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

(остаточний)

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

2023

Рукопис закінчено 15 «грудня» 2023 р.

Результати роботи розглянуті науковою радою СумДУ протокол від ____ грудня 2023 №_

СПИСОК АВТОРІВ

Керівник НДР – Головна наукова співробітниця, д-рка екон. наук, професорка	_____ 15.12.2023	Ольга КУЗЬМЕНКО (розділ 2, 4, підрозділ 3.2)
Відповідальний виконавець Старша наукова співробітниця, канд. екон. наук	_____ 15.12.2023	Вікторія БОЖЕНКО (розділ 1, 4, підрозділ 3.2)
Виконавці: Старший науковий співробітник, доктор екон. наук	_____ 15.12.2023	Антон БОЙКО (розділ 2, 5)
Виконавець за договором підряду, асистент	_____ 15.12.2023	Олександр КУШНЕРЬОВ (розділ 1, 2, підрозділ 3.1, 3.2)
Старший науковий співробітник, канд. екон. наук	_____ 15.12.2023	Андрій БОЖЕНКО (підрозділ 3.2)
Старша наукова співробітниця, доктор філософії	_____ 15.12.2023	Тетяна ДОЦЕНКО (підрозділ 1.1, 4.1, 5.1)
Виконавець за договором підряду, канд. екон. наук	_____ 15.12.2023	Андрій СЕМЕНОГ (підрозділ 2.3)
Виконавиця за договором підряду, канд. екон. наук	_____ 15.12.2023	Олена ПАХНЕНКО (підрозділ 4.1, 5.1)
Науковий співробітник, доктор філософії	_____ 15.12.2023	Сергій МИНЕНКО (підрозділ 2.2, 2.3, 4.3, розділ 5)

Виконавиця за договором підряду, аспірантка _____ 15.12.2023 Юлія ДОЛЯ (розділ 4)

Виконавиця за договором підряду, аспірантка _____ 15.12.2023 Аліна ЄФІМЕНКО (підрозділ 5.1)

Виконавець за договором підряду, аспірант _____ 15.12.2023 Євген ПІГУЛЬ (висновки)

Виконавець за договором підряду, студент _____ 15.12.2023 Артем ШТЕФАН (підрозділ 2.2)

Виконавиця за договором підряду, студентка _____ 15.12.2023 Анастасія КІЛЬДЕЙ (підрозділ 1.2, 2.1)

Виконавиця за договором підряду, студентка _____ 15.12.2023 Карина ПЕТРЕНКО (підрозділ 2.3)

Виконавиця за договором підряду, студентка _____ 15.12.2023 Марія ГАБЕНКО (підрозділ 1.2)

Виконавиця за договором підряду, студентка _____ 15.12.2023 Валерія ГЕРАСИМЕНКО (підрозділ 3.2)

РЕФЕРАТ

Звіт про НДР: 387 с., 84 табл., 123 рис., 6 дод., 160 джерел.

КІБЕРШАХРАЙСТВА, КРИПТОВАЛЮТА, НЕЗАКОННІ ФІНАНСОВІ ОПЕРАЦІЇ, РЕГУЛЮВАННЯ, СПОЖИВАЧІ ФІНАНСОВИХ ПОСЛУГ, ФІНАНСОВИЙ СЕКТОР, DATA MINING, FINTECH

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 загальнонаукові методи (наукової абстракції, аналізу, синтезу, індукції, дедукції, узагальнення) – для уточнення понятійно-категоріального апарату дослідження; комплексне поєднання бібліометричного та трендового аналізів – для дослідження змістовно-контекстуальних та еволюційно-просторових закономірностей публікаційної активності у сфері кібербезпеки; методи попарного порівняльного та статистичного аналізів – для характеристики поточного стану та тенденцій закономірностей розвитку кібершахрайств в Україні та світі; методи формально-логічного аналізу – для визначення основних передумов поширення кіберзагроз в економічній системі; кластерний, дисперсіний аналізи та дерева класифікації – при проведенні типологізації країн за рівнем участі їх резидентів у здійсненні кібернетичних та фінансових шахрайств; сплайн-моделювання – для визначення імпульсів активізації фінансових злочинів, спричинених цифровізацією економіки; метод групового врахування аргументів Івахненка – при розрахунку інтегрального індексу кіберзагроз; метод опорних векторів – при формалізації ключових

детермінантів активізації кіберзагроз; поєднання методів головних компонент та узагальненого знижуючого градієнту –при визначенні рівня кібервразливості споживачів фінансових послуг; нейромережева модель – при розрахунку ризику фінансових кібершахрайств; трансформована мультиплікативна згортка Кіні – при визначенні інтегральних показників для характеристики діджиталізації фінансового сектору, технологічного розвитку та ризику кіберзагроз; метод побудови таблиць виживання та метод Каплана-Мейєра – для оцінювання ефективності інституційних змін системи протидії легалізації доходів, одержаних незаконним шляхом; поліноміальна модель розподіленого лагу Алмона – при оцінюванні впливу фінансових та кібернетичних злочинів на рівень довіри до фінансового сектору.

При виконанні НДР були отримані наступні нові наукові та прикладні результати: 1) вперше розроблено науково-методичний підхід до оцінювання каузальних зв’язків між розвитком фінтех інновацій, кількістю фінансових та кібернетичних правопорушень на основі багатомірних адаптивних регресивних MAR-сплайнів; 2) розроблено методологію формалізації факторів стрімкого поширення кіберзагроз на основі побудови сигмоїдної моделі із застосуванням методів машинного навчання SVM; 3) розроблено методологію інтегрального оцінювання кібервразливості споживачів фінансових послуг шляхом системного поєднання за допомогою методів головних компонент, узагальненого знижуючого градієнту та мультиплікативної згортки Кіні; 4) розроблено методику для формування кластерів країн за рівнем фактичної або ймовірної участі їх резидентів у протиправних кібернетичних правопорушеннях шляхом використання методу одномірного розгалуження CART; 5) розроблено науково-методичний підхід до оцінювання впливу аспектів використання криптовалют на оцінку кібербезпеки країни; 6) розроблено науково-методичний підхід до оцінювання дискретного лагового впливу фінансових кібершахрайств на рівень довіри клієнтів до фінансових установ на основі поліноміальної моделі розподіленого лагу Алмона; 7) удосконалено науково-методичний підхід до оцінювання

ефективності протидії використання послуг та/або інфраструктури фінансових посередників для легалізації кримінальних доходів шляхом побудови системи симультативних рівнянь; 8) розроблено науково-методичний підхід до оцінювання рівня ефективності розслідування злочинів легалізації доходів, отриманих незаконним шляхом за допомогою методу аналізу виживання Каплана-Мейєра.

Результати проекту мають не лише наукову та практичну цінність, а також використовуються як розробки методичного характеру при викладанні курсів. Зокрема, результати досліджень були використані при викладанні наступних навчальних дисциплін: «Технології інтелектуальну аналізу даних», «Прикладна економетрика», «Програмне забезпечення математичного та статистичного аналізу», «Системи штучного інтелекту в моделюванні економіки» «Моделювання економіки» та «Прикладна статистика» для студентів освітнього ступеня бакалавр та магістр за спеціальністю 051 «Економіка».

У межах дослідження підготовлено та захищено 2 дисертації на здобуття наукового ступеня доктора філософії (Доценко Т.В. [1], Миненко С.В. [2]), 1 дисертацію на здобуття наукового ступеня доктора філософії подано до разової спеціалізованої вченої ради (Кушнерьов О.С.) та 1 дисертацію на здобуття наукового ступеня доктора економічних наук подано до постійної спеціалізованої вченої ради (Семеног А.Ю.).

