розподіленого лагу Алмона в розрізі впливу вартості криптовалюти BTC на фінансову стабільність Фінляндії набуває вигляду:

$$Finland(t) = 0.2144 \cdot 10^{-6} \cdot BTC\_USD(t-2) \quad (2.20)$$

де $Finland(t)$ – індекс фінансової стабільності Фінляндії в момент часу t;

$BTC\_USD(t-m)$ – значення вартості криптовалюти BTC в момент часу $t-m$.

Таблиця 2.18 – Фрагмент поліноміальної моделі розподіленого лагу Алмона в розрізі впливу обсягів криптовалюти BTC на фінансову стабільність Фінляндії

Lag	Almon Polyn. Distr.Lags; Regression Coefficients (Spreadsheet1.sta) Indep: Volume BTC Dep: FINLAND Lag: 4 Polyn. order: 1 R=,4677 R-square=,2187 N: 1414			
	Regressn Coeff.	Standard Error	T(1409)	p
0	0,000000000000123	0,000000000000	1,01252753635	0,311459749601
1	0,000000000000187	0,000000000000	3,03185744160	0,002474902026
2	0,000000000000251	0,000000000000	19,85632071844	0,000000000000
3	0,000000000000315	0,000000000000	5,10091923414	0,000000384040
4	0,000000000000379	0,000000000000	3,11936058516	0,001849182216

На основі статистично значущих лагів та регресійних коефіцієнтів поліноміальна моделі розподіленого лагу Алмона в розрізі впливу обсягів криптовалюти BTC на фінансову стабільність Фінляндії набуває вигляду:

$$Finland(t) = 0.251 \cdot 10^{-12} \cdot VBTC(t-2) + 0.315 \cdot 10^{-12} \cdot VBTC(t-3) + 0.379 \cdot 10^{-12} \cdot VBTC(t-4) + 0.187 \cdot 10^{-12} \cdot VBTC(t-1) \quad (2.21)$$

$VBTC(t-m)$ – значення обсягів криптовалюти BTC в момент часу $t-m$.

Таблиця 2.19 – Фрагмент поліноміальної моделі розподіленого лагу Алмона в розрізі впливу вартості криптовалюти ETH на фінансову стабільність Фінляндії

Lag	Almon Polyn. Distr.Lags; Regression Coefficients (Spreadsheet1.sta) Indep: ETH2 Dep: FINLAND Lag: 4 Polyn. order: 1 R=,3015 R-square=,0909 N: 1194			
	Regressn Coeff.	Standard Error	T(1189)	p
0	-0,000008687986	0,000010603602	-0,81934297612	0,412754935229
1	-0,000002754557	0,000005305288	-0,51920977680	0,603711107125
2	0,000003178871	0,000000292235	10,87778597415	0,000000000000
3	0,000009112300	0,000005315479	1,71429511415	0,086735120044
4	0,000015045729	0,000010613804	1,41756233999	0,156580568591

На основі застосування статистично значущих лагів та регресійних коефіцієнтів (таблиця 2.19) поліноміальна моделі розподіленого лагу Алмона в розрізі впливу вартості криптовалюти ETH на фінансову стабільність Фінляндії набуває вигляду:

$$Finland(t) = 0.3179 \cdot 10^{-5} \cdot ETH(t-2) \quad (2.22)$$

де $ETH(t-m)$ – значення вартості криптовалюти ETH в момент часу $t-m$.

Таблиця 2.20 – Фрагмент поліноміальної моделі розподіленого лагу Алмона в розрізі впливу обсягів криптовалюти ETH на фінансову стабільність Фінляндії

Lag	Almon Polyn. Distr.Lags; Regression Coefficients (Spreadsheet1.sta) Indep: Volume ETH Dep: FINLAND Lag: 4 Polyn. order: 1 R=,4114 R-square=,1692 N: 1194			
	RegressnCoeff.	StandardError	T(1189)	p
0	0,000000000000027	0,000000000000	0,08198726881	0,934670635708
1	0,000000000000222	0,000000000000	1,35770223273	0,174815784609
2	0,000000000000418	0,000000000000	15,54091540005	0,000000000000
3	0,000000000000614	0,000000000000	3,74243407419	0,000190949153
4	0,000000000000809	0,000000000000	2,49422306531	0,012758280560

На основі застосування статистично значущих лагів та регресійних коефіцієнтів (таблиця 2.20) поліноміальна моделі розподіленого лагу Алмона в розрізі впливу обсягів криптовалюти ETH на фінансову стабільність Фінляндії набуває вигляду:

$$Finland(t) = 0.418 \cdot 10^{-12} \cdot VETH(t-2) + 0.614 \cdot 10^{-12} \cdot VETH(t-3) + 0.809 \cdot 10^{-12} \cdot VETH(t-4) \quad (2.23)$$

де $VETH(t-m)$ – значення обсягів криптовалюти ETH в момент часу $t-m$.

Таблиця 2.21 – Фрагмент поліноміальної моделі розподіленого лагу Алмона в розрізі впливу вартості криптовалюти BTC на фінансову стабільність Великобританії

Lag	Almon Polyn. Distr.Lags; Regression Coefficients (Spreadsheet1.sta) Indep: BTC Dep: United Kingdom Lag: 5 Polyn. order: 1 R=,3264 R-square=,1065 N: 1413			
	Regressn Coeff.	StandardError	T(1407)	p
0	0,000000859043	0,000000878588	0,977753622949	0,328364265747
1	0,000000626032	0,000000527211	1,187441310728	0,235254014181
2	0,000000393021	0,000000176526	2,226426952363	0,026143422041
3	0,000000160010	0,000000177615	0,900884978380	0,367803672115
4	-0,000000073000	0,000000528307	-0,138177791395	0,890119684015
5	-0,000000306011	0,000000879685	-0,347864375935	0,727994080570

На основі застосування статистично значущих лагів та регресійних коефіцієнтів (таблиця 2.21) поліноміальна моделі розподіленого лагу Алмона в розрізі впливу вартості криптовалюти BTC на фінансову стабільність Великобританії набуває вигляду:

$$United\_Kingdom(t) = 0.3930 \cdot 10^{-6} \cdot BTC\_USD(t-2) \qquad (2.24)$$

де $United\_Kingdom(t)$ – індекс фінансової стабільності Великобританії в момент часу t;

$BTC\_USD(t-m)$ – значення вартості криптовалюти BTC в момент часу $t-m$.

Таблиця 2.22 – Фрагмент поліноміальної моделі розподіленого лагу Алмона в розрізі впливу обсягів криптовалюти BTC на фінансову стабільність Великобританії

Lag	Almon Polyn. Distr.Lags; Regression Coefficients (Spreadsheet1.sta) Indep: Volume BTC Dep: United Kingdom Lag: 5 Polyn. order: 1 R=,5385 R-square=,2900 N: 1413			
	Regressn Coeff.	StandardError	T(1407)	p
0	0,000000000000313	0,000000000000	1,94050070477	0,052518405064
1	0,000000000000338	0,000000000000	3,45935773563	0,000557639446
2	0,000000000000362	0,000000000000	10,15565562057	0,000000000000
3	0,000000000000387	0,000000000000	10,80069719453	0,000000000000
4	0,000000000000411	0,000000000000	4,20506911815	0,000027747998
5	0,000000000000436	0,000000000000	2,69611632943	0,007098968547

На основі застосування статистично значущих лагів та регресійних коефіцієнтів (таблиця 2.22) поліноміальна моделі розподіленого лагу Алмона в розрізі впливу обсягів криптовалюти BTC на фінансову стабільність Великобританії набуває вигляду:

$$United\_Kingdom(t) = 0.362 \cdot 10^{-12} \cdot VBTC(t-2) + 0.387 \cdot 10^{-12} \cdot VBTC(t-3) + 0.411 \cdot 10^{-12} \cdot VBTC(t-4) + 0.338 \cdot 10^{-12} \cdot VBTC(t-1) + 0.436 \cdot 10^{-12} \cdot VBTC(t-5) + 0.313 \cdot 10^{-12} \cdot VBTC(t) \quad (2.25)$$

де $VBTC(t-m)$ – значення обсягів криптовалюти BTC в момент часу $t-m$.

Таблиця 2.23 – Фрагмент поліноміальної моделі розподіленого лагу Алмона в розрізі впливу вартості криптовалюти ETH на фінансову стабільність Великобританії

Lag	Almon Polyn. Distr.Lags; Regression Coefficients (Spreadsheet1.sta) Indep: ETH2 Dep: United Kingdom Lag: 5 Polyn. order: 1 R=,2539 R-square=,0645 N: 1193			
	RegressnCoeff.	StandardError	T(1187)	p
0	-0,000003347205	0,000013120472	-0,255113155108	0,798679890966
1	-0,000000624843	0,000007875208	-0,079343082199	0,936773113315
2	0,000002097519	0,000002644698	0,793103275950	0,427876141979
3	0,000004819880	0,000002659583	1,812269339778	0,070197156189
4	0,000007542242	0,000007890232	0,955896141883	0,339319317417
5	0,000010264604	0,000013135508	0,781439460434	0,434699910761

На основі застосування статистично значущих лагів та регресійних коефіцієнтів (таблиця 2.23) поліноміальна моделі розподіленого лагу Алмона в розрізі впливу вартості криптовалюти ETH на фінансову стабільність Великобританії набуває вигляду:

$$United\_Kingdom(t) = 0.4820 \cdot 10^{-5} \cdot ETH\_USD(t-2) \quad (2.26)$$

де $ETH\_USD(t-m)$ – значення вартості криптовалюти ETH в момент часу $t-m$.

Таблиця 2.24 – Фрагмент поліноміальної моделі розподіленого лагу Алмона в розрізі впливу обсягів криптовалюти ETH на фінансову стабільність Великобританії

Lag	Almon Polyn. Distr.Lags; Regression Coefficients (Spreadsheet1.sta) Indep: Volume ETH Dep: United Kingdom Lag: 5 Polyn. order: 1 R=,4634 R-square=,2148 N: 1193			
	Regressn Coeff.	Standard Error	T(1187)	p
0	0,000000000000311	0,000000000000	0,731465453946	0,464639277821
1	0,000000000000430	0,000000000000	1,677095838265	0,093787016082
2	0,000000000000549	0,000000000000	6,029639564365	0,000000002191
3	0,000000000000668	0,000000000000	7,305297621390	0,000000000001
4	0,000000000000787	0,000000000000	3,065102968320	0,002225073772
5	0,000000000000906	0,000000000000	2,129714599025	0,033400444334

На основі застосування статистично значущих лагів та регресійних коефіцієнтів (таблиця 2.24) поліноміальна моделі розподіленого лагу Алмона в розрізі впливу обсягів криптовалюти ETH на фінансову стабільність Великобританії набуває вигляду:

$$United\_Kingdom(t) = 0.549 \cdot 10^{-12} \cdot VETH(t-2) + 0.668 \cdot 10^{-12} \cdot VETH(t-3) + 0.787 \cdot 10^{-12} \cdot VETH(t-4) + 0.906 \cdot 10^{-12} \cdot VETH(t-5) \quad (2.27)$$

де $VETH(t-m)$ – значення обсягів криптовалюти ETH в момент часу $t-m$.

Аналіз наведених вище моделей розподіленого лагу (2.9) – (2.25) дозволяє систематизувати величини лагових затримок та напрямки впливу криптовалют на фінансову стабільність Німеччини, Фінляндії, Франції, Великобританії у вигляді таблиці 2.25.

Таблиця 2.25 – Максимальні статистично значущі величини лагів впливу криптовалют на фінансову стабільність держави

Країна	BTC	Volume BTC	ETH	Volume ETH
Німеччина	2+	3+	2+	3+
Фінляндія	2+	4+	2+	4+
Франція	2+	4+	2+	4+
Великобританія	2+	5+	3*+	4+

Примітка: * - статистична значущість на рівні 0,9

Таким чином, найбільший обсяг лагової затримки спостерігається на рівні 5 днів в розрізі Великобританії за показником обсягів кріптовалюти BTC, причому у першому випадку вплив є прямим, тобто зі збільшенням факторної ознаки результативна зростає, а в другому випадку – відповідно, оберненим. При зростанні вартості криптовалюти BTC рівень фінансової стабільності Німеччини, Фінляндії, Франції та Великобританії буде зростати із затримкою у 2 дні, але дана закономірність характерна з меншим рівнем статистичної знучащості (0,9, а не 0,95). Лагова затримка на рівні 2 днів характерна і в розрізі впливу вартості криптовалюти ETH на фінансову стабільність Німеччини, Фінляндії та Франції. Виключенням із 2-днівної закономірності лагу залежності фінансової стабільності під впливом варіації вартості криптовалюти ETH виступає Великобританія, затримка для яких є тривалішою на рівні 3 дні і 5 днів відповідно. При зростанні обсягів криптовалюти BTC та ETH рівень фінансової стабільності Фінляндії та Франції буде зростати із затримкою у 4 дні. Такий же 4-денний лаг характерний в розрізі впливу зміни обсягів криптовалюти ETH на результативну ознаку. В цілому справедливо зауважити, що для всіх Європейських країн в межах різник криптовалют часовий лаг затримки є майже однаковим, це свідчить про відносну подібність реагування фінансової системи держав на виклики цифрового суспільства.

Визначивши величини лагової затримки впливу криптовалют на фінансову стабільність держави для розглянутих країн, виникає необхідність кількісного оцінювання обсягу даного впливу, що пропонується провести на

основі регресійних коефіцієнтів поліноміальної моделі розподіленого лагу Алмона (таблиця 2.26).

Таблиця 2.26 – Регресійні коефіцієнти поліноміальної моделі розподіленого лагу Алмона при максимальній статистично значущій величині лагу впливу криптовалют на фінансову стабільність держави

Країни	BTC	Volume BTC	ETH	Volume ETH
Німеччина	$0.2318 \cdot 10^{-6}$	$0.333 \cdot 10^{-12}$	$0.3114 \cdot 10^{-5}$	$0.534 \cdot 10^{-12}$
Фінляндія	$0.2144 \cdot 10^{-6}$	$0.251 \cdot 10^{-12}$	$0.3179 \cdot 10^{-5}$	$0.418 \cdot 10^{-12}$
Франція	$0.2244 \cdot 10^{-6}$	$0.270 \cdot 10^{-12}$	$0.3281 \cdot 10^{-5}$	$0.451 \cdot 10^{-12}$
Великобританія	$0.3930 \cdot 10^{-6}$	$0.362 \cdot 10^{-12}$	$0.4820 \cdot 10^{-5}$	$0.549 \cdot 10^{-12}$

Примітка: * - статистична значущість на рівні 0,9

На основі представлених в таблиці 2.26 регресійних коефіцієнтів можна зробити висновок, на скільки збільшиться/зменшиться рівень фінансової стабільності певної держави при збільшенні значення факторної ознаки (вартості та обсягів криптовалют BTC та ETH) на 1 одиницю. Наприклад, при збільшенні вартості криптовалюти BTC на 1 дол. Індекс фінансової стабільності Німеччини збільшиться на $0.2318 \cdot 10^{-6}$ частки одиниці.