ЗМІСТ

ВСТУП 9
1 ТЕОРЕТИЧНІ ЗАСАДИ ВИЗНАЧЕННЯ ЗМІСТУ КІБЕРЗАГРОЗ ТА ТЕНДЕНЦІЇ ЇХ ПОШИРЕННЯ 12
1.1 Декомпозиційний аналіз змістовних аспектів кіберзагроз в системі економічних відносин 12
1.2 Сучасні тенденції поширення кіберзлочинності в Україні та світі 28
1.3 Методичний підхід до визначення детермінантів поширення кібершахрайств 47
1.4 Проведення типологізації країн за рівнем участі їх резидентів у здійсненні кібернетичних та фінансових шахрайств 63
2 РОЗВИТОК МЕТОДИЧНОГО ІНСТРУМЕНТАРІЮ ОЦІНЮВАННЯ ПЕРЕДУМОВ ТА ПОТОЧНОГО СТАНУ КІБЕРЗАГРОЗ В УМОВАХ ДІДЖИТАЛІЗАЦІЇ ЕКОНОМІКИ 81
2.1 Методичні засади до оцінювання ризику фінансових кібершахрайств 81
2.2 Науково-методологічне підґрунтя визначення фінансових шахрайств у соціальних мережах 93
2.3 Визначення імпульсів активізації фінансових злочинів, спричинених цифровізацією економіки 106
2.4 Науково-методичний підхід до ідентифікації критичних зон кіберзагроз фінансовому сектору економіки України 129
3 ОСОБЛИВОСТІ ВІКТИМНОЇ ПОВЕДІНКИ СПОЖИВАЧІВ ФІНАНСОВИХ ПОСЛУГ У КІБЕРПРОСТОРІ 151
3.1 Науково-методичний підхід до оцінювання рівня кіберврразливості економічних агентів 151
3.2 Побудова фазового портрету потенційної жертви кіберзлочинності у сфері фінансових послуг 163
3.3 Оцінювання впливу фінансових та кібернетичних злочинів на рівень довіри до фінансового сектору 176
4 ІДЕНТИФІКАЦІЯ ІНФОРМАЦІЙНИХ ОЗНАК, ЯКІ ЗАСВІДЧУЮТЬ ЗДІЙСНЕННЯ НЕЗАКОННИХ ОПЕРАЦІЙ З КРИПТОВАЛЮТОЮ 192
4.1 Дослідження можливостей та загроз, які спричиняє криптовалюта для національної економіки 192
4.2 Визначення закономірностей здійснення фінансових кібершахрайств з використанням криптовалюти 204
4.3 Оцінювання впливу використання криптовалют на кібербезпеку країни 229
4.4 Методичні засади дослідження вплив криптовалюти на фінансову стабільність держави 243
5 МЕТОДИЧНІ ЗАСАДИ ОЦІНЮВАННЯ РОЛІ ДІДЖИТАЛІЗАЦІЇ В СИСТЕМІ ПРОТИДІЇ ЛЕГАЛІЗАЦІЇ ДОХОДІВ, ОТРИМАНИХ НЕЗАКОННИМ ШЛЯХОМ 285

5.1 Дослідження місця та значення діджиталізації в системі протидії легалізації доходів, отриманих незаконним шляхом 285
5.2 Оцінювання ефективності інституційних змін системи протидії легалізації доходів одержаних незаконним шляхом 294
5.3 Прогнозування ефективності каналів протидії легалізації кримінальних доходів 306
5.4 Дорожня карта реформ національної системи протидії легалізації доходів одержаних незаконним шляхом 324
ВИСНОВКИ 339
ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ 347
ДОДАТКИ 366

ВСТУП

Перехід людства до якісно нового етапу інноваційної економіки – Індустрії 4.0 супроводжується структурною перебудовою соціально-економічних відносин у країні. Проникнення цифрових технологій, автоматизація і використання технологій штучного інтелекту й машинного навчання, акумулювання великих даних, поширення Інтернету речей з однієї сторони відкривають нові можливості для інтенсивного розвитку держави, а з іншого – підвищують вразливість національної економіки перед зовнішніми викликами і загрозами цифрових трансформацій. Масова імплементація технологій у промислове виробництво та в організацію бізнес-процесів формує потенційну вразливість інформаційних систем до технологічних збоїв та кіберзагроз. За даними звітів Allianz Risk Barometer у 2022 та 2023 роках кіберінциденти є головними бізнес-ризиками у світі. Економічні суб'єкти щоденно стикаються з численними кіберзагрозами, що походять як із зовнішніх, так і з внутрішніх джерел. Світова статистика засвідчує, що 64% компаній наражалися на спроби веб-атак, 62% – зазнавали атак фішингу та соціальної інженерії, 59% – стикалися зі шкідливим програмним забезпеченням і ботнетами, 51% – протистояли атакам типу «відмова в обслуговуванні». Застаріле програмне забезпечення, низький рівень цифрової гігієни працівників, недостатній рівень інвестицій у систему кіберзахисту корпоративних інформаційних систем та інші види вразливостей можуть призвести до значних матеріальних збитків, неавторизованого доступу до конфіденційної інформації, компрометації даних, репутаційних втрат тощо.

Виходячи з цього, у сучасних умовах забезпечення стійкості об'єктів критичної інфраструктури до кіберзагроз та підвищення культури безпекового поводження громадян в кіберпросторі є одним із ключових питань державної політики для регуляторних і наглядових органів.

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 загальнонаукові методи (наукової абстракції, аналізу, синтезу, індукції, дедукції, узагальнення) – для уточнення понятійно-категоріального апарату дослідження; комплексне поєднання бібліометричного та трендового аналізів – для дослідження змістовно-контекстуальних та еволюційно-просторових закономірностей публікаційної активності у сфері кібербезпеки; методи попарного порівняльного та статистичного аналізів – для характеристики поточного стану та тенденцій закономірностей розвитку кібершахрайств в Україні та світі; методи формально-логічного аналізу – для визначення основних передумов поширення кіберзагроз в економічній системі; кластерний, дисперсіний аналізи та дерева класифікації – при проведенні типологізації країн за рівнем участі їх резидентів у здійсненні кібернетичних та фінансових шахрайств; сплайн-моделювання – для визначення імпульсів активізації фінансових злочинів, спричинених цифровізацією економіки; метод групового врахування аргументів Івахненка – при розрахунку інтегрального індексу кіберзагроз; метод опорних векторів – при формалізації ключових детермінантів активізації кіберзагроз; поєднання методів головних компонент та узагальненого знижуючого градієнту –при визначенні рівня кібервразливості споживачів фінансових послуг; нейромережева модель – при розрахунку ризику фінансових кібершахрайств; трансформована мультиплікативна згортка Кіні – при визначенні інтегральних показників для характеристики діджиталізації фінансового сектору, технологічного розвитку

та ризику кіберзагроз; метод побудови таблиць виживання та метод Каплана-Мейєра – для оцінювання ефективності інституційних змін системи протидії легалізації доходів, одержаних незаконним шляхом; поліноміальна модель розподіленого лагу Алмона – при оцінюванні впливу фінансових та кібернетичних злочинів на рівень довіри до фінансового сектору.

Інформаційну базу дослідження склали: закони України, міжнародні нормативно-правові акти, нормативно-правова база профільних міністерств та відомств, звітно-аналітична інформація Державної служби статистики України; дані Міжнародного валютного фонду, Світового банку, Організації економічного співробітництва та розвитку, Євробарометр, результати наукових досліджень у сфері кібербезпеки та кіберзахисту.

У межах дослідження підготовлено та захищено 2 дисертації на здобуття наукового ступеня доктора філософії (Доценко Т.В. [1], Миненко С.В. [2]), 1 дисертацію на здобуття наукового ступеня доктора філософії подано до разової спеціалізованої вченої ради (Кушнерьов О.С.) та 1 дисертацію на здобуття наукового ступеня доктора економічних наук подано до постійної спеціалізованої вченої ради (Семеног А.Ю.).

1 ТЕОРЕТИЧНІ ЗАСАДИ ВИЗНАЧЕННЯ ЗМІСТУ КІБЕРЗАГРОЗ ТА ТЕНДЕНЦІЇ ЇХ ПОШИРЕННЯ

1.1 Декомпозиційний аналіз змістовних аспектів кіберзагроз в системі економічних відносин

Швидкі темпи цифровізації економічних відносин, автоматизація бізнес-процесів, перехід на електронне урядування ставить нові виклики безпеки у кіберпросторі перед урядами багатьох країн. Анонімність, невизначеність географічної зони здійснення кіберзлочину, постійне удосконалення способів здійснення кібератак відрізняє кіберзагрози від традиційних загроз стабільного функціонування національної економіки.

На сьогодні протидія кіберзагрозам є однією із головних тем для обговорення на міжнародних економічних форумах і конференціях, дана проблематика широко висвітлена у працях зарубіжних та вітчизняних науковців. Кібершахрайство представляє загрозу економічній безпеці будь-якої країни, вона набуває глобального характеру, оскільки різні способи кібератак доволі часто мають транскордонний характер. Саме тому розвиток сучасної економічної науки неможливий в межах ізольованої території окремої країни. Виходячи з цього, джерелом даних про наукові публікації для проведення бібліометричного аналізу виступила міжнародна наукометрична база даних Scopus.

Для пошуку публікацій у сфері кіберзахисту та кібербезпеки у контексті розвитку національної економіки обрано декілька ключових слів. Зауважимо, до для бібліографічного аналізу відібрано тільки наукові статті, які опубліковані протягом 2012-2022 років та входять до трьох галузей знань «соціальні науки», «бізнес, управління та облік» та «економіка, економетрика та фінанси». Результати проведеного пошуку наукових публікацій у наукометричній базі Scopus подано в таблиці 1.1.

Таблиця 1.1 – Динаміка наукових публікацій, присвячених вивченню питання кіберзагроз та інших споріднених понять у системі економічних відносин, одиниць

Ключові слова для пошуку	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	ВСЬОГО
1. Cyber AND threat*	29	51	46	60	74	97	123	165	211	235	246	1337
2. Cyber AND attack*	34	71	59	52	83	117	154	196	214	267	306	1553
3. Cyber AND security	64	106	105	125	137	193	267	373	400	472	507	2749
4. Cyber AND crime	53	60	46	55	69	96	108	133	128	152	139	1039
5. Cyber AND threat* OR attack* OR security OR crime	111	164	152	173	211	299	366	491	552	648	690	3857

Джерело: складено автором на основі наукометричної бази Scopus

Дані таблиці 1.1 демонструють, що протягом останніх десяти років науковий інтерес до вивчення питань кіберзагроз постійно та динамічно зростає. Зокрема, близько половини наукових статтей з досліджуваної проблематики опублікована протягом останніх трьох років (2020-2022): напрямок «cyber threat» – 692 публікації або 51,8% від загального обсягу протягом 2012-2022 рр.; напрямок «cyber attack» – 787 публікації або 50,7%; напрямок «cyber security» – 1379 публікації або 50,2%; напрямок «cyber crime» – 419 публікації або 40,3%.

Для уникнення дублювання наукових статей, які будуть використані для подальшого бібліографічного аналізу, пошуковий запит сформульовано наступним чином «Cyber AND threat* OR attack* OR security OR crime». За цим запитом відібрано 3857 науковий публікацій із середньорічним темпом зростання опублікованих наукових статей на рівні 20%. Щодо резиденства наукових авторів, якими найбільше опубліковано статей з цієї проблематики, то це США – 1174 статті (або 30,4% від загального обсягу), Великобританія – 509 статей (або 13,2%), Індія – 282 статті (або 7,3%). Зауважимо, що науковцями з України протягом 2012-2022 років опубліковано 67 статей. Дані цифри наочно демонструють, що протидія кіберзагрозам залишається пріоритетним для будь-яких країн світу незалежно від рівня економічного її розвитку.

З метою проведення більш ґрунтовного дослідження визначення підходів до виявлення та протидії кіберзагрозам проведено бібліометричний аналіз за допомогою інструментарію VOSViewerv.1.6.10, що дозволяє ідентифікувати взаємозв'язки між об'єктами, проводити кластеризацію і візуалізацію наукометричних даних. Особливістю кластерного бібліографічного аналізу полягає в тому, що чим схожишіми є ключові слова у кластері, тим сильнішим є їх взаємозв'язок і більше науковий статей, в яких зустрічаються дані ключові слова. Об'єктом бібліометричного аналізу обрано 3857 наукові статті у виданнях, що індексуються наукометричною базою даних Scopus, які відповідають одночасному врахуванні в пошуковому запиті таких категорій як «кібер загрози», «кібер атаки», «кібер безпека», «кіберзлочин» за період 2012–2022 рр.

Проаналізувавши ключові слова в анотаціях відібраних наукових статей виявлено значну кількість дублювань понять (наприклад, «cyber-attack», «cyberattack», «cyberattacks», «cyber attack» тощо). Для усунення цієї проблеми було складено спеціальний тезаурус, щоб об'єднати схожі терміни та усунути помилки у ключових словах.

За результатами бібліографічного аналізу було виявлено 14 838 спільних ключових слів, які зустрічаються в анотаціях та назвах наукових статей. Для візуалізації спільного використання ключових слів встановлено порогове значення на рівні 7 повторень, що дозволило відфільтрувати 200 ключових слів. Графічна візуалізація результатів бібліометричного аналізу за допомогою інструментарію VOSviewer представлена на рисунку 1.1.

За результатами аналізу частоти використання ключових слів з цієї проблематики у наукових статтях виокремлено чотири кластери:

Науковий кластер 1 (червоний колір) присвячений вивченню кібербезпеки та складові її забезпечення (74 ключові слова). Основними ключовими словами цього кластеру є: кібер безпека, кібер загрози, компю'ютерні мережі, управління ризиком, інформаційна безпека, управління знаннями, технології, приватність, ланцюги поставок, діджиталізація тощо.