З метою визначення на скільки відсотків зміниться результативна ознака при зміні факторної на 1% відносно середнього рівня розрахуємо на основі даних таблиці 2.26 коефіцієнти еластичності на основі формули (2.28):

$$EK = \frac{dy}{dx} \cdot \frac{\bar{x}}{\bar{y}} \quad (2.28)$$

де EK - коефіцієнт еластичності;

$\frac{dy}{dx}$ – похідна фунції y(x) за змінною x;

$\bar{x}, \bar{y}$ – середнє значення факторної та результативної ознак відповідно.

Оскільки для даного випадку $\frac{dy}{dx}$ буде дорівнювати регресійним коефіцієнтам (b_k), представленим в таблиці 2.27, формула (2.28) буде набувати наступного вигляду:

$$EK(b_k) = b_k \cdot \frac{\bar{x}}{\bar{y}} \tag{2.29}$$

Для обчислення коефіцієнта еластичності за формулою (2.27) виникає необхідність проведення проміжних розрахунків. Так, визначимо середні значення факторних ознак, тобто вартості та обсягів криптовалют BTC та ETH, а також результативної ознаки індексу фінансової стабільності держав та представимо їх в табличному вигляді (таблиця 2.27 та таблиця 2.28 відповідно).

Таблиця 2.27 – Середні значення вартості та обсягів криптовалют BTC та ETH за період з 2017-01-02 по 2022-06-06

Країни	BTC	Volume BTC	ETH	Volume ETH
Німеччина	17468,227	22774266314	1104,073067	13297186136
Фінляндія	17468,227	22774266314	1104,073067	13297186136
Франція	17468,227	22774266314	1104,073067	13297186136
Великобританія	17468,227	22774266314	1104,073067	13297186136

Таблиця 2.28 – Середні значення індексу фінансової стабільності держав за період з 2017 р. по 2022 р.

Країни	BTC	Volume BTC	ETH	Volume ETH
Німеччина	0,05228742	0,05228742	0,05228742	0,05228742
Фінляндія	0,034955477	0,034955477	0,034955477	0,034955477
Франція	0,040155972	0,040155972	0,040155972	0,040155972
Великобританія	0,071105654	0,071105654	0,071105654	0,071105654

Отже, підставляючи значення регресійних коефіцієнтів (таблиця 2.21) та середніх значень факторних та результативної ознак для Німеччини, Фінляндії, Франції, Великобританії (таблиці 2.27 та 2.28) у формулу (2.29)

обчислимо коефіцієнти еластичності впливу 1%-вої зміни фінансових активів на відсоткову зміну індексу фінансової стабільності держав (таблиця 2.29).

Таблиця 2.29 – Коефіцієнти еластичності впливу 1%-вої зміни фінансових активів на відсоткову зміну індексу фінансової стабільності держав

Країни	BTC	Volume BTC	ETH2	Volume ETH
Німеччина	0,07744	0,145041	0,065754	0,135801
Фінляндія	0,107142	0,163532	0,100409	0,159009
Франція	0,097616	0,153129	0,09021	0,149343
Великобританія	0,096547	0,115944	0,074841	0,102666

Таким чином, на основі даних таблиці 2.29 можна стверджувати, що при зростанні вартості криптовалюти BTC на 1% відносно середнього рівня, фінансова стабільність буде зростати на 0,077% для Німеччини, 0,107% для Фінляндії, 0,098% для Франції, 0,097% для Великобританії. Досить схожа тенденція характерна для криптовалюти ETH, для якої коефіцієнти еластичності набувають значень 0,069%, 0,100%, 0,090% та 0,075% відповідно. Зміна обсягів розглянутих криптовалют має більший за розмірами вплив на результативну ознаку. Так, в розрізі обсягів криптовалюти BTC коефіцієнт еластичності коливається в межах від 0,116% до 0,164%, а криптовалюти ETH – від 0,103% до 0,159%. Таким чином, справедливо зробити висновок, що на даний час криптовалюти не здійснюють суттєвого впливу на фінансову стійкість Європейських країн. Проте, зважаючи на активний розвиток криптовалют та щорічне проникнення у фінансові відносини, більш потужні відсоткові значення їх зростання призведуть й до зміни фінансових стабільності кожної країни.

Переходячи до дослідження впливу криптовалюти на показника фінансової стійкості України, зауважимо, що розширення результативних показників, наддасть змогу більш ґрунтовно дослідити вектори впливу цифрових активів на стійкість національної економіки. Отже, побудуємо поліноміальні моделі розподіленого лагу Алмона в розрізі впливу вартості та

обсягів криптовалют BTC та ETH на індекс фінансового стресу, субіндексів банківського сектору, поведінки домогосподарств, валютного ринку для України.

Таблиця 2.30 – Фрагмент поліноміальної моделі розподіленого лагу Алмона в розрізі впливу вартості криптовалюти BTC на індекс фінансового стресу для України

Lag	Almon Polyn. Distr.Lags; Regression Coefficients (Spreadsheet22 Україна.sta) Indep: BTC Dep: IFC Lag: 6 Polyn. order: 1 R=,5869 R-square=,3444 N: 1011			
	RegressnCoeff.	StandardError	T(1004)	P
0	0,000000599819	0,000000204774	2,92918130078	0,003475406323
1	0,000000442277	0,000000136399	3,24253450184	0,001223738064
2	0,000000284735	0,000000068101	4,18107756587	0,000031545542
3	0,000000127192	0,000000005633	22,57942033337	0,000000000000
4	-0,000000030350	0,000000069185	-0,43867622658	0,660990540801
5	-0,000000187892	0,000000137486	-1,36663041674	0,172047110165
6	-0,000000345434	0,000000205861	-1,67799540797	0,093659191837

На основі застосування статистично значущих лагів та регресійних коефіцієнтів (таблиця 2.30) поліноміальна моделі розподіленого лагу Алмона в розрізі впливу вартості криптовалюти BTC на індекс фінансового стресу для України набуває вигляду:

$$IFC(t) = 0.1272 \cdot 10^{-6} \cdot BTC\_USD(t-3) + 0.2847 \cdot 10^{-6} \cdot BTC\_USD(t-2) + 0.4423 \cdot 10^{-6} \cdot BTC\_USD(t-1) + 0.5998 \cdot 10^{-6} \cdot BTC\_USD(t) \quad (2.30)$$

де $IFC(t)$ – індекс фінансового стресу для України в момент часу t;

$BTC\_USD(t-m)$ – значення вартості криптовалюти в момент часу $t-m$.

На основі застосування статистично значущих лагів та регресійних коефіцієнтів (таблиця 2.31) поліноміальна моделі розподіленого лагу Алмона в розрізі впливу обсягів криптовалюти BTC на індекс фінансового стресу для України набуває вигляду:

$$IFC(t) = 0.110 \cdot 10^{-12} \cdot VBTC(t-2) + 0.106 \cdot 10^{-12} \cdot VBTC(t-3) + 0.102 \cdot 10^{-12} \cdot VBTC(t-4) + 0.114 \cdot 10^{-12} \cdot VBTC(t-1) + 0.098 \cdot 10^{-12} \cdot VBTC(t-5) + 0.118 \cdot 10^{-12} \cdot VBTC(t) + 0.095 \cdot 10^{-12} \cdot VBTC(t-6) \quad (2.31)$$

де $VBTC(t-m)$ – значення обсягів криптовалюти BTC в момент часу $t-m$.

Таблиця 2.31 – Фрагмент поліноміальної моделі розподіленого лагу Алмона в розрізі впливу обсягів криптовалюти BTC на індекс фінансового стресу для України

Lag	Almon Polyn. Distr.Lags; Regression Coefficients (Spreadsheet22 Україна.sta) Indep: Volume BTC Dep: IFC Lag: 6 Polyn. order: 1 R=,6433 R-square=,4138 N: 1011			
	Regressn Coeff.	StandardError	T(1004)	P
0	0,000000000000118	0,000000000000	2,82696815574	0,004792426336
1	0,000000000000114	0,000000000000	4,07836912992	0,000048943038
2	0,000000000000110	0,000000000000	7,65548116885	0,000000000000
3	0,000000000000106	0,000000000000	26,68288017469	0,000000000000
4	0,000000000000102	0,000000000000	7,08767776226	0,000000000003
5	0,000000000000098	0,000000000000	3,51367732805	0,000461648367
6	0,000000000000095	0,000000000000	2,26308942475	0,023843055243

Таблиця 2.32 – Фрагмент поліноміальної моделі розподіленого лагу Алмона в розрізі впливу вартості криптовалюти ETH на індекс фінансового стресу для України

Lag	Almon Polyn. Distr.Lags; Regression Coefficients (Spreadsheet22 Україна.sta) Indep: ETH2 Dep: IFC Lag: 6 Polyn. order: 1 R=,5123 R-square=,2624 N: 1011			
	Regressn Coeff.	StandardError	T(1004)	P
0	0,000004257994	0,000001975916	2,15494646051	0,031403242615
1	0,000003484212	0,000001317125	2,64531540091	0,008288980243
2	0,000002710430	0,000000661020	4,10037585287	0,000044582918
3	0,000001936648	0,000000103100	18,78414930611	0,000000000000
4	0,000001162866	0,000000675179	1,72230951578	0,085321400031
5	0,000000389085	0,000001331411	0,29223467026	0,770167588863
6	-0,000000384697	0,000001990226	-0,19329319320	0,846768444087

На основі застосування статистично значущих лагів та регресійних коефіцієнтів (таблиця 2.32) поліноміальна моделі розподіленого лагу Алмона

в розрізі впливу вартості криптовалюти ETH на індекс фінансового стресу для України набуває вигляду:

$$IFC(t) = 0.1937 \cdot 10^{-5} \cdot ETH\_USD(t-3) + 0.2710 \cdot 10^{-5} \cdot ETH\_USD(t-2) + 0.3484 \cdot 10^{-5} \cdot ETH\_USD(t-1) + 0.4258 \cdot 10^{-5} \cdot ETH\_USD(t) \quad (2.32)$$

де $ETH\_USD(t-m)$ – значення вартості криптовалюти ETH в момент часу $t-m$.

Таблиця 2.33 – Фрагмент поліноміальної моделі розподіленого лагу Алмона в розрізі впливу обсягів криптовалюти ETH на індекс фінансового стресу для України

Lag	Almon Polyn. Distr.Lags; Regression Coefficients (Spreadsheet22 Україна.sta) Indep: Volume ETH Dep: IFC Lag: 6 Polyn. order: 1 R=,6015 R-square=,3618 N: 1011			
	RegressnCoeff.	StandardError	T(1004)	P
0	0,000000000000220	0,000000000000	2,13156246900	0,033285137000
1	0,000000000000211	0,000000000000	3,05142984404	0,002337401417
2	0,000000000000201	0,000000000000	5,72664811518	0,000000013526
3	0,000000000000192	0,000000000000	23,90870925655	0,000000000000
4	0,000000000000183	0,000000000000	5,15572461252	0,000000304230
5	0,000000000000173	0,000000000000	2,49853790683	0,012629606292
6	0,000000000000164	0,000000000000	1,58232884473	0,113889455017

На основі застосування статистично значущих лагів та регресійних коефіцієнтів (таблиця 2.33) поліноміальна моделі розподіленого лагу Алмона в розрізі впливу обсягів криптовалюти ETH на індекс фінансового стресу для України набуває вигляду:

$$IFC(t) = 0.192 \cdot 10^{-12} \cdot VETH(t-3) + 0.201 \cdot 10^{-12} \cdot VETH(t-2) + 0.183 \cdot 10^{-12} \cdot VETH(t-4) + 0.211 \cdot 10^{-12} \cdot VETH(t-1) + 0.173 \cdot 10^{-12} \cdot VETH(t-5) + 0.220 \cdot 10^{-12} \cdot VETH(t) \quad (2.33)$$

де $VETH(t-m)$ – значення обсягів криптовалюти ETH в момент часу $t-m$.

Таблиця 2.34 – Фрагмент поліноміальної моделі розподіленого лагу Алмона в розрізі впливу вартості криптовалюти BTC на субіндекс банківського сектору для України

Lag	Almon Polyn. Distr.Lags; Regression Coefficients (Spreadsheet22 Україна.sta) Indep: BTC Dep: CBC Lag: 2 Polyn. order: 1 R=,4577 R-square=,2095 N: 1015			
	Regressn Coeff.	Standard Error	T(1012)	P
0	0,000000072585	0,000000236909	0,30638241863	0,759376509062
1	0,000000086023	0,000000005256	16,36582857819	0,000000000000
2	0,000000099462	0,000000237468	0,41884316704	0,675419631035

На основі застосування статистично значущих лагів та регресійних коефіцієнтів (таблиця 2.34) поліноміальна моделі розподіленого лагу Алмона в розрізі впливу вартості криптовалюти BTC на субіндекс банківського сектору для України набуває вигляду:

$$CBC(t) = 0.8602 \cdot 10^{-7} \cdot BTC\_USD(t-1) \qquad (2.34)$$

де $CBC(t)$ – субіндекс банківського сектору для України в момент часу t;
$BTC\_USD(t-m)$ – значення вартості криптовалюти BTC в момент часу $t-m$.