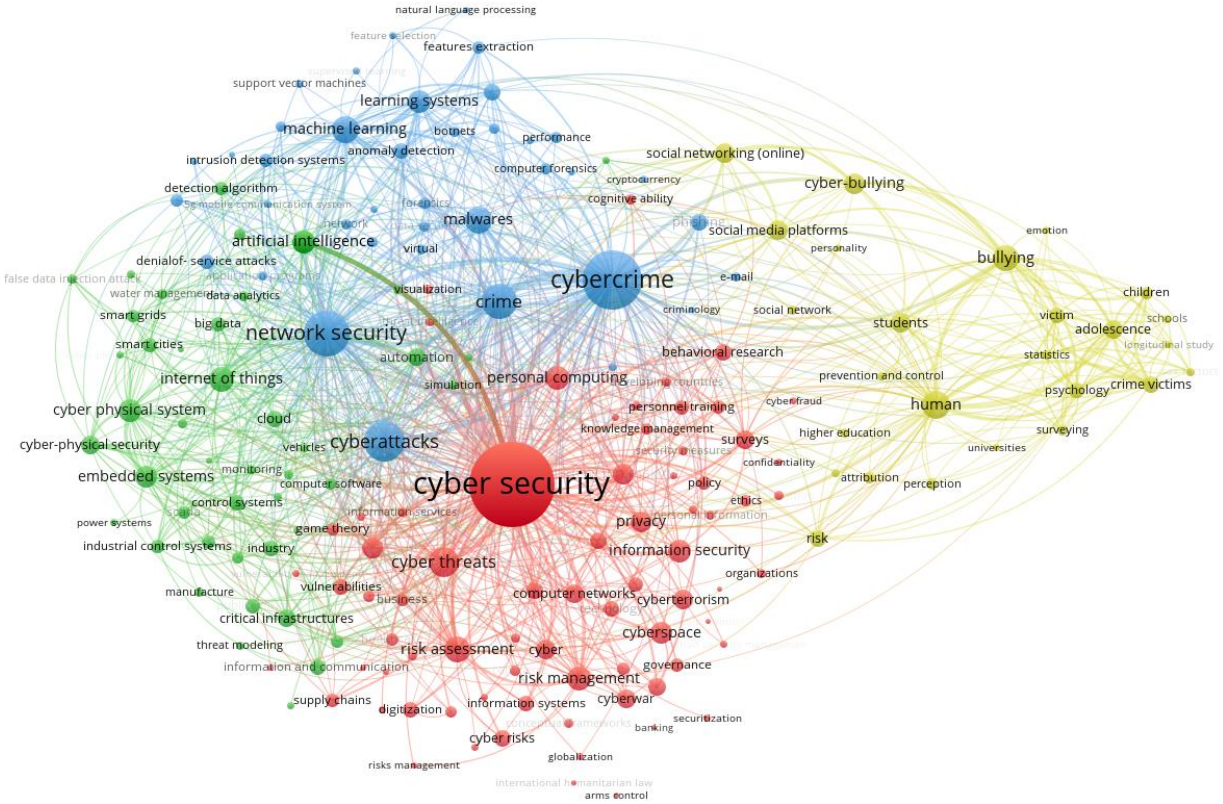


Рисунок 1.1 – Результати бібліометричного аналізу наукових праць з питань кібербезпеки в економічному вимірі у виданнях, що індексуються наукометричною базою даних Scopus

Джерело: складено автором з використанням інструментарію VOSViewerv.1.6.10

Науковий кластер 2 (синій колір) сфокусований на дослідженні та пошуку засобів та технологій ідентифікації кіберзагроз, а також протидії кібератакам (39 ключових слів). До кластеру включено наукові статті, ключовими словами яких є: кібер атаки, кібер злочин, машинне навчання, нейронні мережі, візуалізація, автоматизація, мережева безпека, кіберкриміналістика, розслідування, виявлення аномалій тощо.

Науковий кластер 3 (зелений колір) має спеціалізацію щодо дослідження об’єктів кіберзахисту, які мають пріоритетне значення в умовах діджиталізації економіки (44 ключових слів). Основними ключовими словами даного кластеру є: кіберфізична система, критична інфраструктура, хмарні технології, виробництво, «розумні» міста, управління водними ресурсами, розумні системи електропостачання, інтернет речей тощо.

Науковий кластер 4 (жовтий колір) присвячений дослідженню впливу кіберзагроз на життєдіяльність людини (26 ключових слів). Ключовими словами даного кластеру є: кібер булінг, підлітковий вік, людина, кібер жертва, психологія, соціальні мережі, емоції, студенти тощо.

Більш детальніше проаналізуємо окремі наукові праці у розрізі кожного з виділених кластерів.

Науковий кластер 1.

Найбільш цитованою працею даного кластеру є стаття [5] в якій представлено фундаментальну роль кібербезпеки у суспільстві та її критичні відмінності від інформаційної безпеки. Зокрема, кібербезпека виходить за рамки традиційної інформаційної безпеки, включаючи захист не лише інформаційних ресурсів, а й інших активів, включаючи саму особу.

Однією з найбільш поширених кібератак є фішинг, метою якого є викрадення конфіденційної персональної та фінансової інформації. Науковцями [6] запропоновано модель класифікатора фішингової електронної пошти, яка застосовує алгоритми глибокого навчання з використанням згорткової мережі графів (GCN). Експериментальні тести підтвердили, що класифікатор ідентифікував фішингові листи з точністю 98,2%.

У роботі [7] представлено результати опитуваннння керівників інформаційних служб та служб інформаційної безпеки, що дозволило виокремити основні виклики, з якими стикаються малі, середні та великі підприємства в галузі фінансових послуг щодо безпеки даних та надання відповідних інструментів і стратегій для їх захисту.

Науковий кластер 2.

На сьогодні активно впроваджують методи машинного навчання у системи захисту інформації та забезпечення кібербезпеки, які дозволяють ефективно вирішувати завдання аналізу, класифікації та прогнозування широкого класу даних. Колектив авторів [8] у своєму тематичному дослідженні довели, що блокчейн здатний захистити конфіденційну інформацію, а також усунути посередництво будь-яких установ.

У роботі [9] проаналізовано сфери практичного застосування нейронних мереж та генетичних алгоритмів в системі управління інформаційною безпекою комерційних банків. У роботі [10] побудовано фазові профілі кібершахраїв на основі аналізу моделей їх атак шляхом використання техніки розподільної семантики обробки природної мови. А. Бердюгін та П.Ревенков [11] розробили за допомогою Borland Delphi програмне забезпечення для кількісної оцінки ймовірності ризику кібератак на технології електронного банківського обслуговування.

У роботі [12] обґрунтовано необхідність посилення інформаційної безпеки серед працівників фінансових установ. Єрдон [13] запропоновано використовувати активні індикатори відстеження очей для визначення кібершахраїв з числа працівників великих компаній.

Науковий кластер 3.

Протягом останнього десятиріччя інфраструктура Інтернету речей розвивається стрімкими темпами, що трансформує традиційні системи надання суспільних послуг, організацію бізнес-процесій та побуту населення. Крім можливостей та зручностей, що привносить концепція «інтернет речей» у суспільстві, посилюється питання кіберзахисту цих технологій та пристроїв. У роботі [14] представлено детальний аналіз моделей глибокого навчання для покращення рівня кіберзахисту на систему «розумного міста», а саме машини Больцмана, обмежені машини Больцмана, мережі глибоких переконань, рекурентні нейронні мережі, згорткові нейронні мережі та генеративні змагальні мережі. Зокрема, [15] запропоновано орієнтовану на IoT інфраструктуру на основі глибокого навчання для безпечного розумного міста, де блокчейн забезпечує розподілене середовище на етапі зв’язку CPS, а програмно-визначена мережа встановлює протоколи для пересилання даних у мережі.

Науковцями С. Твенебоа-Кодуа та С. Тосун [16], М. Аркурі [17] оцінено вплив кібератак на динаміку зміни вартості цін на акції компаній залежно від їх галузевої приналежності. Доведено, що кібератака на фінансові компанії

призводить до значної волатильності їх акцій протягом тривалого періоду часу.

Науковий кластер 4.

Різке зростання використання соціальних мереж кинуло виклик традиційним суспільним структурам і перемістило значну частину міжособистісного спілкування з фізичного світу в кіберпростір. Найчастішою причиною зараження шкідливим програмним забезпеченням і порушення конфіденційності є соціальні мережі [18].

На думку П. Андреу і С. Аніфантакі [19] одним із факторів стрімкого поширення кіберзагроз є низький рівень цифрової та фінансової грамотності, а також недостатня обізнаність населення про кібератаки та їх потенційні руйнівні наслідки. Зокрема, у роботі [20] визначено набір навичок кібербезпеки не-ІТ-спеціалістів, які дозволяють зменшити ризики інформаційній безпеці компанії.

Розширюючи дослідження, проаналізуємо контекстуально-часовий блок бібліометричного аналізу (рисунок 1.2). Насиченість кольору на рисунку 1.2 змінюється від темно-синього кольору (ранні публікації) до жовтого кольору (сучасні публікації).

Отже, за результатами контекстуально-часового аналізу з питань кібершахрайств встановлено, що протягом 2017-2018 років науковці активно досліджували питання кібербулінгу, кіберзлочинів, персонального захисту в кіберпросторі. У період з 2019 по 2020 роки з розвитком електронних коштів і блокчейну основна увага почала приділятися технологіям та засобам забезпечення кібербезпеки у сучасних реаліях. Починаючи з 2021 року науковий інтерес був зміщений на дослідження кіберфізичних систем, використання технологій штучного інтелекту для протидії кібератакам, вивчення ролі кіберзахисту при реалізації «розумних» технологій для управління електропостачанням, комунальними послугами та транспортною інфраструктурою.

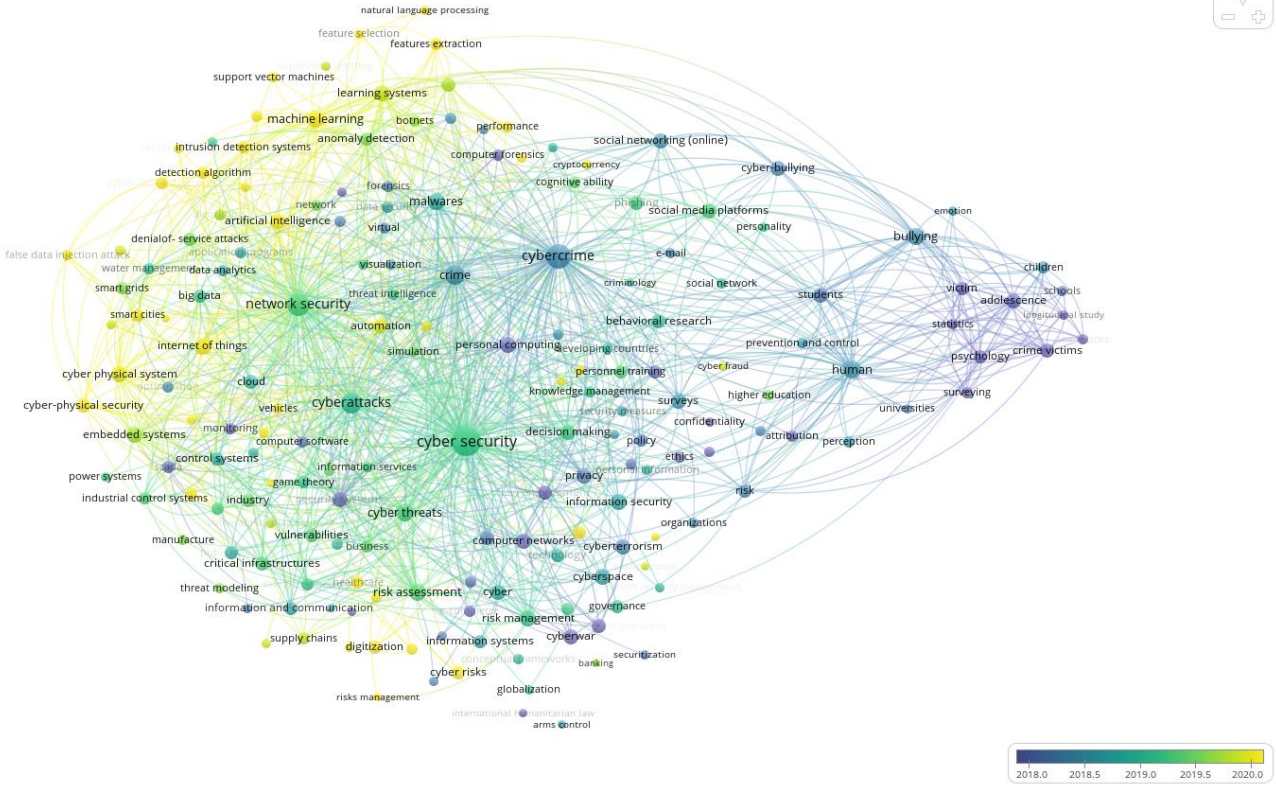


Рисунок 1.2 – Візуалізаційна карта контекстуально-часового виміру досліджень з питань кібербезпеки в контексті економічних відносин

Джерело: складено автором з використанням інструментарію VOSViewerv.1.6.10

Отже, за результатами обробки бібліографічних даних, їх візуалізації та co-occurrence-аналізу, можемо зробити наступні висновки:

–дослідження в сфері кібербезпеки є мультидисциплінарними та охоплюють широке коло питань технічного, фінансово-економічного, соціального характеру;

–кількість наукових публікацій, присвячених питанням кібербезпеки, динамічно зростає з кожним роком. Нині найбільш актуальними напрямками у даній тематиці є використання технологій штучного інтелекту та машинного навчання для вчасної ідентифікації кіберзагроз та побудови ефективної системи кіберзахисту, а також механізми посилення кіберзахисту розумних технологій в сучасній екосистемі.

–географія локація дослідницьких груп в основному зконцентрована в наукових школах та центрах таких країн як США, Великобританія Індія та Китай;

– забезпечення кіберзахисту відіграє фундаментальну роль стабільного розвитку національної економіки з урахуванням стрімких темпів впровадження цифрованих інновацій та технологій в екосистему.

З метою ефективної реалізації державної політики щодо захисту економічних агентів у кіберпросторі та понесення відповідальності за вчинення протиправних кібернетичних дій доцільно чітко визначити зміст «кіберзагроз» та інших споріднених понять: «кібершахрайство», «інтернет-злочин», «комп'ютерний злочин», «кіберризик», «кіберінцидент», «кіберзлочин», «кіберінцидент», «кібератака» тощо.

Першочергово доцільно проаналізувати зміст цього питання в чинному вітчизняному законодавстві. Основним нормативно-правовим актом, що легітимізує законодавчі дефініції у сфері кіберзахисту є Закон України «Про основні засади забезпечення кібербезпеки України» [20], в якому визначено сутність таких основних понять як «кіберзагроза», «кіберінцидент», «кібератака», «кіберзлочин». Зокрема, «кіберзагроза - наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об'єктів». На нашу думку, зазначене визначення є фрагментарним, та охоплює виключно захист кібербезпеки держави та її об'єктів, при цьому залишаючи поза увагу захист громадян країни. Водночас міжнародними стандартами ISO/IEC TS 27100:2020 визначення «кіберзагроз» [22] є більш загальним, а саме як «потенційні причини небажаного кіберінциденту, який може завдавати збитків системі, людині, суспільству, організації чи іншим суб'єктам у кіберпросторі».

Заслуговує на увагу й визначення «кіберзагроз» у роботі [23], що трактується як будь-яка подія, що може завдати шкоди національним

кіберактивам через інформаційну систему, несанкціонований доступ, знищення, розголошення, зміну інформації та/або перешкоджання наданню послуг. Компанії, які працюють у галузі цифрової безпеки, в основному розглядають кіберзагрозу як зловмисну дію, спрямована на викрадення чи пошкодження даних або порушення цифрового добробуту та стабільності суб'єкта господарювання.

На основі аналізу існуючих підходів до визначення «кіберзагроз», запропонуємо власне трактування цього поняття як «дію наявних та/або потенційно можливих дестабілізуючих факторів та умов навмисного або випадкового порушення безпеки функціонування громадянина, економічних суб'єктів та держави у кіберпросторі». Зауважимо, що кіберзагрози можуть виникати випадково (із-за низької якості аутентифікації сторони, інші слабкі місця в безпеці) або результатом спланованих дій зацікавленої сторони.

Наступною парою понять, які доволі часто ототожнюються у науковій літературі та практичній діяльності – це «кібератака» та «кіберінцидент».

Фахівцями IBM запропоновано трактувати кібератаки як будь-яку навмисну спробу викрасти, викрити, змінити, вивести з ладу або знищити дані, програми чи інші активи шляхом несанкціонованого доступу до мережі, комп'ютерної системи чи цифрового пристрою [24]. У роботі [25] кібератаки розглянуто як дії, що здійснюються країнами з метою проникнення в комп'ютери чи інформаційні мережі інших країн з метою нанесення шкоди або збою у функціонування їх систем. Фактично дане визначення враховує частину кібератак, які ініційовані урядами інших країн, залишаючи поза увагою інших суттєвих учасників – кіберзловмисники, терористичні групи, хактивісти, перснонал компанії тощо.