Таблиця 2.35 – Фрагмент поліноміальної моделі розподіленого лагу Алмона в розрізі впливу обсягів криптовалюти BTC на субіндекс банківського сектору для України

Lag	Almon Polyn. Distr.Lags; Regression Coefficients (Spreadsheet22 Україна.sta) Indep: Volume BTC Dep: CBC Lag: 2 Polyn. order: 1 R=,5193 R-square=,2697 N: 1015			
	Regressn Coeff.	Standard Error	T(1012)	P
0	0,000000000000072	0,000000000000	3,03979067361	0,002428287102
1	0,000000000000073	0,000000000000	19,33993815200	0,000000000000
2	0,000000000000073	0,000000000000	3,08592798619	0,002084332170

На основі застосування статистично значущих лагів та регресійних коефіцієнтів (таблиця 2.35) поліноміальна моделі розподіленого лагу Алмона

в розрізі впливу обсягів криптовалюти BTC на субіндекс банківського сектору для України набуває вигляду:

$$CBC(t) = 0.073 \cdot 10^{-12} \cdot VBTC(t-1) + 0.073 \cdot 10^{-12} \cdot VBTC(t-2) + 0.072 \cdot 10^{-12} \cdot VBTC(t) \quad (2.35)$$

де $CBC(t)$ – субіндекс банківського сектору для України в момент часу t;
$VBTC(t-m)$ – значення обсягів криптовалюти BTC в момент часу $t-m$.

Таблиця 2.36 – Фрагмент поліноміальної моделі розподіленого лагу Алмона в розрізі впливу вартості криптовалюти ETH на субіндекс банківського сектору для України

Lag	Almon Polyn. Distr.Lags; Regression Coefficients (Spreadsheet22 Україна.sta) Indep: ETH Dep: CBC Lag: 2 Polyn. order: 1 R=,3844 R-square=,1478 N: 1015			
	Regressn Coeff.	Standard Error	T(1012)	P
0	0,000001438028	0,000001298394	1,10754352126	0,268322176767
1	0,000001237380	0,000000093509	13,23269487874	0,000000000000
2	0,000001036733	0,000001285815	0,80628440712	0,420268282674

На основі застосування статистично значущих лагів та регресійних коефіцієнтів (таблиця 2.36) поліноміальна моделі розподіленого лагу Алмона в розрізі впливу вартості криптовалюти ETH на субіндекс банківського сектору для України набуває вигляду:

$$CBC(t) = 0.1237 \cdot 10^{-5} \cdot ETH\_USD(t-1) \quad (2.36)$$

де $CBC(t)$ – субіндекс банківського сектору для України в момент часу t;
$ETH\_USD(t-m)$ – значення вартості криптовалюти ETH в момент часу $t-m$.

Таблиця 2.37 – Фрагмент поліноміальної моделі розподіленого лагу Алмона в розрізі впливу обсягів криптовалюти ETH на субіндекс банківського сектору для України

Lag	Almon Polyn. Distr.Lags; Regression Coefficients (Spreadsheet22 Україна.sta) Indep: Volume ETH Dep: CBC Lag: 2 Polyn. order: 1 R=,4686 R-square=,2196 N: 1015			
	Regressn Coeff.	Standard Error	T(1012)	P
0	0,000000000000122	0,000000000000	1,62207946885	0,105097783700
1	0,000000000000127	0,000000000000	16,88488732333	0,000000000000
2	0,000000000000132	0,000000000000	1,74850312334	0,080680127302

На основі застосування статистично значущих лагів та регресійних коефіцієнтів (таблиця 2.37) поліноміальна моделі розподіленого лагу Алмона в розрізі впливу обсягів криптовалюти ETH на субіндекс банківського сектору для України набуває вигляду:

$$CBC(t) = 0.127 \cdot 10^{-12} \cdot VETH(t-1) \qquad (2.37)$$

де $CBC(t)$ – субіндекс банківського сектору для України в момент часу t;
$VETH(t-m)$ – значення обсягів криптовалюти ETH в момент часу $t-m$.

Таблиця 2.38 – Фрагмент поліноміальної моделі розподіленого лагу Алмона в розрізі впливу вартості криптовалюти BTC на субіндекс поведінки домогосподарств для України

Lag	Almon Polyn. Distr.Lags; Regression Coefficients (Spreadsheet22 Україна.sta) Indep: BTC Dep: CPD Lag: 5 Polyn. order: 1 R=,5681 R-square=,3228 N: 1012			
	Regressn Coeff.	Standard Error	T(1006)	P
0	0,000000051938	0,000000108298	0,479588788885	0,631624069153
1	0,000000055704	0,000000064919	0,858055356905	0,391066272256
2	0,000000059470	0,000000021638	2,748471109264	0,006094538969
3	0,000000063236	0,000000022124	2,858257409740	0,004347632901
4	0,000000067002	0,000000065409	1,024347324945	0,305917517259
5	0,000000070768	0,000000108788	0,650507852364	0,515512780657

На основі застосування статистично значущих лагів та регресійних коефіцієнтів (таблиця 2.38) поліноміальна моделі розподіленого лагу Алмона в розрізі впливу вартості криптовалюти BTC на субіндекс поведінки домогосподарств для України набуває вигляду:

$$CPD(t) = 0.5947 \cdot 10^{-7} \cdot BTC\_USD(t-2) + 0.6324 \cdot 10^{-7} \cdot BTC\_USD(t-3) \quad (2.38)$$

де $CPD(t)$ – субіндекс поведінки домогосподарств для України в момент часу t;

$BTC\_USD(t-m)$ – значення вартості криптовалюти BTC в момент часу $t-m$.

Таблиця 2.39 – Фрагмент поліноміальної моделі розподіленого лагу Алмона в розрізі впливу обсягів криптовалюти BTC на субіндекс поведінки домогосподарств для України

Lag	Almon Polyn. Distr.Lags; Regression Coefficients (Spreadsheet22 Україна.sta) Indep: Volume BTC Dep: CPD Lag: 5 Polyn. order: 1 R=,6385 R-square=,4077 N: 1012			
	Regressn Coeff.	Standard Error	T(1006)	P
0	0,000000000000048	0,000000000000	2,42952481650	0,015292796269
1	0,000000000000049	0,000000000000	4,14787936022	0,000036389724
2	0,000000000000051	0,000000000000	11,65475966320	0,000000000000
3	0,000000000000053	0,000000000000	11,96614637366	0,000000000000
4	0,000000000000054	0,000000000000	4,53820891694	0,000006358146
5	0,000000000000056	0,000000000000	2,82796662271	0,004777438485

На основі застосування статистично значущих лагів та регресійних коефіцієнтів (таблиця 2.39) поліноміальна моделі розподіленого лагу Алмона в розрізі впливу обсягів криптовалюти BTC на субіндекс поведінки домогосподарств для України набуває вигляду:

$$CPD(t) = 0.051 \cdot 10^{-12} \cdot VBTC(t-2) + 0.053 \cdot 10^{-12} \cdot VBTC(t-3) + 0.054 \cdot 10^{-12} \cdot VBTC(t-4) + 0.049 \cdot 10^{-12} \cdot VBTC(t-1) + 0.056 \cdot 10^{-12} \cdot VBTC(t-5) + 0.048 \cdot 10^{-12} \cdot VBTC(t) \quad (2.39)$$

де $CBC(t)$ – субіндекс поведінки домогосподарств для України в момент часу t;

$VBTC(t-m)$ – значення обсягів криптовалюти BTC в момент часу $t-m$.

Таблиця 2.40 – Фрагмент поліноміальної моделі розподіленого лагу Алмона в розрізі впливу вартості криптовалюти ETH на субіндекс поведінки домогосподарств для України

Lag	Almon Polyn. Distr.Lags; Regression Coefficients (Spreadsheet22 Україна.sta) Indep: ETH2 Dep: CPD Lag: 5 Polyn. order: 1 R=,4855 R-square=,2357 N: 1012			
	Regressn Coeff.	Standard Error	T(1006)	p
0	0,000000553999	0,000000930716	0,595239542229	0,551817236716
1	0,000000694588	0,000000559112	1,242306602159	0,214412983548
2	0,000000835177	0,000000191211	4,367828495822	0,000013848347
3	0,000000975766	0,000000195192	4,999003600517	0,000000679484
4	0,000001116355	0,000000563223	1,982082160598	0,047741820704
5	0,000001256944	0,000000934839	1,344557039421	0,179071428023

На основі застосування статистично значущих лагів та регресійних коефіцієнтів (таблиця 2.40) поліноміальна моделі розподіленого лагу Алмона в розрізі впливу вартості криптовалюти ETH на субіндекс поведінки домогосподарств для України набуває вигляду:

$$CPD(t) = 0.9758 \cdot 10^{-6} \cdot ETH\_USD(t-3) + 0.8352 \cdot 10^{-6} \cdot ETH\_USD(t-2) + 0.1116 \cdot 10^{-6} \cdot ETH\_USD(t-4) \quad (2.40)$$

де $CPD(t)$ – субіндекс поведінки домогосподарств для України в момент часу t;

$ETH\_USD(t-m)$ – значення вартості криптовалюти ETH в момент часу $t-m$.

Таблиця 2.41 – Фрагмент поліноміальної моделі розподіленого лагу Алмона в розрізі впливу обсягів криптовалюти ETH на субіндекс поведінки домогосподарств для України

Lag	Almon Polyn. Distr.Lags; Regression Coefficients (Spreadsheet22 Україна.sta) Indep: Volume ETH Dep: CPD Lag: 5 Polyn. order: 1 R=,5848 R-square=,3420 N: 1012			
	Regressn Coeff.	Standard Error	T(1006)	P
0	0,000000000000074	0,000000000000	1,461578635611	0,144169012416
1	0,000000000000081	0,000000000000	2,652990719061	0,008103895161
2	0,000000000000088	0,000000000000	8,132923043972	0,000000000000
3	0,000000000000095	0,000000000000	8,699335149597	0,000000000000
4	0,000000000000102	0,000000000000	3,327691892705	0,000907408388
5	0,000000000000109	0,000000000000	2,146542192230	0,032068327125

На основі застосування статистично значущих лагів та регресійних коефіцієнтів (таблиця 2.41) поліноміальна моделі розподіленого лагу Алмона в розрізі впливу обсягів криптовалюти ETH на субіндекс поведінки домогосподарств для України набуває вигляду:

$$CPD(t) = 0.088 \cdot 10^{-12} \cdot VETH(t-2) + 0.095 \cdot 10^{-12} \cdot VETH(t-3) + 0.102 \cdot 10^{-12} \cdot VETH(t-4) + 0.081 \cdot 10^{-12} \cdot VETH(t-1) + 0.109 \cdot 10^{-12} \cdot VETH(t-5) \quad (2.41)$$

де $CPD(t)$ – субіндекс поведінки домогосподарств для України в момент часу t;

$VETH(t-m)$ – значення обсягів криптовалюти ETH в момент часу $t-m$.

Таблиця 2.42 – Фрагмент поліноміальної моделі розподіленого лагу Алмона в розрізі впливу вартості криптовалюти BTC на субіндекс валютного ринку для України

Lag	Almon Polyn. Distr.Lags; Regression Coefficients (Spreadsheet22 Україна.sta) Indep: BTC Dep: CVR Lag: 2 Polyn. order: 1 R=,5811 R-square=,3377 N: 1015			
	Regressn Coeff.	Standard Error	T(1012)	P
0	0,000000174212	0,000000319296	0,54561328652	0,585452018802
1	0,000000160754	0,000000007084	22,69203474870	0,000000000000
2	0,000000147297	0,000000320049	0,46023216963	0,645448454732

На основі застосування статистично значущих лагів та регресійних коефіцієнтів (таблиця 2.42) поліноміальна моделі розподіленого лагу Алмона в розрізі впливу вартості криптовалюти BTC на субіндекс валютного ринку для України набуває вигляду:

$$CVR(t) = 0.1608 \cdot 10^{-6} \cdot BTC\_USD(t-1) \qquad (2.42)$$

де $CVR(t)$ – субіндекс валютного ринку для України в момент часу t;
$BTC\_USD(t-m)$ – значення вартості криптовалюти BTC в момент часу $t-m$.

Таблиця 2.43 – Фрагмент поліноміальної моделі розподіленого лагу Алмона в розрізі впливу обсягів криптовалюти BTC на субіндекс валютного ринку для України

Lag	Almon Polyn. Distr.Lags; Regression Coefficients (Spreadsheet22 Україна.sta) Indep: Volume BTC Dep: CVR Lag: 2 Polyn. order: 1 R=,6765 R-square=,4576 N: 1015			
	Regressn Coeff.	Standard Error	T(1012)	P
0	0,000000000000139	0,000000000000	4,61649144212	0,000004404357
1	0,000000000000139	0,000000000000	29,23669630929	0,000000000000
2	0,000000000000140	0,000000000000	4,64393056915	0,000003868367

На основі застосування статистично значущих лагів та регресійних коефіцієнтів (таблиця 2.43) поліноміальна моделі розподіленого лагу Алмона

в розрізі впливу обсягів криптовалюти BTC на субіндекс валютного ринку для України набуває вигляду:

$$CVR(t) = 0.139 \cdot 10^{-12} \cdot VBTC(t-1) + 0.140 \cdot 10^{-12} \cdot VBTC(t-2) + 0.139 \cdot 10^{-12} \cdot VBTC(t) \quad (2.43)$$

де $CVR(t)$ – субіндекс валютного ринку для України в момент часу t;
$VBTC(t-m)$ – значення обсягів криптовалюти BTC в момент часу $t-m$.

Таблиця 2.44 – Фрагмент поліноміальної моделі розподіленого лагу Алмона в розрізі впливу вартості криптовалюти ETH на субіндекс валютного ринку для України

Lag	Almon Polyn. Distr.Lags; Regression Coefficients (Spreadsheet22 Україна.sta) Indep: ETH2 Dep: CVR Lag: 2 Polyn. order: 1 R=,4910 R-square=,2411 N: 1015			
	Regressn Coeff.	Standard Error	T(1012)	P
0	0,000003357544	0,000001804028	1,86113764451	0,063014532294
1	0,000002329394	0,000000129925	17,92880879638	0,000000000000
2	0,000001301245	0,000001786550	0,72835616577	0,466564085734

На основі застосування статистично значущих лагів та регресійних коефіцієнтів (таблиця 2.44) поліноміальна моделі розподіленого лагу Алмона в розрізі впливу вартості криптовалюти ETH на субіндекс валютного ринку для України набуває вигляду:

$$CVR(t) = 0.2329 \cdot 10^{-5} \cdot ETH\_USD(t-1) \quad (2.44)$$

де $CPD(t)$ – субіндекс валютного ринку для України в момент часу t;
$ETH\_USD(t-m)$ – значення вартості криптовалюти ETH в момент часу $t-m$.

Таблиця 2.45 – Фрагмент поліноміальної моделі розподіленого лагу Алмона в розрізі впливу обсягів криптовалюти ETH на субіндекс валютного ринку для України

Lag	Almon Polyn. Distr.Lags; Regression Coefficients (Spreadsheet22 Україна.sta) Indep: Volume ETH Dep: CVR Lag: 2 Polyn. order: 1 R=,6201 R-square=,3845 N: 1015			
	Regressn Coeff.	Standard Error	T(1012)	P
0	0,000000000000243	0,000000000000	2,45870390980	0,014110505414
1	0,000000000000248	0,000000000000	25,15596225717	0,000000000000
2	0,000000000000253	0,000000000000	2,56301845244	0,010520282864

На основі застосування статистично значущих лагів та регресійних коефіцієнтів (таблиця 2.45) поліноміальна моделі розподіленого лагу Алмона в розрізі впливу обсягів криптовалюти ETH на субіндекс валютного ринку для України набуває вигляду:

$$CVR(t) = 0.248 \cdot 10^{-12} \cdot VETH(t-1) + 0.253 \cdot 10^{-12} \cdot VETH(t-2) + 0.243 \cdot 10^{-12} \cdot VETH(t) \quad (2.45)$$

де $CVR(t)$ – субіндекс валютного ринку для України в момент часу t;
$VETH(t-m)$ – значення обсягів криптовалюти ETH в момент часу $t-m$.

Систематизуємо максимальні ідентифіковані та записані за допомогою моделей розподіленого лагу Алмона затримки впливу криптовалют на складові фінансової стабільності України (таблиця 2.46).

На основі аналізу таблиці 2.46 можна зробити висновок про варіацію лагів впливу криптовалют на фінансову стабільність України від 1 до 6 днів. Триваліші лаги затримки спостерігаються в розрізі обсягів криптовалют BTC та ETH в розрізі індексу фінансового стресу для України та субіндексу поведінки домогосподарств. Для України спостерігається прямий зв’язок впливу на фінансову стабільність всіх факторних ознак.

Таблиця 2.46 – Максимальні статистично значущі величини лагів впливу криптовалют на індекс фінансового стресу, субіндекси банківського сектору, поведінки домогосподарств та валютного ринку України

Показник	BTC	Volume BTC	ETH	Volume ETH
Індекс фінансового стресу	3+	6+	3+	5+
Субіндекс банківського сектору	1+	2+	1+	1+
Субіндекс поведінки домогосподарств	3+	5+	4+	4+
Субіндекс валютного ринку	1+	2+	1+	2+

Визначивши величини лагової затримки впливу криптовалют на фінансову стабільність України, виникає необхідність кількісного оцінювання обсягу даного впливу, що пропонується провести на основі регресійних коефіцієнтів поліноміальної моделі розподіленого лагу Алмона (таблиця 2.47).

Таблиця 2.47 – Регресійні коефіцієнти поліноміальної моделі розподіленого лагу Алмона при максимальній статистично значущій величині лагу впливу криптовалютна фінансову стабільність України

Показник	BTC	Volume BTC	ETH	Volume ETH
Індекс фінансового стресу	$0.1272 \cdot 10^{-6}$	$0.110 \cdot 10^{-12}$	$0.1937 \cdot 10^{-5}$	$0.192 \cdot 10^{-12}$
Субіндекс банківського сектору	$0.8602 \cdot 10^{-7}$	$0.073 \cdot 10^{-12}$	$0.1237 \cdot 10^{-5}$	$0.127 \cdot 10^{-12}$
Субіндекс поведінки домогосподарств	$0.5947 \cdot 10^{-7}$	$0.051 \cdot 10^{-12}$	$0.9758 \cdot 10^{-6}$	$0.088 \cdot 10^{-12}$
Субіндекс валютного ринку	$0.1608 \cdot 10^{-6}$	$0.139 \cdot 10^{-12}$	$0.2329 \cdot 10^{-5}$	$0.248 \cdot 10^{-12}$

На основі представлених в таблиці 2.47 регресійних коефіцієнтів можна зробити висновок, на скільки збільшиться/зменшиться рівень фінансової стабільності певної держави при збільшенні значення факторної ознаки (вартості та обсягів криптовалют BTC та ETH) на 1 одиницю. Наприклад, при збільшенні вартості криптовалюти BTC на 1 дол. індекс фінансового стресу для України збільшиться на $0.1272 \cdot 10^{-6}$ частки одиниці.

З метою визначення на скільки відсотків зміниться результативна ознака при зміні факторної на 1% відносно середнього рівня розрахуємо на основі даних таблиці 2.47 коефіцієнти еластичності на основі формули (2.29).

Для обчислення коефіцієнта еластичності за формулою (2.29) виникає необхідність проведення проміжних розрахунків. Так, визначимо середні значення факторних ознак, тобто вартості та обсягів криптовалют BTC та ETH, а також результативних ознак Індекс фінансового стресу для України, субіндекс банківського сектору, субіндекс поведінки домогосподарств, субіндекс валютного ринку для України та представимо їх в табличному вигляді (таблиця 2.48 та таблиця 2.49 відповідно).

Таблиця 2.48 – Середні значення факторних ознак

Показники	BTC	Volume BTC	ETH	Volume ETH
Індекс фінансового стресу	17817,81964	26166817737	900,9744686	12708826131
Субіндекс банківського сектору	17817,81964	26166817737	900,9744686	12708826131
Субіндекс поведінки домогосподарств	17817,81964	26166817737	900,9744686	12708826131
Субіндекс валютного ринку	17817,81964	26166817737	900,9744686	12708826131

Таблиця 2.49 – Середні значення результативних ознак

Показники	BTC	Volume BTC	ETH	Volume ETH
Індекс фінансового стресу	0,029661278	0,029661278	0,029661278	0,029661278
Субіндекс банківського сектору	0,011826018	0,011826018	0,011826018	0,011826018
Субіндекс поведінки домогосподарств	0,014920924	0,014920924	0,014920924	0,014920924
Субіндекс валютного ринку	0,018794503	0,018794503	0,018794503	0,018794503

Отже, підставляючи значення регресійних коефіцієнтів (таблиця 2.47) та середніх значень факторних та результативної ознак для України (таблиці 2.48 та 2.49) у формулу (2.29) обчислимо коефіцієнти еластичності вливу 1%-вої зміни фінансових активів на відсоткову зміну індексу фінансової стабільності держав (таблиця 2.50).

Таблиця 2.50 – Значення коефіцієнтів еластичності

Показники	BTC	Volume BTC	ETH	Volume ETH
Індекс фінансового стресу	0,07641	0,097041	0,058837	0,082265
Субіндекс банківського сектору	0,129603	0,161523	0,094242	0,136481
Субіндекс поведінки домогосподарств	0,071016	0,089439	0,058922	0,074954
Субіндекс валютного ринку	0,152444	0,193524	0,111648	0,167697

Таким чином, на основі даних таблиці 2.50 можна стверджувати, що при зростанні вартості криптовалюти BTC на 1% відносно середнього рівня, індекс фінансового стресу для України зросте на 0,076%, субіндекс банківського сектору на 0,130%, субіндекс поведінки домогосподарств на 0,071%, субіндекс валютного ринку на 0,152%. Досить схожа тенденція характерна для криптовалюти ETH, для якої коефіцієнти еластичності набувають значень 0,082%, 0,136%, 0,075% та 0,168% відповідно. Зміна обсягів розглянутих криптовалют має більший за розмірами вплив на результативні ознаки. Так, в розрізі обсягів криптовалюти BTC коефіцієнт еластичності коливається в межах від 0,089% до 0,194%, а криптовалюти ETH – від 0,075% до 0,168%.

Підводячи підсумок справедливо зазначити, що існуючий рівень розвитку криптовалют не здійснює суттєвого впливу а фінансову стабільність країн світу. Безумовно впливу вартості та обсягу криптовалют на складові фінансового стабільності є, проте наразі він складає не більше 0,25% при зміні факторних показників на 1%.

3 МЕТОДИЧНІ ЗАСАДИ ПРОТИДІЇ КІБЕРШАХРАЙСТВАМ В УМОВАХ ЦИРОВІЗАЦІЇ ФІНАНСОВОГО СЕКТОРУ

3.1. **Оцінка ефективності протидії використання послуг та/або інфраструктури фінансових посередників для легалізації кримінальних доходів та здійснення кібершахрайств**

Стрімкий розвиток інформаційних технологій зумовлює адаптивну трансформацію всіх сфер людської діяльності. За останні двадцять років докорінні зміни відбулись в сфері продаж, так питома вага он-лайн продаж перевищила реальні продажі (RetailTech). Суттєво змінилась й сфера освіти. ІТ-технології дозволили не тільки проводити дистанційні зайняття, але й симулювати буд які технічні чи біологічні процеси (EdTech). Не залишилися осторонь й фінансові послуги. Так в банківській сфері ІТ технології змінили швидкість проведення транзакцій, підвищили рівень доступності клієнтів до банківських послуг, розширили спектр банківських послуг та інше.

Проте поряд з позитивними зрушеннями в фінансовій сфері ІТ технологій активізували процеси легалізації кримінальних доходів, пришвидшили час їх реалізації та ускладнили процес їх викриття й моніторингу. За 4 квартал 2019 року банківськими установами було передано до Державної служби фінансового моніторингу понад 3 мільйони повідомлень про операції, які підлягають обов’язковому фінансовому моніторингу.

Таким чином, актуальності набуває дослідження рівня ефективності системи протидії легалізації кримінальних доходів та результативних факторів, які на це впливають.

Розглядаючи ефективність системи протидії легалізації кримінальних доходів у контексті діджиталізації банківської діяльності зупинимось, в першу чергу, на безпосередньому понятті «ефективність». Так, в економіці цю категорію розглядають з різних точок зору: як перевищення доходів над витратами, як абсолютна економія, як приріст прибутку чи як зниження собівартості. Авторами статті запропоновано розглядати ефективність, як

характеристику об’єкта, що відображає його здатність приносити корисність, тобто позитивну зміну певних параметрів досліджуваного об’єкта [110**Ошибка! Источник ссылки не найден.**].

Базуючись на даному твердженні, математичну формалізацію процесу оцінювання рівня ефективності системи протидії легалізації кримінальних доходів в банку доцільно розглядати з точки зору теорії корисності.

Відповідно до класичного підходу, корисність – це задоволення, або ж ефект, який клієнт отримує від споживання набору товарів чи послуг. Коли мова йде про корисність, розуміється що є декілька альтернативних варіантів наборів благ, які мають різну цінність для споживача. Попарне їх порівняння формується у вигляді кривої байдужості [111**Ошибка! Источник ссылки не найден.**].

Використання зазначеного підходу для аналізу ефективності системи протидії легалізації кримінальних доходів вимагає виділення наступних концептів.

Споживачем у даному випадку виступає система протидії легалізації доходів, отриманих незаконним шляхом. Система, прагнучі до максимальної ефективності, обирає один з двох альтернативних шляхів свого розвитку: розвиток механізмів та типологій ідентифікації операцій, як таких що підлягають обов’язковому фінансовому моніторингу чи обширне впровадження інформаційних технологій як і у банківське обслуговування, так і у всю систему протидії.

Для економіко-математичної формалізації функції корисності пропонується результативною ознакою обрати частку направлених до суду обвинувальних актів у загальній кількості кримінальних правопорушень, за якими проводилось досудове розслідування у відповідний період. Саме цей параметр дозволяє оцінити рівень превентивних заходів, які в майбутньому повинні зменшити кількість фінансових шахрайства. Динаміка результативної ознаки відображена на рисунку 3.1.

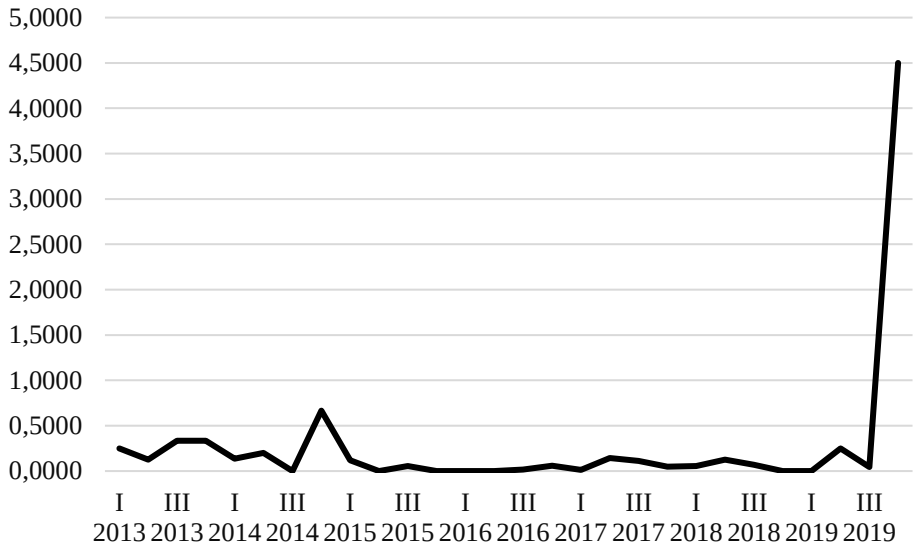


Рисунок 3.1 – Частка направлених до суду обвинувальних актів у загальній кількості кримінальних правопорушень, за якими проводилось досудове розслідування у відповідний період

Джерело: Складено авторами на основі [112]

На основі даних рисунку 3.1 зауважимо, що тільки у 4 кварталі 2019 року було значне перевищення кількості направлених до суду обвинувальних актів в порівнянні з кількістю правопорушень, за якими проводилось розслідування. За весь досліджуваний період даний показник не перевищував 0,5 одиниць. В середньому ж, частка обвинувальних актів склала 0,27 од., а медіанна частка обвинувальних актів була на рівні 0,06 од. Досліджені дані свідчать про низький рівень розслідування кримінальних правопорушень. Причини цього явища можуть бути різні: від некомпетентності слідчих до системних недоліків досудового розслідування.