Визначення «кібератаки», що представлено в Законі України «Про основні засади забезпечення кібербезпеки України», є змістовним та повним, оскільки у трактуванні даного терміну зазначено інструменти й засоби здійснення кібератак, мету цих протизаконних дій у кіберпросторі та наслідки для держави й суспільства.

Кібератака зазвичай вважається передвісником кіберінциденту. Встановлення факту кіберінциденту відбувається тоді, коли кібератака фактично вплинула на конфіденційність, цілісність або доступність ІТ-системи. Суб'єкти національної системи кібербезпеки, інших державних органів, а також критичної інфраструктур, мають повідомляти про кіберінциденти у встановлений спосіб. Беручи до уваги рекомендації Європейської агенції з кібербезпеки та Європейського центру боротьби з кіберзлочинністю Європолу, урядова команда реагування на комп'ютерні надзвичайні події України, яка функціонує в складі Державної служби спеціального зв'язку та захисту інформації України (CERT-UA), сформувала перелік 10 категорій кіберінцидентів [26].

Наступною групою понять, трактування яких викликає дискусії серед науковців та практиків, є «кіберзлочин» та «комп'ютерний злочин». Зокрема, у Законі України «Про основні засади забезпечення кібербезпеки України» дані поняття ототожнюються та розглядаються як «суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України». Оскільки кіберзлочинність – будь-яке протиправне діяння, пов'язане з використанням як комп'ютерів, так і інформаційно-комунікативних засобів та технологій, тоді як «комп'ютерна злочинність» належить до правопорушень, де комп'ютер або комп'ютерні дані є основною метою злочинців [27]. І тому, поняття «кіберзлочинність» є більш ширшим порівняно з поняттям «комп'ютерна злочинність».

У Кримінальному Кодексі України зазначено, що правопорушення вважалося злочином, воно повинно містити в собі такі ознаки: кримінальна протиправність, суспільна небезпека, винність, караність [28]. Відповідно до Кримінального Кодексу України можна набути кримінальну відповідальність за:

1) злочини, що вчиняються за допомогою комп’ютерних технологій: порушення авторського права і суміжних прав (ст. 176), шахрайство (ст. 190), незаконні дії з документами на переказ, платіж. картками, банк. рахунками (ст. 200), незаконне збирання відомостей, що становлять комерційну або банківську таємницю (ст. 231), ввезення, виготовлення, збут і розповсюдження порнографічних матеріалів (ст. 301)

2) злочини у сфері використання комп’ютерів, систем та мереж: несанкціоноване втручання в роботу комп'ютерів (ст. 361), створення шкідливих програмних чи технічних засобів (ст. 361-1), несанкціоновані збут або розповсюдження інформації з обмеженим доступом (ст. 361-2), несанкціоновані дії з інформацією, яка оброблюється комп'ютерах (ст.362), порушення правил експлуатації комп'ютерів (ст. 363), перешкоджання роботі комп'ютерів шляхом розповсюдження повідомлень електрозв'язку (ст. 363-1).

Крім кримінальної відповідальності, існує й адімністративна відповідальність – особа, яка набула майно або зберегла його у себе за рахунок іншої особи без достатньої правової підстави, зобов’язана повернути потерпілому це майно (ст. 1212 Цивільного кодексу України) [29].

Кіберінцидент переходить в категорію «кіберзлочин» за умови кваліфікації правопорушення відповідно до чинного законодавства. Проте специфікою кіберзлочинів є їх транскордонний та організований характер, анонімність, постійне удосконалення способів здійснення кібератак, що ускладнює проведення як розшукових, так і процесуальних заходів [30]. Тому виникає ситуація, коли офіційна статистика щодо кіберзлочинів фактично в рази нижча, ніж реальна ситуація в країні.

Проаналізувавши сутнісні характеристики ключових понять у сфері кібербезпеки, представимо структурно-логічну схему розуміння основних кібер-понять (рисунок 1.3).

Рисунок 1.3 – Структурно-логічна схема співвідношення основних кібер-понять

Джерело: розробка автора

Для успішної ідентифікації та локалізації кіберзагроз у контексті стабільного розвитку національної економіки доцільно проаналізувати суб’єктно-об’єктну парадигму системи кіберзахисту та ініціаторів-виконавців кібератак.

Унаслідок всепроникності кіберзагроз та їх потенційний вплив на різноманітні аспекти життя й галузі господарювання, питання кіберзахисту має фундаментальне значення для стабільного розвитку національної економіки. Саме тому координація діяльності у сфері кібербезпеки здійснюється Президентом України через Раду національної безпеки і оборони України. Основними суб’єктами, які задіяні до забезпечення кібербезпеки, є: міністерства та інші центральні органи виконавчої влади, органи місцевого самоврядування; правоохоронні та інші суб’єкти оперативно-розшукової діяльності; військові формування; підприємства, установи та організації, віднесені до об’єктів критичної інфраструктури, Національний банк України;

суб’єкти господарювання та громадяни, які взаємодіють з іншими суб’єктами у кіберпросторі; міжнародні організації (НАТО, Європол, Комп'ютерна група реагування на надзвичайні ситуації (CERT, Робочої групи команд реагування на інциденти безпеки); спеціалізованими установами з кіберзахисту інших країн світу.

У Законі України «Про основні засади забезпечення кібербезпеки України» [21] визначено три об’єкта кібербезпеки:

– інформаційно-комунікаційні системи суб’єктів господарювання всіх форм власності, через які здійснюється обмін інформацією з органами державної влади та місцевого самоврядування, іншими органами публічного управління;

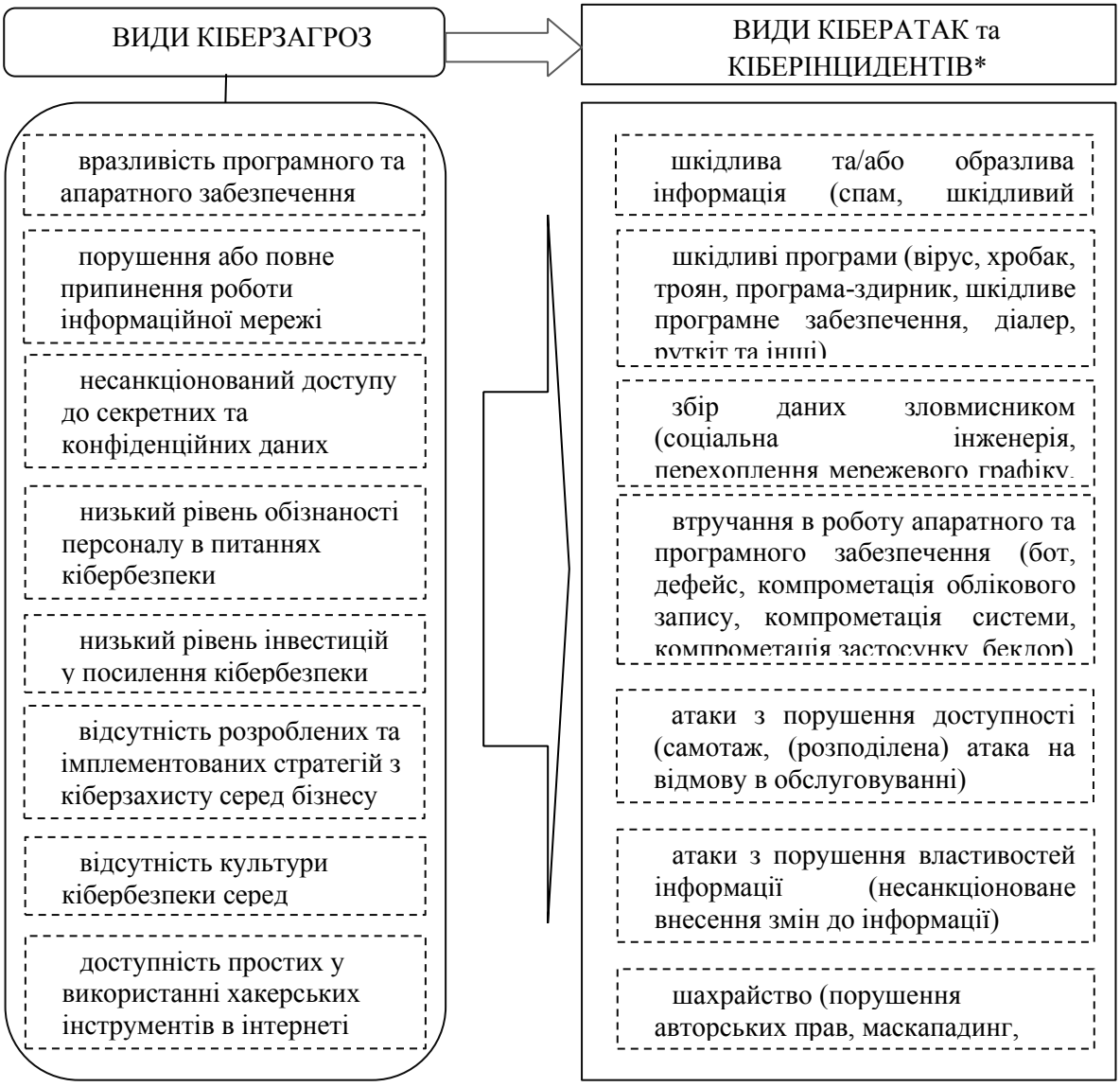
– інформаційно-комунікаційні системи, які використовуються у сферах електронного урядування, електронних державних послуг, електронної комерції та інших сферах для задоволення суспільних потреб (система охорони здоров’я, освіти, соціального забезпечення тощо);

– інформаційно-комунікаційні системи об’єктів критичної інфраструктури.

Беручи до уваги, всеохоплюючий характер кіберзагроз та їх деструктивний вплив на функціонування не лише суб’єктів господарювання, а також й життєдіяльність громадян країни, то доцільно включити до складу об’єктів кібербезпеки також інформаційно-комунікаційні засоби фізичних осіб, які використовуються ними для реалізації суспільно та життєвоважливих потреб під час використання кіберпростору.

Важливим завданням державної політики у сфері інформаційної безпеки на всіх рівнях є підвищити рівень резильєнтності до кіберзагроз, а також швидко адаптуватися до змін безпекового середовища, що сприятиме стабільному розвитку національної економіки. У рамках даного дослідження доцільно проаналізувати ключові кіберзагрози, які матимуть потенційний вплив на функціонування окремих галузей господарювання або національної економіки загалом.

У науковій літературі [31], [32] та профільних звітах компаній, які спеціалізуються на інформаційній безпеці, відбувається ототожнення «видів кіберзагроз» та «видів кібератак». Ґрунтуючись на вищенаведеному змістовному аналізі понять, на рисунку 1.4 наведені основні види «кіберзагроз», «кібератак», «кіберінцидентів».



* кібератака фактично вплинула на конфіденційність, цілісність або доступність даних

Рисунок 1.4 – Види кіберзагроз та кібератак

Джерело: складено автором на основі [33, 34, 35, 36]

Досліджуючи сутнісні характеристики кіберзагроз у системі економічних відносин, доцільно проаналізувати основних ініціаторів шахрайських дій і кіберпросторі. Базовим завданням для зловмисників є

отримання доступу до пристроїв і мереж, що дозволить в подальшому незаконно використовувати процесорну потужність комп'ютерів, викрасти або маніпулювати інформацією, вимагати отримати фінансової винагороди. Загалом кожна категорія суб'єктів кіберзагрози має власну мотивацію в здійсненні протиправної діяльності. Отже, до основних ініціаторів кібератак варто віднести [37]:

– хакерів та хактивістів, мотивами яких є цікавість, привернення уваги, помста, порушення норм соціальної справедливості тощо. Хакери зазвичай використовують вже наявний інструментарій, базові сценарії або веб-ресурси;

– злочинців та шахраїв, які націлені виключно на отримання фінансових ресурсів. Дана група шахраїв можуть розробляти власні програмні інструменти для здійснення кіберзлочину;

– держава та її шпигуни, які здійснюють незаконну діяльність з метою викрадення конфіденційних даних, збору конфіденційної інформації або порушення критичної інфраструктури іншого уряду, встановлення геополітичних інтересів, впливу на громадську думку на національному на міжнародному рівнях та інше Основними способами кібератак національних урядів є шпигунство або кібервійна;

– інсайдерів, мотивами зловмисної діяльності яких є отримання фінансової винагороди, збір та передача конфіденційної інформації, завдати шкоду діловій репутації організації [38]. Крім цього, суб'єкти внутрішньої загрози не завжди мають зловмисні наміри. Деякі завдають шкоди своїм компаніям через людську помилку – через мимовільне встановлення шкідливого програмного забезпечення або втрату пристрою, виданого компанією, який кіберзлочинець знаходить і використовує для доступу до мережі.

Незалежно від ініціатора кібератак вони є постійною загрозою в усьому світі як для урядів, компаній, так і для окремих осіб. Публічне визнання порушення зазвичай несе значну репутаційну шкоду на додаток до втрат через викрадені дані та інтелектуальну власність, пошкоджені системи. До основних

наслідків кіберінцидентів можно віднести: крадіжка грошових коштів як економічних суб'єктів; несанкціоноване розголошення особистої інформації третіх осіб; репутаційні втрати, спричинені розкриттям комерційної таємниці, викрадення конфіденційної інформації або її шифрування, додаткові витрати на розслідування інциденту та відновлення після кібератак; втрата довіри стейкхолдерів до суб'єктів господарювання; витрати на юридичні позови від постраждалих клієнтів. У сучасних умовах для захисту економічних суб'єктів у кіберпросторі доцільно інвестувати кошти у придбанні складніших засобів захисту для забезпечення належного рівня інформаційної безпеки, а також постійно удосконалювати навички та знання існуючого персоналу та здійснювати пошук кваліфікованих спеціалістів для вирішення поточних та майбутніх прогалин у системі інформаційної безпеки економічних суб'єктів.

Підсумовуючи, зазначимо, що кібербезпека є безперервним і вкрай актуальним процесом для стабільного функціонування економічних суб'єктів з урахуванням цифрових трансформацій. У сучасних умовах розвитку вкрай важливо для суб'єктів кібербезпеки вчасно запобігати кібератакам на ранньому етапі та здійснювати комплекс превентивних заходів для підвищення рівня їх кіберзахисту.

1.2 Сучасні тенденції поширення кіберзлочинності в Україні та світі

Цифровізація сучасного світу, розвиток інформаційних технологій, поширення Internet, комп'ютерні мережі, використання кіберпростору, наразі виступають основою сучасного суспільства. Оскільки використання Інтернету та підключених до мережі комп'ютерів зростає, а також відбувається інтенсивний розвиток інноваційних технологій, що в кінцевому підсумку сприяє зростанню кіберзагроз. Зростання кількості кібератак є результатом стрімкого використання інноваційних цифрових технологій у діяльності економічних суб'єктів, появою фінтех компаній, а також збільшенням попиту на цифрові фінансові продукти та розвитком електронної комерції із-за

пандемії COVID-19. Зокрема, під час пандемії кількість порушень у сфері кібербезпеки серед FinTech компаній в середньому збільшився на 17% [39].

У 2020 році збитки від кіберзлочинів у США оцінювалися на рівні 4,2 млн дол США, що вдвічі більше порівняно з 2018 роком (2,7 млн дол США). При цьому впродовж останніх років виробнича сфера та сфера фінансових послуг були та залишаються основними таргетами для кіберзлочинців. IBM щорічно визначає індекс загроз (X-Force Threat Intelligence Index), який відображає ландшафт кіберзагроз у світі (таблиця 1.2).