Характеристикою першої альтернативи виступає частка кримінальних правопорушень, по яким проводилось досудове розслідування, яка припадає на одне повідомлення про операцію, що було передане до Державної служби фінансового моніторингу (рисунок 3.2). Значення цього показника протягом досліджуваного періоду часу мало флуктаційний характер. В середньому, на 10000 повідомлень про операції припадало 2,56 од. підтверджених кримінальних правопорушень та 1,73 од. у медіанному вимірі. Низькі значення

цього показника свідчать про або неспроможність довести що підозріла операція мала ознаки кримінального правопорушення, або ж про те що більшість операцій були законними і не були направлені на легалізацію кримінальних доходів. Аналізуючи даний показник, можна зробити висновок, що ефективність використання ресурсів системи протидії легалізації кримінальних доходів у даному випадку не є очевидною

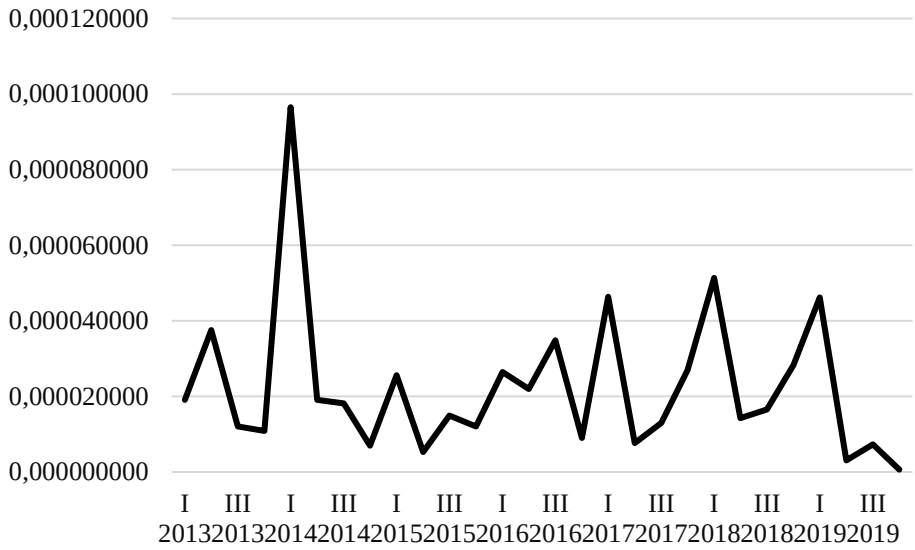


Рисунок 3.2 – Частка кримінальних правопорушень по яких проводилось досудове розслідування, яка припадає на одне повідомлення про операцію, що було передане до Державної служби фінансового моніторингу

Джерело: складено авторами на основі [113]

Характеристикою другої альтернативи є показник діджиталізації економіки, який є відношенням кількості абонентів мережі інтернет до чисельності населення (рисунок 3.3). Значення даного показника свідчать що починаючи із кінця 2015 року зростає кількість активних користувачів інтернет мережі. На кінець 2019 року кількість абонентів мережі інтернет складала понад 28 млн осіб. В повній мірі можемо вважати, що користувачі мережі інтернет оплачують послуги провайдера для доступу до онлайн сервісів, в тому числі і банківських. Все більше зростає цифрова обізнаність населення.

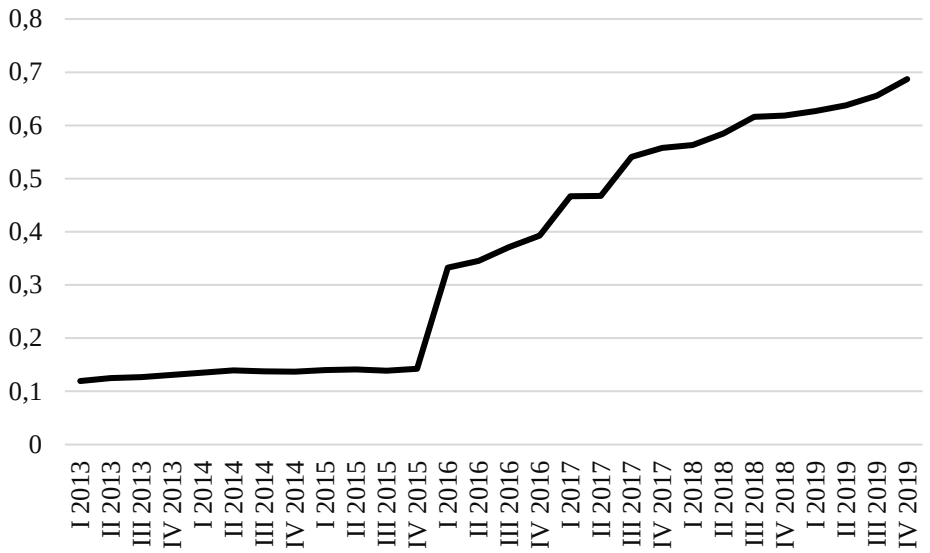


Рисунок 3.3 – Динаміка діджиталізації економіки

Для специфікації функції залежності результативної ознаки від факторних, побудуємо корелограму нульових різниць (рисунок 3.4) та таблицю автокореляційної функції (рисунок 3.5).

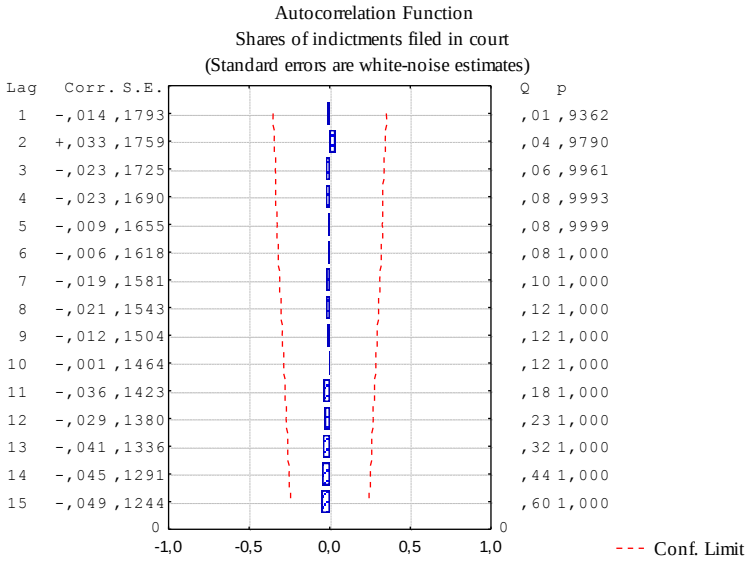


Рисунок 3.4 – Корелограма нульових різниць Частки направлених до суду обвинувальних актів

Lag	Autocorrelation Function (Spreadsheet1.sta Shares of indictments filed in court (Standard errors are white-noise estimates) Auto-Corr.	Std.Err.	Box & Ljung Q	p
1	-0,01434	0,17928	0,00639	0,93624
2	0,03343	0,17593	0,04251	0,97896
3	-0,02308	0,17251	0,06042	0,99612
4	-0,02257	0,16903	0,07826	0,99925
5	-0,00863	0,16547	0,08098	0,99990
6	-0,00600	0,16183	0,08236	0,99998
7	-0,01906	0,15811	0,09689	0,99999
8	-0,02079	0,15430	0,11505	1,00000
9	-0,01220	0,15039	0,12164	1,00000
10	-0,00145	0,14638	0,12174	1,00000
11	-0,03557	0,14226	0,18426	1,00000
12	-0,02897	0,13801	0,22832	1,00000
13	-0,04078	0,13363	0,32145	1,00000
14	-0,04533	0,12909	0,44475	1,00000
15	-0,04908	0,12440	0,60444	1,00000

Рисунок 3.5 – Значення автокореляційної функції та статистична значущість коефіцієнтів автокореляції нульових різниць Частки направлених до суду обвинувальних актів

Як видно з рисунків 3.4 та 3.5, немає чіткої залежності значень коефіцієнтів автокореляції різних порядків від часового лагу, крім того коефіцієнти актокореляції є статистично незначущими (p-value близьке до 1). Це свідчить про відхилення гіпотези про лінійну залежність частки направлених до суду обвинувальних актів у загальній кількості кримінальних правопорушень, за якими проводилось досудове розслідування, від двох альтернатив: частка кримінальних правопорушень, по яким проводилось досудове розслідування, яка припадає на одне повідомлення про операцію, що було передане до Державної служби фінансового моніторингу; діджиталізація економіки. Саме тому доцільно обрати у якості функції підгонки – нелінійну функцію впливу факторних ознак на результативну.

Для оцінювання ефективності системи протидії легалізації кримінальних доходів пропонується використати функцію корисності Стоуна-Гірі, яка в загальному вигляді набуває наступного вигляду:

$$u(x_1, x_2, x_3, \dots, x_n) = \prod_{j=1}^{n} (x_j - \varphi_j)^{\beta_j} \quad (3.1)$$

де $x_1, x_2, x_3, \dots, x_n$ – множина допустимих альтернатив системи протидії легалізації кримінальних доходів;

n – загальна кількість розглянутих допустимих альтернатив системи протидії легалізації кримінальних доходів;

$u(x_1, x_2, x_3, \dots, x_n)$ – функція корисності формалізації залежності ефективності системи протидії легалізації кримінальних доходів від допустимих альтернатив її досягнення;

φ_j – константа в розрізі j-тої альтернативи системи протидії легалізації кримінальних доходів;

β_j – коефіцієнт еластичності функції корисності в розрізі j-тої альтернативи системи протидії легалізації кримінальних доходів.

Розглянемо в якості результативної ознаки формалізації ефективності системи протидії легалізації кримінальних доходів в умовах діджиталізації банківської діяльності за допомогою побудови функції корисності Стоуна-Гірі показник частки направлених до суду обвинувальних актів, а в якості факторних ознак відповідно 2 показники: частка кримінальних правопорушень на 1 повідомлення про фінансову операцію; показник діджиталізації економіки. Крім того, роблячи припущення щодо нульових значень φ_j функції корисності Стоуна-Гірі, формула (3.1) набуває вигляду функції Кобба-Дугласа (формула 3.2).

$$u(x_1, x_2) = \prod_{j=1}^{2} (x_j)^{\beta_j}, \sum_{j=1}^{2} \beta_j = 1 \quad (3.2)$$

Враховуючи обмеження $\sum_{j=1}^{2} \beta_j = 1$ формули (3.2), для формалізації ефективності системи протидії легалізації кримінальних доходів в умовах діджиталізації банківської діяльності за допомогою побудови функції корисності, пропонується розглянути задачу пошуку значень коефіцієнтів еластичності двох розглянутих альтернатив як задачу нелінійного програмування:

$$\sum_{t=1}^{T} \left(u_t - \prod_{j=1}^{2} (x_{jt})^{\beta_j} \right)^2 \rightarrow min \quad (3.3)$$

$$\sum_{j=1}^{2} \beta_j = 1 \, , \beta_j \geq 0$$

де u_t - частка направлених до суду обвинувальних актів за t-ий часовий інтервал (квартал відповідного року досліджуваного часового діапазону);

Т – довжина досліджуваного часового ряду.

Для вирішення задачі нелінійного програмування мінімізації суми квадратів відхилень фактичних значень частка направлених до суду обвинувальних актів від їх теоретичних рівнів, визначених за допомогою функції корисності пропонується використати метод узагальненого градієнта за допомогою застосування інструментарію Дані/Пошук рішення програмного пакету MS Excel.

Таким чином, вирішення нелінійної оптимізаційної задачі (3.3) оцінювання ефективності системи протидії легалізації кримінальних доходів за допомогою функції корисності дозволяє отримати наступні результати

(функція 3.4) при мінімальному значенні суми квадратів відхилень фактичних значень частка направлених до суду обвинувальних актів від їх теоретичних рівнів на рівні 18,28 од.

$$u(x_1, x_2) = {x_1}^{0,0019} \cdot {x_2}^{0,9981} \quad (3.4)$$

Коефіцієнт $\beta_1 = 0{,}0019$, відображає міру еластичності ефективності системи протидії легалізації кримінальних доходів від Частки кримінальних правопорушень по яких проводилось досудове розслідування, яка припадає на одне повідомлення про операцію, що було передане до Державної служби фінансового моніторингу. Наближеність коефіцієнта до 0 свідчить про низьку ефективність існуючого підходу протидії легалізації і низьку корисність від виявлення операцій, що підлягають обов'язковому фінансовому моніторингу.

Коефіцієнт $\beta_2 = 0{,}9981$, відображає міру еластичності ефективності системи протидії легалізації кримінальних доходів від показника діджиталізації економіки, який є відношенням кількості абонентів мережі інтернет до чисельності населення. Наближеність даного коефіцієнта до 1 свідчить про високий вплив інноваційних цифрових технологій на систему протидії легалізації кримінальних доходів. Очікується значний рівень корисності від впровадження інформаційних технологій у систему протидії легалізації кримінальних доходів. При тому, ефект очікується як від провадження інноваційних технологій як на етапі моніторингу за банківськими операціями, так і на етапі досудового розслідування відповідного правопорушення.

Отже, в ході проведеного дослідження було емпірично доведено, що сучасний вигляд системи протидії легалізації кримінальних доходів є неефективним. Значні зусилля докладаються до виявлення операцій, які мають ознаки легалізації, але правоохоронний блок системи протидії легалізації кримінальних доходів не здатний забезпечити високий рівень доказовості у розслідуванні конкретних кримінальних правопорушень. Як наслідок,

виявляються мільйони підозрілих транзакцій, а до суду в квартал надходять 1-4 обвинувальних акти.

Більшу корисність для системи протидії легалізації кримінальних доходів має діджиталізація економіки. Впровадження інноваційних систем здійснення фінансових операцій, наприклад за допомогою захищеного блокчейну, не тільки знизить ризик використання даного інструменту в легалізації кримінальних доходів, а й заощадить ресурси необхідні для виявлення підозрілих операцій за рахунок автоматизації. Розвиток інформаційних систем дозволить ефективніше працювати органам досудового розслідування кримінальних правопорушень у фінансовій сфері. При цьому варто зазначити готовність інформаційної системи України до впровадження інноваційних технологій в систему протидії легалізації кримінальних доходів, отриманих незаконним шляхом.

3.2. **Концептуальні засади протидії фінансовим кібершахрайствам**

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 [68].

Після виявлення яким шляхом можуть проводитись фінансові шахрайства, формується протидія фінансовим злочинам шляхом визначення тактичних заходів з використанням наступних інструментів:

– Забезпечення нагляду, виявлення, попередження ризикивих та шахрайських операцій (безперервного нагляду за використанням онлайн

операцій, в тому числі блокчейна; пріоритетність виявлення та попередження на ранніх етапах незаконних фінансових транзакцій ґрунтуючись на інформації по ризиковим джерелам; виявлення підставних організацій у фінансових схемах за допомогою динамічної соціальної мережі; застосування, як одного з інструментів, програмного комплексу «Certified Threat Intelligence Analyst» - аналітична програма, що включає планування, аналітику, звітність загроз, навчання навиків ідентифікації та боротьби з загрозами, та ін. можливості);

– Застосування передових новітніх інструментів IT галузі (поглиблене машинне навчання, використання вбудованих графіків, для виявлення незаконної активності; побудова моделей оцінювання та прогнозування незаконних фінансових потоків; використання технологій штучного інтелекту в систему управління корпоративними фінансовими ризиками з урахуванням певних недоліків таких технологій (недостатня інтерпритованість для реалізації комплексної перевірки); застосування методу групового SHAP у банківських установах для моніторингу клієнтів (оцінка різноманітних показників організації); практичне застосування технології інженерії знань, а також онтології для розслідування злочинів, що передбачає генерування даних, аналіз, інтегрування у систему фінансової безпеки, виявлення взаємозв’язків і тенденцій у діях фінансових злочинців, прогнозування на основі використання інструменту семантичного мислення та візуалізації процесів а знань);

– Дотримання регламенту та регулювань Європейського Союзу щодо відмивання грошей в частині введення обмежень по використанню податкових гаваней (закриття філіалів та офісів непрозорих фінансових об’єктів;

– Розробка інноваційних систем кіберзахисту з ефективнішими алгоритмами, протоколами, інструментами (охорона мережі за її периметром, використання брандмауерів, антивірусів; онлайн-рішення для забезпечення кібербезпеки, управління вразливістю кіберзахисту при недостатності

відповідних кадрів, хмарна безпека даних; використання гнучких процесів автоматизації кібербезпеки з інтергацією; безпечна та надійна веб-структури з керуванням вразливістю в режимі онлайн; використання на смарт-пристроях централізованих торгових майданчиків - App Store, Play Market).

У 2022 році міжнародна організація Інтерпол успішла провела операцію HAECHI III, результатом якої стало затримання майже 1000 підозрюваних осіб та конфіскація віртуальних фінансових активів на суму 130 млн дол США [115]. Організована група злочинців використовувала наступні інструменти протиправної діяльності: голосовий фішинг, романтичне шахрайство, сексторцію, інвестиційне шахрайство та відмивання грошей, пов’язаних із незаконними азартними іграми в Інтернеті.

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. 3.6). 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 3.6 – Ключові елементи системи протидії шахрайству з банківськими платіжними картками

Джерело: складено авторами

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.

Отже,

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.

Аналізуючи вектори досліджень сучасних трендів фінансових злочинів, зазначимо, що повинні ідентифікуватись, поглиблено розглядатись та вивчатись кожне з потенційних джерел та інструментів фінансових шахрайств з їх негативними, шкідливими аспектами, таких як: зростаюча у геометричній прогресії кількість пристроїв з конфіденційними фінансовими даними, що підключаються до мережі Internet, розширення кіберпростору; використання шахраями новітніх технологій – біометрії, штучного інтелекту; суперечливе

поширення новітньої технології 5G; надмірне використання смарт-пристроїв; поширення кіберстрахування; шахрайства з криптовалютою - особливості смарт-контрактів в онлайн-сервісах, що базуються на технології блокчейн - криптовалюта та платформа Bitcoin, Ethereum; фінансування розповсюдження зброї масового знищення.

Розроблено науково-методичний підхід до оцінювання та прогнозування ризику кібершахрайств у сфері фінансових послуг на підставі згорткової нейронної мережі передбачає виконання наступних етапів: формування вхідної інформаційної бази дослідження (цільове призначення фінансової транзакції; сума транзакції; стать особи, що проводила платіж; вік особи, що проводила платіж; час доби проведення операції; день тижня проведення операції); проведено пошук форми нейронної мережі, яка забезпечують високу точність навчання тестової вибірки; представлення алгоритму прогнозування ризику кібершахрайств у сфері фінансових послуг.

У роботі удосконалено методологічний базис визначення підозрілих шахрайських фінансових операцій за допомогою методів мережевого аналізу. Для масового збору коментарів було використано інструмент Instaloader, який призначено для завантаження публікацій з соціальної мережі Instagram повністю або частково. Збір коментарів відбувався через консоль редактора коду Visual Studio Code. Для виявлення схожих ознак у текстах з метою їх кластеризації дані (762 JSON-файли з коментарями) було вирішено об’єднати в колекції. Для ідентифікації профілей осіб та їх коментарів з ознаками шахрайства, які пропонують певні фінансові послуги, було побудовано кластер зі спам-контентом.

Доведено, що динамічний розвиток криптовалют обумовлений такими їх перевагами, як наявність відкритого блокчейну, який забезпечує анонімність та надійність транзакцій; відсутність кордонів, швидкість адоптації та впровадження інновацій. Це зумовило початок процесу поступальної легалізації криптовалют на державному рівні в таких країнах та об’єднаннях як Багамські острови, Нігерія, Східнокарибський валютний союз,

Швеція, Китай, Ямайка, Україна. У той же час, розвиток криптовалют призводить до акумуляції значних шоків в міжнародній та національних фінансових системах. До деструктивних характеристик криптовалют справедливо віднести: анархічність системи (обсяг криптовалюти залежить від рівня попиту на неї), проблема довіри (вартість основана виключно на довірі та кон'юнктурі ринку), схожість на фінансову піраміду, активне використання з метою легалізації коштів отриманих незаконним шляхом, руйнівний вплив на сталий розвиток (майнінг криптовалют вимагає значного обсягу електроенергії).

Встановено, що залежно від характеру операцій, ознаками незаконних операцій з криптовалютою є: непрозорі криптовалютні контракти; зашифровані криптовалютні угоди; неперсоніфіковані транзакції; роздроблені систематичні операції на граничні, лімітовані суми для уникнення ідентифікації; операції, що не відповідають затвердженим протоколам транзакцій; операції обміну валюти неідентифікованими трейдерами; проведення заплутаного обміну криптовалюти в інші форми електронних коштів з метою виведення таких кошів у готівку; та ін.

Доведено, що відповідно до шляхів проведення, ознаками незаконних операцій з криптовалютою можуть бути: використання та комбінація офшорних акаунтів; операції через гібридні біржі; транзакції з електронним гаманцем з прямим посиланням на ринок, з правом власності первісній особі; підзвітні вузлові гаманці у разі циклічного та частого перетинання чи сходження їх транзакцій; «смурфінг», тобто створення другого додаткового облікового запису для проведення транзакцій; фальшиві платформи для торгівлі; скам-біржі криптовалют; хмарний майнінг; фішинг; віруси-здирники; клони криптовалютних гаманців; інвестиційні схеми; шахрайство із додатковим залученням обмінників; фейкові роздачі; схеми з пожертвуваннями; фінансові піраміди; підроблена криптовалюта; шахрайські фонди; та ін.

В роботі сформовано статистичну базу визначення закономірностей впливу криптовалют на фінансову стабільність держав (Німеччини, Фінляндії, Франції, Великобританії та України) у вигляді індексу фінансової стабільності, фінансового стресу, субіндексів банківського сектору, поведінки домогосподарств, валютного ринку, а також вартості та обсягів криптовалют BTC та ETH. Проведено кореляційний аналіз залежності показників характеристики криптовалют та фінансової стабільності держави, який дозволив підтвердити гіпотезу необхідності виявлення закономірностей з урахуванням лагових затримок. Реалізований автокореляційний аналіз за допомогою автокореляційних функцій та корелограм дозволивший ідентифікувати величини лагових затримок в розрізі розглянутих країн світу. Побудовано поліноміальні моделі розподіленого лагу Алмона впливу криптовалютна фінансову стабільність держави, параметри яких дозволили визначити напрямок та величину зазначеного впливу.

Кількісно підтверджено, що на даному етапі розвитку криптовалют, зміна їх вартості та обсягу майже не впливає на фінансову стабільність держави. Зростання будь-якої характеристики криптовалюти на 1% призводить до зміни показників фінансової стабільності менше ніж на 0,2% як для України, так і для Німеччини, Фінляндії, Франції та Великобританії.

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).

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.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Кільдей А. Д. Моделювання ризику шахрайства з банківськими платіжними картками : робота на здобуття кваліфікаційного ступеня бакалавра : спец. 051 - економіка / наук. кер. О. В. Кузьменко. Суми : Сумський державний університет, 2022. 51 с.

2. Sigetová K., Užíková L., Dotsenko T., Boyko A. Recent trends in financial crime. *Financial and Credit Activity: Problems of Theory and Practice*. 2022. 5(46). P. 258-270 https://doi.org/10.55643/fcaptp.5.46.2022.3897

3. Кузьменко О.В., Бойко А.О., Доценко Т.В. Сучасні тенденції оцінювання ризику легалізації коштів клієнтом банку від азартних ігор, що проводять в мережі інтернет. *Вісник СумДУ. Серія Економіка*. 2022. №3. С. 31-41.

4. Agbor A. A. A delineation of the impact of illicit financial flows on the right to development: Details from Cameroon's special criminal court. *Journal of Financial Crime*. 2022. doi:10.1108/JFC-03-2022-0071

5. Gerbrands P., Unger B., Getzner M., Ferwerda J. The effect of anti-money laundering policies: An empirical network analysis. *EPJ Data Science*. 2022. 11(1). doi:10.1140/epjds/s13688-022-00328-8

6. Mahi-Al-rashid A., Hossain F., Anwar A., Azam S. False data injection attack detection in smart grid using energy consumption forecasting. *Energies*. 2022. 15(13) doi:10.3390/en15134877

7. Müller W., Mühlenberg D., Pallmer D., Zeltmann U., Ellmauer C., Demestichas K. Knowledge engineering and ontology for crime investigation 2022. doi:10.1007/978-3-031-08333-4_39

8. Pandey A. B., Tripathi A., Vashist P. C. A Survey of Cyber Security Trends, Emerging Technologies and Threats. In: Agrawal, R., He, J., Shubhakar Pilli, E., Kumar, S. (eds) Cyber Security in Intelligent Computing and Communications. *Studies in Computational Intelligence*, vol 1007. Springer, Singapore. https://doi.org/10.1007/978-981-16-8012-0_2

9. Sallaberry J. D., Flach L. Analysis of whistleblower beliefs in latin america. [Análise das crenças whistleblower na América Latina; Análisis de las creencias whistleblower en América Latina] *Revista Criminalidad*. 2022. 64(1). P. 133-153. doi:10.47741/17943108.336

10. Singh V., Sharma S. K. Application of blockchain technology in shaping the future of food industry based on transparency and consumer trust. *Journal of Food Science and Technology*. 2022. doi:10.1007/s13197-022-05360-0

11. Klimczak K. M., Sison A. J. G., Prats M., Torres M. B. How to deter financial misconduct if crime pays? *Journal of Business Ethics*. 2022. 179(1). P. 205-222. doi:10.1007/s10551-021-04817-0

12. Wang S., Zhu X., Zhang B. A new financial crime: Proliferation financing and china's countermeasures. *Security Journal*. 2022. doi:10.1057/s41284-022-00340-7

13. Supporting an effective cyber insurance market. OECD Report fo the G7 Presidency. 2017. URL: https://www.oecd.org/daf/fin/insurance/Supporting-an-effective-cyber-insurance-market.pdf

14. Financial crime and fraud in the age of cybersecurity. McKinsey^Compane. 2019. URL: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/financial-crime-and-fraud-in-the-age-of-cybersecurity

15. ENISA Threat Landscape Report 2020. Teropean Comossion. URL: https://www.enisa.europa.eu/news/enisa-news/enisa-threat-landscape-2020

16. Financial crime – don’t become a victim! Interpol. URL: https://www.interpol.int/Crimes/Financial-crime/Financial-crime-don-t-become-a-victim

17. Global Payment Fraud Statistics, Trends & Forecasts. Merchant Savvy: веб-сайт. URL: https://www.merchantsavvy.co.uk/payment-fraud-statistics/ (дата звернення 25.05.2022).

18. 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).

19. 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).

20. 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.

21. 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.

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

23. 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). P. 69-80. doi:10.21511/bbs.16(1).2021.07

24. 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).

25. 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

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

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

28. 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).

29. 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).

30. Аналіз ринку платіжних карток та шахрайських операцій з їх використанням. URL: https://docs.google.com/presentation/d/1B3jtIWzbAJQngatOnIMwWcyvHfMnuDv3/edit#slide=id.p5 (дата звернення 01.06.2022).

31. Degtereva V., Gladkova S., Makarova O., Melkostupov E. Forming a mechanism for preventing the violations in cyberspace at the time of digitalization: Common cyber threats and ways to escape them. *ACM International Conference Proceeding Series*. 2020. doi:10.1145/3446434.3446468

32. Chen S., Gao C., Jiang D., Hao M., Ding F., Ma T., . . . Li S. The spatiotemporal pattern and driving factors of cyber fraud crime in china. *ISPRS International Journal of Geo-Information*. 2021. 10(12) doi:10.3390/ijgi10120802

33. Porcedda M. G., Wall D. S. Modelling the cybercrime cascade effect in data crime. Paper presented at the *Proceedings - 2021 IEEE European Symposium on Security and Privacy Workshops, Euro S and PW*. 2021, P. 161-177. doi:10.1109/EuroSPW54576.2021.00025

34. Sturc B., Gurova T., Zelenková N., Shestak V. Developing a system of indicators for clustering financial cybercrime. *Journal of Applied Security Research*. 2021. doi:10.1080/19361610.2021.2013112.

35. Nicholls J., Kuppa A., Le-Khac N. Financial cybercrime: A comprehensive survey of deep learning approaches to tackle the evolving financial crime landscape. IEEE Access. 2021. Vol. 9. P. 163965-163986. doi:10.1109/ACCESS.2021.3134076

36. Reznik O., Utkina M., Bondarenko O. Financial intelligence (monitoring) as an effective way in the field of combating money laundering. *Journal of Money Laundering Control*. 2021. doi:10.1108/JMLC-09-2021-0102.

37. Damaševičius R., Zailskaitė-Jakštė L. Usability and security testing of online links: A framework for click-through rate prediction using deep learning. *Electronics (Switzerland).* 2022. Vol. 11(3) doi:10.3390/electronics11030400.

38. Maclachlan F. The case for the public provisioning of the payments system. *Journal of Post Keynesian Economics.* 2021. doi:10.1080/01603477.2021.1969952.

39. Brychko M., Savchenko T., Vasylieva T., Piotrowski P. Illegal activities of financial intermediaries: A burden of trust crisis. *Journal of International Studies.* 2021. Vol. 14(1). P. 172-189. doi:10.14254/2071-8330.2021/14-1/12.

40. Costa M. P. L., Araujo E. Fuzzy financial fraud risk governance system in an information technology environment. *International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies, 3ICT*. 2021. P. 726-732. doi:10.1109/3ICT53449.2021.9581461

41. Mukhopadhyay A., Chatterjee S., Bagchi K., Kirs P. J., Shukla G. K. Cyber risk assessment and mitigation (CRAM) framework using logit and probit models for cyber insurance. *Information Systems Frontiers*. 2019. Vol. 21(5). P. 997-1018. doi:10.1007/s10796-017-9808-5

42. Rubasundram G. A. Fraud risk assessment: A tale of the possible corporate executive fraud and the perceived cyber-security. *International Journal of Recent Technology and Engineering.* 2019. 7(5 Special Issue). P. 164-168.

43. Gaol F. L., Budiansa A. D., Weniko Y. P., Matsuo T. *The digital fraud risk control on the electronic-based companies*. 2022. doi:10.1007/978-981-16-5640-8_56

44. Kraiwanit T., Srijaem P. Evaluation of internet transaction fraud in thailand. *Indian Journal of Economics and Business*. 2021. Vol. 20(1). P. 212-223.

45. Silva C. M. R. D., Feitosa E. L., Garcia V. C. Heuristic-based strategy for phishing prediction: A survey of URL-based approach. *Computers and Security*. 2020. Vol. 88. doi:10.1016/j.cose.2019.101613.

46. Suresh Babu, M., Bhavana Raj, K., & Asha Devi, D. (2019). Future trends of business intelligence and big data analytics in ubiquitous

environment. *International Journal of Engineering and Advanced Technology, 8*(3 Special Issue), 773-778

47. Cao Q., Ma B., Zhu Y. Shadow banking participation and stock market crash risk: Evidence from china. *Applied Economics*. 2021. doi:10.1080/00036846.2021.2001420.

48. Woyames Dreher V. Divergent effects of international regulatory institutions. regulating global banks and shadow banking after the global financial crisis of 2007–2009. *Review of International Political Economy*. 2020. Vol. 27(3). P. 556-582. doi:10.1080/09692290.2019.1675743

49. Bivand R., Müller W.G, Reder M. Power calculations for global and local Moran's I. *Computational Statistics & Data Analysis*. 2009. Vol. 53. P. 2859–2872. https://doi.org/10.1016/j.csda.2008.07.021

50. Leathwick J., Elith J., Hastie T. Comparative performance of generalized additive models and multivariate adaptive regression splines for statistical modelling of species distributions. *Ecological Modeling*. 2006. Vol. 199. P. 188–196. https://doi.org/10.1016/j.ecolmodel.2006.05.022.

51. 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 01.06.2022).

52. Субботін С. О. Нейронні мережі : теорія та практика: навч. посіб. / С. О. Субботін. – Житомир : Вид. О. О. Євенок, 2020. – 184 с.

53. The Global State of Digital in October 2022 – DataReportal – Global Digital Insights. (n.d.). DataReportal – Global Digital Insights. URL: https://datareportal.com/reports/digital-2022-global-overview-report

54. Bozhenko V., Mynenko S., Shtefan A. Financial Fraud Detection on Social Networks Based on a Data Mining Approach. *Financial Markets, Institutions and Risks.* 2022. Vol. 6(4). P. 119-124. http://doi.org/10.21272/fmir.6(4).119-124.2022

55. Тихомирова Є. Соціальна інженерія. In Advances in Technology and Science. 2021. P. 225–228. Library of Congress Cataloging-in-Publication Data.

56. Jakobsson M. Understanding Social Engineering Based Scams. Springer New York, NY. 2016. URL: https://link.springer.com/book/10.1007/978-1-4939-6457-4

57. Бурячок В.Л., Толубко В.Б., Хорошко В.О., Толюпа С. В. *Інформаційна та кібербезпека: соціотехнічний аспект*. 2015. URL: https://dut.edu.ua/ua/lib/1/category/1311/view/1209

58. Як не стати жертвою шахраїв в інтернеті та що робити, якщо ви потрапили у пастку. Міністрство Юстиції України. URL: https://minjust.gov.ua/m/yak-ne-stati-jertvoyu-shahraiv-v-interneti-ta-scho-robiti-yakscho-vi-potrapili-u-pastku

59. Appel G., Grewal L., Hadi R., Stephen A. T. The future of social media in marketing. *Journal of the Academy of Marketing Science*. 2019. Vol. 48(1). P. 79–95. URL: https://link.springer.com/article/10.1007/s11747-019-00695-1?utm_source=getftr&utm_medium=getftr&utm_campaign=getftr_pilot

60. Cinelli M., De Francisci Morales G., Galeazzi A., Quattrociocchi W., StarniniM. The echo chamber effect on social media. *Proceedings of the National Academy of Sciences.* 2021. 118(9). Article e2023301118.

61. Salahdine F., Kaabouch N. Social Engineering Attacks: A Survey. *Future Internet.* 2019. Vol. 11(4). 89 P.

62. Штонда Р. М., Паламарчук Н. А., Островський С. М. Соціальні мережі в інтернеті як інструмент загрози національній системі кібербезпеки України. *Актуальні проблеми управління інформаційною безпекою держави*. 2018. P. 190–192.

63. Василик А. В., Іщенко О. В. Використання соціальних мереж у сучасному рекрутингу України. *Економічний простір*. 2018. Vol. 131. P. 53–63.

64. Втрачені можливості: українці надають більшу перевагу розважальним соцмережам, ніж професійному LinkedIn | GlobalLogic Ukraine. (n.d.). GlobalLogic Ukraine

65. Instaloader – Download Instagram Photos and Metadata. (n.d.). Instaloader. URL: https://instaloader.github.io/

66. Data Mining. Orange Data Mining. URL: https://orangedatamining.com/

67. Кудь А. А. Феномен віртуальних активів: економічний та правовий аспекти. Харків. 2020. URL: IJES.2020.4.2.pdf (culturehealth.org).

68. Боженко В.В., Кільдей А.Д. Цифрові активи: можливості та загрози для національної економіки / Проблеми та перспективи забезпечення макроекономічної стабільності : монографія / за ред. С. В. Лєонова, М. М. Бричко. Суми : Сумський державний університет, 2022. С. 9-21.

69. Bank of international settlements. Annual Economic Report 2022 of the BIS. 2022. URL: https://www.bis.org/publ/arpdf/ar2022e.pdf

70. Bank of international settlements. DeFi risks and the decentralisation illusion. 2021. URL: https://www.bis.org/publ/qtrpdf/r_qt2112b.htm

71. Кудь О. О., Кучерявенко, М. П., Смичок,Є. М. (2019). Цифрові активи та їх правове регулювання у світі розвитку технології блокчейн : монографія. Харків : Право, 216 с.

72. Милош Д.В., Герасенко В.П. Перспективы развития цифровых финансовых активов. Економічний вісник університету. 2020. Випуск № 44. С. 56-63.

73. Про віртуальні активи: Закон України від 17.02.2022 № 2074-IX. URL: https://tinyurl.com/r76rpn6f.

74. Вища школа адвокатури НААУ. Класифікація віртуальних активів в Україні. 2021. URL: https://tinyurl.com/574pv2x4.

75. Central Bank Digital Currency. Which countries are using, launching, piloting their own digital currencies. 2022. URL: https://www.euronews.com/next/2022/03/09/cbdcs-these-are-the-countries-are-using-launching-or-piloting-their-own-digital-currencies

76. Coinmarketcap. URL: https://coinmarketcap.com

77. The Economic Times. Can every currency of the world be a stablecoin? 2022. URL: https://tinyurl.com/23uwbdcs.

78. Gemini. Types of Blockchains: PoW, PoS, and Private. URL: https://www.gemini.com/cryptopedia/blockchain-types-pow-pos-private.

79. Міжнародний валютний фонд. URL:https://www.imf.org/ru/home

80. Cambrige Bitcoin Electricity Consumption Index. URL: https://ccaf.io/cbeci/index.

81. Jaag C., Bach C. Cryptocurrencies: New Opportunities for Postal Financial Services. 2015. URL: www.swiss-economics.ch.

82. Darlington J. K. The Future of Bitcoin: Mapping the Global Adoption of World's Largest Cryptocurrency Through Benefit Analysis.University of Tennessee, Knoxville. 2015. URL: https://trace.tennessee.edu/utk_chanhonoproj/1770

83. Zhao L. The function and impact of cryptocurrency and data technology in the context of financial technology: Introduction to the issue. *Financial Innovationю 2021*.7(1). doi:10.1186/s40854-021-00301-w.

84. Liu X. F., Ren H. -., Liu S. -., Jiang X. -. Characterizing key agents in the cryptocurrency economy through blockchain transaction analysis. *EPJ Data Science. 2021*. 10(1). doi:10.1140/epjds/s13688-021-00276-9.

85. Bailey A. M., Rettler B., Warmke C. Philosophy, politics, and economics of cryptocurrency II: The moral landscape of monetary design. *Philosophy Compass. 2021*. 16(11) doi:10.1111/phc3.12784.

86. López-Martín C., Benito Muela S., Arguedas R. Efficiency in cryptocurrency markets: New evidence. *Eurasian Economic Review. 2021*. 11(3). 403-431. doi:10.1007/s40822-021-00182-5

87. Haq I. U., Maneengam A., Chupradit S., Suksatan W., Huo C. Economic policy uncertainty and cryptocurrency market as a risk management avenue: A systematic review. *Risks. 2021*.9(9). doi:10.3390/risks9090163

88. Mahdavi-Damghani B., Fraser R., Howell J., Halldorsson J. S. Cryptocurrency sectorization through clustering and web-scraping: Application to systematic trading. *Journal of Financial Data Science*. 2022. 4(1). P. 158-179. doi:10.3905/jfds.2021.1.080

89. Fang F., Ventre C., Basios M., Kanthan L., Martinez-Rego D., Wu F., Li L. Cryptocurrency trading: A comprehensive survey. *Financial Innovation*. 2022. 8(1) doi:10.1186/s40854-021-00321-6.

90. Bziker Z. The status of cryptocurrency in morocco. *Research in Globalization, 2021, 3* doi:10.1016/j.resglo.2021.100040

91. Widjaja G. Cryptocurrency and the role of indonesian central bank. *Journal of Legal, Ethical and Regulatory Issues*. 2021. 24(2). P. 1-8.

92. Riley J. The current status of cryptocurrency regulation in china and its effect around the world. *China and WTO Review*. 2021. 7(1). P. 135-152. doi:10.14330/cwr.2021.7.1.06.

93. Ukwueze F. O. Cryptocurrency: Towards regulating the unruly enigma of fintech in nigeria and south africa. *Potchefstroom Electronic Law Journal*. 2021. 24. doi:10.17159/1727-3781/2021/V24I0A10743

94. Delva Benavides J. E., Torres Amaya F. E. Legal, tax and accounting treatment of cryptocurrencies in mexico. *Global Jurist. 2*021. doi:10.1515/gj-2021-0061.

95. Nghiem H., Muric G., Morstatter F., Ferrara E. Detecting cryptocurrency pump-and-dump frauds using market and social signals. *Expert Systems with Applications*. 2021.182 doi:10.1016/j.eswa.2021.115284.

96. Teichmann F. M. J., Falker M. Cryptocurrencies and financial crime: Solutions from liechtenstein. *Journal of Money Laundering Control. 2021*. 24(4). P. 775-788. doi:10.1108/JMLC-05-2020-0060.

97. Huang S. Cryptocurrency and crime. FinTech, artificial intelligence and the law: Regulation and crime prevention. 2021. P. 125-143.

98. Kolesnikova K., Mezentseva O., Mukatayev T. Analysis of bitcoin transactions to detect illegal transactions using convolutional neural networks. Paper presented at the *SIST 2021 - 2021 IEEE International Conference on Smart Information Systems and Technologies*. 2021. doi:10.1109/SIST50301.2021.9465983

99. Dupuis D., Gleason K. Money laundering with cryptocurrency: Open doors and the regulatory dialectic. *Journal of Financial Crime.* 2021. 28(1). P. 60-74. doi:10.1108/JFC-06-2020-0113

100. Trozze A., Kamps J., Akartuna E. A., Hetzel F. J., Kleinberg B., Davies T., Johnson S. D. Cryptocurrencies and future financial crime. *Crime Science.* 2022. 11(1) doi:10.1186/s40163-021-00163-8.

101. Ren B., Lucey B. Do clean and dirty cryptocurrency markets herd differently? *Finance Research Letters. 2022. 47* doi:10.1016/j.frl.2022.102795

102. Akartuna E. A., Johnson S. D., Thornton A. Preventing the money laundering and terrorist financing risks of emerging technologies: An international policy delphi study. *Technological Forecasting and Social Change*. 2022. 179. doi:10.1016/j.techfore.2022.121632.

103. Lucey B. M., Vigne S. A., Yarovaya L., Wang Y. The cryptocurrency uncertainty index. *Finance Research Letters.* 2022. 45 doi:10.1016/j.frl.2021.102147.

104. Liu X. F., Ren H. -., Liu S. -., Jiang X. Characterizing key agents in the cryptocurrency economy through blockchain transaction analysis. EPJ Data Science. 2021.10(1) doi:10.1140/epjds/s13688-021-00276-9.

105. Savchuk T. O., Pryimak N. V., Slyusarenko N. V., Smolarz A., Smailova S., Amirgaliyev Y. Improved method of searching the associative rules while developing the software. *International Journal of Electronics and Telecommunications*. 2020. 66(3), 425-430. doi:10.24425-ijet.2020.131895/715.

106. Horban H., Kandyba I., Dvoretskyi M., Boiko A. Principles of searching for a variety of types of associative rules in OLAP-cubes. *CEUR Workshop Proceedings*. 2021. 2845. P.181-192.

107. Конспект лекцій з дисципліни «Самонавчання складних систем» для студентів спеціальності 8.04030301 «Системний аналіз і управління». Державний вищий навчальний заклад “Національний гірничий університет”. 2011. URL: https://sau.nmu.org.ua/ua/osvita/metod/magistr/Self_ conditioning_of_complex_systems(Lecture)_NMU_SAU.pdf

108. The Use of Ethereum in Illegal Activities Rises for Many Criminals. Korea IT Times. 2022. URL: https://www.koreaittimes.com/news/articleView.html?idxno=115122Hj

109. Ethereum Fraud Detection Dataset. Kaggle. URL: https://www.kaggle.com/datasets/vagifa/ethereum-frauddetection-dataset

110. Чучук Ю. Теоретична сутність понять економічна ефективність та ефективність діяльності. *Ефективна економіка.* 2014. №2. URL: http://www.economy.nayka.com.ua/?op=1&z=2765

111. Małecka M. Values in economics: a recent revival with a twist. *Journal of Economic Methodology*. 2021. 28:1. P. 88-97

112. Генеральна прокуратура України: офіційний веб сайт. URL: https://www.gp.gov.ua/ua/1stat

113. Державна служба фінансового моніторингу України: офіційний веб-сайт. URL: https://fiu.gov.ua/pages/dijalnist/funkcional/statistika-ta-infografika

114. Державні служба статистики Укаїни: офіційни веб-сайт. URL: http://www.ukrstat.gov.ua/

115. Cyber-enabled financial crime: USD 130 million intercepted in global INTERPOL police operation. Interpol. URL: https://www.interpol.int/News-and-Events/News/2022/Cyber-enabled-financial-crime-USD-130-million-intercepted-in-global-INTERPOL-police-operation

ДОДАТКИ

ДОДАТОК А

Результати побудови нейромережевих моделей для оцінювання ризику фінансового кібершахрайства

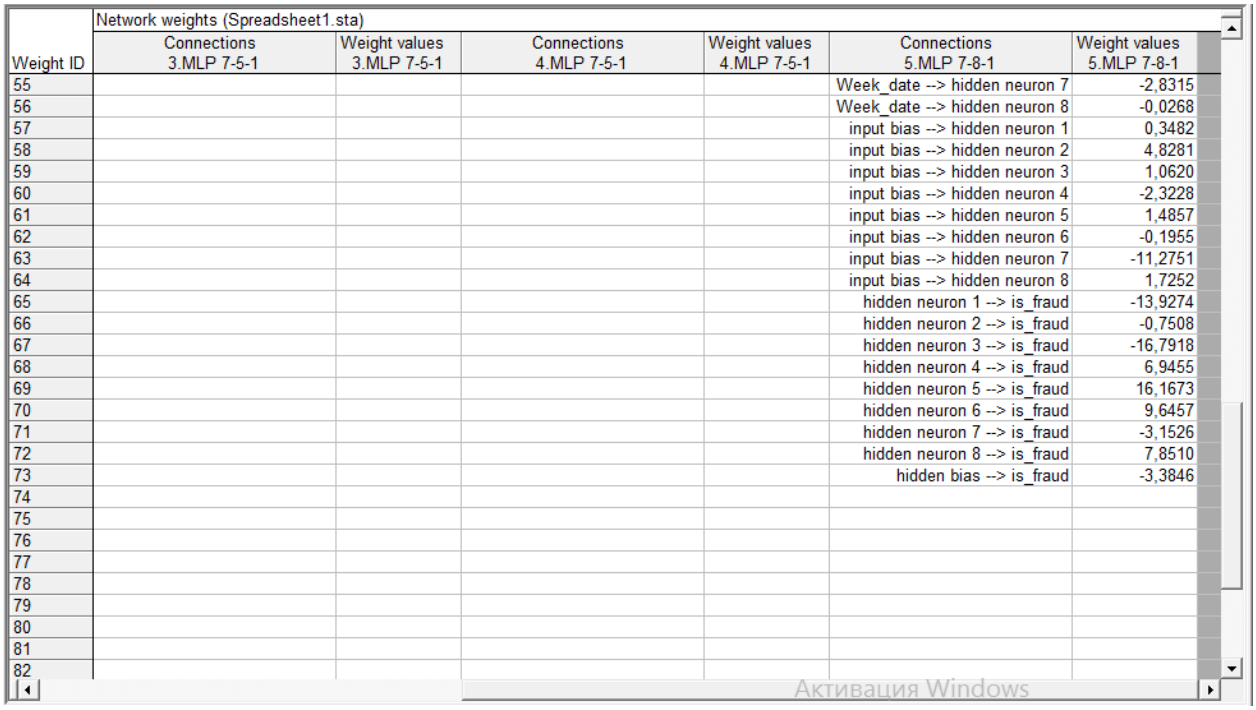
Network weights (Spreadsheet1.sta)

Weight ID	Connections 3.MLP 7-5-1	Weight values 3.MLP 7-5-1	Connections 4.MLP 7-5-1	Weight values 4.MLP 7-5-1	Connections 5.MLP 7-8-1	Weight values 5.MLP 7-8-1
1	cc_num --> hidden neuron 1	-4,0240	cc_num --> hidden neuron 1	-1,5944	cc_num --> hidden neuron 1	-0,1076
2	cc_num --> hidden neuron 2	-12,6913	cc_num --> hidden neuron 2	-3,5831	cc_num --> hidden neuron 2	-65,7287
3	cc_num --> hidden neuron 3	14,1261	cc_num --> hidden neuron 3	-7,7976	cc_num --> hidden neuron 3	0,7629
4	cc_num --> hidden neuron 4	35,2826	cc_num --> hidden neuron 4	-1,2634	cc_num --> hidden neuron 4	2,1286
5	cc_num --> hidden neuron 5	27,9063	cc_num --> hidden neuron 5	7,3452	cc_num --> hidden neuron 5	0,2560
6	amt --> hidden neuron 1	18,7772	amt --> hidden neuron 1	-14,5368	cc_num --> hidden neuron 6	1,8959
7	amt --> hidden neuron 2	-23,2665	amt --> hidden neuron 2	-0,8644	cc_num --> hidden neuron 7	0,1180
8	amt --> hidden neuron 3	-0,1395	amt --> hidden neuron 3	4,1276	cc_num --> hidden neuron 8	0,1076
9	amt --> hidden neuron 4	-70,3528	amt --> hidden neuron 4	-19,5980	amt --> hidden neuron 1	-15,0494
10	amt --> hidden neuron 5	0,5410	amt --> hidden neuron 5	-0,8575	amt --> hidden neuron 2	0,7691
11	birth --> hidden neuron 1	-2,6496	birth --> hidden neuron 1	-3,1104	amt --> hidden neuron 3	2,0294
12	birth --> hidden neuron 2	2,0735	birth --> hidden neuron 2	-3,1853	amt --> hidden neuron 4	-6,9032
13	birth --> hidden neuron 3	0,0485	birth --> hidden neuron 3	-1,9019	amt --> hidden neuron 5	-0,2054
14	birth --> hidden neuron 4	-0,2636	birth --> hidden neuron 4	-0,4376	amt --> hidden neuron 6	-0,0154
15	birth --> hidden neuron 5	-0,7097	birth --> hidden neuron 5	1,7453	amt --> hidden neuron 7	0,0077
16	time --> hidden neuron 1	33,6740	time --> hidden neuron 1	2,7679	amt --> hidden neuron 8	40,5452
17	time --> hidden neuron 2	9,3340	time --> hidden neuron 2	-0,7121	birth --> hidden neuron 1	-0,0152
18	time --> hidden neuron 3	-16,2636	time --> hidden neuron 3	-7,1342	birth --> hidden neuron 2	0,5863
19	time --> hidden neuron 4	-2,9899	time --> hidden neuron 4	-2,8074	birth --> hidden neuron 3	-0,1331
20	time --> hidden neuron 5	4,8023	time --> hidden neuron 5	-2,9713	birth --> hidden neuron 4	-1,3970
21	gender2 --> hidden neuron 1	11,8304	gender2 --> hidden neuron 1	-0,3354	birth --> hidden neuron 5	0,0155
22	gender2 --> hidden neuron 2	-29,0316	gender2 --> hidden neuron 2	0,1052	birth --> hidden neuron 6	-0,0485
23	gender2 --> hidden neuron 3	127,4405	gender2 --> hidden neuron 3	-38,4271	birth --> hidden neuron 7	-24,0793
24	gender2 --> hidden neuron 4	-1,6147	gender2 --> hidden neuron 4	0,8018	birth --> hidden neuron 8	0,8223
25	gender2 --> hidden neuron 5	-0,8162	gender2 --> hidden neuron 5	-0,9426	time --> hidden neuron 1	2,2162
26	category2 --> hidden neuron 1	-0,1927	category2 --> hidden neuron 1	0,2355	time --> hidden neuron 2	-2,2427
27	category2 --> hidden neuron 2	-4,1593	category2 --> hidden neuron 2	2,1451	time --> hidden neuron 3	0,5635
28	category2 --> hidden neuron 3	-0,5874	category2 --> hidden neuron 3	-0,0633	time --> hidden neuron 4	0,0390

Network weights (Spreadsheet1.sta)

Weight ID	Connections 3.MLP 7-5-1	Weight values 3.MLP 7-5-1	Connections 4.MLP 7-5-1	Weight values 4.MLP 7-5-1	Connections 5.MLP 7-8-1	Weight values 5.MLP 7-8-1
28	category2 --> hidden neuron 3	-0,5874	category2 --> hidden neuron 3	-0,0633	time --> hidden neuron 4	0,0390
29	category2 --> hidden neuron 4	7,7014	category2 --> hidden neuron 4	-0,2520	time --> hidden neuron 5	0,0030
30	category2 --> hidden neuron 5	5,7137	category2 --> hidden neuron 5	66,6839	time --> hidden neuron 6	1,7963
31	Week_date --> hidden neuron 1	31,4874	Week_date --> hidden neuron 1	-0,9802	time --> hidden neuron 7	-0,2621
32	Week_date --> hidden neuron 2	-29,4272	Week_date --> hidden neuron 2	0,0820	time --> hidden neuron 8	-0,4710
33	Week_date --> hidden neuron 3	7,7142	Week_date --> hidden neuron 3	0,4619	gender2 --> hidden neuron 1	1,4118
34	Week_date --> hidden neuron 4	-13,6799	Week_date --> hidden neuron 4	-0,2642	gender2 --> hidden neuron 2	-0,0290
35	Week_date --> hidden neuron 5	2,8949	Week_date --> hidden neuron 5	0,0382	gender2 --> hidden neuron 3	0,0212
36	input bias --> hidden neuron 1	-20,0664	input bias --> hidden neuron 1	11,1143	gender2 --> hidden neuron 4	-0,1386
37	input bias --> hidden neuron 2	3,6992	input bias --> hidden neuron 2	1,9725	gender2 --> hidden neuron 5	-63,7537
38	input bias --> hidden neuron 3	24,3658	input bias --> hidden neuron 3	9,0650	gender2 --> hidden neuron 6	1,1164
39	input bias --> hidden neuron 4	-8,9063	input bias --> hidden neuron 4	0,2392	gender2 --> hidden neuron 7	3,2812
40	input bias --> hidden neuron 5	-9,8802	input bias --> hidden neuron 5	-7,2556	gender2 --> hidden neuron 8	0,3897
41	hidden neuron 1 --> is_fraud	0,1254	hidden neuron 1 --> is_fraud	-0,0001	category2 --> hidden neuron 1	1,7766
42	hidden neuron 2 --> is_fraud	-2,3985	hidden neuron 2 --> is_fraud	0,8470	category2 --> hidden neuron 2	0,1553
43	hidden neuron 3 --> is_fraud	-4,6354	hidden neuron 3 --> is_fraud	-0,3479	category2 --> hidden neuron 3	0,0709
44	hidden neuron 4 --> is_fraud	-3,2223	hidden neuron 4 --> is_fraud	-2,9155	category2 --> hidden neuron 4	29,7004
45	hidden neuron 5 --> is_fraud	-3,4289	hidden neuron 5 --> is_fraud	-2,0401	category2 --> hidden neuron 5	-0,8916
46	hidden bias --> is_fraud	-4,5542	hidden bias --> is_fraud	0,8388	category2 --> hidden neuron 6	-3,0733
47					category2 --> hidden neuron 7	13,3611
48					category2 --> hidden neuron 8	-0,5454
49					Week_date --> hidden neuron 1	-0,1202
50					Week_date --> hidden neuron 2	0,0484
51					Week_date --> hidden neuron 3	85,4013
52					Week_date --> hidden neuron 4	-0,2817
53					Week_date --> hidden neuron 5	0,0848
54					Week_date --> hidden neuron 6	-0,0995
55					Week_date --> hidden neuron 7	-2,8315

Продовження рисунку А.1



Network weights (Spreadsheet1.sta)

Weight ID	Connections 3.MLP 7-5-1	Weight values 3.MLP 7-5-1	Connections 4.MLP 7-5-1	Weight values 4.MLP 7-5-1	Connections 5.MLP 7-8-1	Weight values 5.MLP 7-8-1
55					Week_date --> hidden neuron 7	-2,8315
56					Week_date --> hidden neuron 8	-0,0268
57					input bias --> hidden neuron 1	0,3482
58					input bias --> hidden neuron 2	4,8281
59					input bias --> hidden neuron 3	1,0620
60					input bias --> hidden neuron 4	-2,3228
61					input bias --> hidden neuron 5	1,4857
62					input bias --> hidden neuron 6	-0,1955
63					input bias --> hidden neuron 7	-11,2751
64					input bias --> hidden neuron 8	1,7252
65					hidden neuron 1 --> is_fraud	-13,9274
66					hidden neuron 2 --> is_fraud	-0,7508
67					hidden neuron 3 --> is_fraud	-16,7918
68					hidden neuron 4 --> is_fraud	6,9455
69					hidden neuron 5 --> is_fraud	16,1673
70					hidden neuron 6 --> is_fraud	9,6457
71					hidden neuron 7 --> is_fraud	-3,1526
72					hidden neuron 8 --> is_fraud	7,8510
73					hidden bias --> is_fraud	-3,3846
74						
75						
76						
77						
78						
79						
80						
81						
82						

Рисунок А.1 – Фрагмент нейронних мереж з архітектурою MLP 7-5-1 (загальна кількість шарів 7, кількість прихованих шарів 5), MLP 7-8-1 (загальна кількість шарів 7, кількість прихованих шарів 8) ризику кібершахрайств