Таблиця 1.2 – Рейтинг вразливості сфер діяльності до кіберзлочинів у період з 2018 по 2022 рр.

Сфери діяльності	2018	2019	2020	2021	2022	Зміна, 2022/2018
Фінансові послуги	19	17	23	22,4	18,9	0
Виробництво	10	8	17,7	23,2	24,8	+15
Енергетика	6	6	11,1	8,2	10,7	+5
Роздрібна торгівля	11	16	10,2	7,3	8,7	-2
Професійні послуги	12	10	8,7	12,7	14,6	+3
Охорона здоров'я	6	3	6,6	5,1	5,8	0
Медіа	8	10	5,7	2,5	0,5	-8
Транспорт	13	13	5,1	4	3,9	-9
Освіта	6	8	4	2,8	7,3	+1
Інші	9	9	7,9	12	4,8	+4

Джерело: складено автором на основі [40]

На основі даних про атаки та інциденти з порушення інформаційної безпеки з керованих мереж X-Force, а також про публічно розкриті кіберзлочини фахівцями IBM встановлено, що протягом 2018-2022 років найбільший приріст зафіксовано по сфері виробництва, при цьому зменшився інтерес кіберзлочинців до транспортної галузі та медіа. Варто відзначити, що протягом останніх п’яти років сфера фінансових відносин має високий рівень вразливості до кіберзлочинів. Це пояснюється тим, що банки – це фактично «кровоносна система» національної економіки, через яку здійснюється обслуговування інтересів держави (виконання державного і місцевих бюджетів, отримання міжнародної допомоги, надання субсидій тощо), суб’єктів господарювання різних галузей економіки, а також громадян

суспільства. З урахуванням цього, банківські установи акумулюють значну за обсягом інформацію від своїх клієнтів. У разі порушення інформаційної безпеки фінансових установ конфіденційні дані можуть бути використані для здійснення протиправної діяльності або продані на темних веб-майданчиках, що може призвести до втрати ділової репутації як фінансових установ, так і їх клієнтів [41].

У таблиці 1.3 представлено найбільші кіберзлочинні угруповання, які атакують фінансові установи в світі.

Таблиця 1.3 – Найбільші кіберзлочинні угруповання, які здійснюють атаки на фінансові установи, у світі

Назва	Рівень складності кібератак	Жертви	Особливості кібератак
Money Taker (Російська Федерація)	використовує власні інструменти кібератак, шкідливе програмне забезпечення, яке працюватиме і після перезавантаження, здійснює налаштування загальнодоступ-них інструментів для своїх потреб.	банки, компанії, що надають послуги та/або технології фінансовим установам	більше 20 успішних атак на банки, фінансові установи та юридичні компанії в США, Великобританії та Росії.
Carbanak (Російська Федерація)	використовує шкідливе програмне забезпечення, яке надає широкий спектр можливостей: авторизація, зчитування даних банківських карток, особистої інформації.	Банки, фінансові компанії, компанії з електронної комерції	понад 300 успішних атак на банки, фінансові установи та роздрібних торговців, у тому числі на систему Oracle
Lazarus Group (Північна Корея)	має потужні можливості, а саме технології ухилення корпоративних систем кібер-захисту, трирівневі атакуючі сервери, зашифровані комунікації.	Банки, фінансові компанії, урядові структури	атака на Sony Pictures, розробник програми, атака на SWIFT, Центральний банк Бангладеша та інші.

Джерело: складено автором на основі [42]

Кіберзагрози досягли безпрецедентного розмаху, що спричинено дією наступних потенційних чинників:

– потужний розвиток електронних обчислювальних машин, мобільних пристроїв дозволив підвищити швидкість обробки даних та отримати постійний доступ до фінансових послуг. Так, у 2019 році у світі

нараховувалося близько 5,2 млрд мобільних користувачів, що охоплює 67% населення світу, тоді як у 2015 р.– 4,66 млрд, 2010 р. – 3,219 млрд осіб [43].

– збільшення кількості пристроїв, підключених до мережі Інтернет. У 2019 р. 39% громадян ЄС, які користувалися Інтернетом, зіткнулися з проблемами безпеки у віртуальному просторі. Значення даного показника значною мірою коливається в різних державах-членах: більше 50% у Великобританії та 10% у Литві [44].

– неможливість відслідкувати територію / країну здійснення кібератаки, що дозволяє анонімно здійснювати інтернаціональну протиправну діяльність;

– збільшення кількості користувачів соціальних мереж, які містять персональні дані. Відповідно до Emarketer рівень проникнення соціальних мереж у світі у 2020 р. становив 41,9% від загальної кількості населення або 3,23 млрд користувачів. Для порівняння: у 2017 р. – 2,3 млрд користувачів або 31,2%, у 2013 р. – 1,6 млрд користувачів або 22,8% [45];

– використання застарілого та неліцензійного програмного забезпечення;

– стрімке зростання технологій Інтернет речей, які використовуються у різних системах господарювання та побуті. Зокрема, у країнах Європейського Союзу у 2021 р. майже третина суб'єктів господарювання користуються на практиці можливостями Інтернет речей, тоді у Австрії – 51% компаній від загального обсягу, Словенія – 49%, Фінляндія та Швеція – по 40% [46];

– збільшення питомої ваги бізнес-процесів, які передаються на управління третім особам, у тому числі й закордон;

– використання хмарних технологій для зберігання та передачі даних. У 2021 році У 2021 році у середньому 41% підприємств ЄС використовували хмарні обчислення, переважно для електронної пошти та зберігання файлів. Проте між країнами можна спостерігати значні відмінності: у Швеції (75 % підприємств використовували хмарні обчислення), Фінляндії (75 %), Нідерландах (65 %), Данії (65 %), тоді як у Румунії (14 %), Болгарії (13 %), Польща (29%), Україна (10,1%) [47]. Проте протягом 2023-2030 рр. очікується

збільшення використання хмарних технологій у бізнес-процесах приблизно на 14,1% [48];

– розширене використання робототехніки або алгоритмів для здійснення автоматичної торгівлі та розробки додатків. У 2019 році на європейських виробничих компаніях на 10 000 працівників припадає 500 роботів, США – 293 роботи на 10 000 працівників, а в Сінгапурі – 918 на 10 000 працівників [49];

– збільшення використання віртуальних та цифрових валют. Сумарна капіталізація ринку криптовалют всього за одне десятиліття збільшилася до позначки 1.2 трильйона дол.

Забезпечення кібербезпеки є динамічним процесом швидкого реагування та адаптації до швидко змінюваних кіберзагроз, що обумовлено використанням нових технологій зловмисниками при реалізації кібератак. Проаналізуємо основні патерни кіберзагроз у світі протягом 2005-2020 років. Джерелом даних про кіберінциденти слугувала база даних Європейського репозитарію кіберінцидентів (European Repository of Cyber Incidents, EuRepoC) [50]. Дослідження ландшафту кіберзагроз у світі проведено на основі 785 кіберінцидентів, які призвели до значущих змін у стабільному функціонування національної економіки (атака на центральні банки, державні установи, міжнародні компанії тощо). При цьому зазначимо, що щодня відбувається близько 4000 нових кібератак. Кожні 14 секунд компанія стає жертвою атаки програм-вимагачів, що може призвести до катастрофічних фінансових втрат [51]. Дані щодо кіберінцидентів згруповані за наступними характеристиками: за країною-ініціатором, за країною-жертвою, типом кібератак (шпіонаж, відмова в обслуговуванні, пошкодження або знищення інформації, дефейс, фінансова крадіжка, доксинг, саботаж), за сферою госпдарювання (публічний та приватний сектор, військовий сектор, громадянське суспільство), за датою проведення кібератаки (у розрізі років, місяців, днів тижня, днів). Динаміка аналізованих кіберінцидентів по роках представлена на рисунку 1.5.

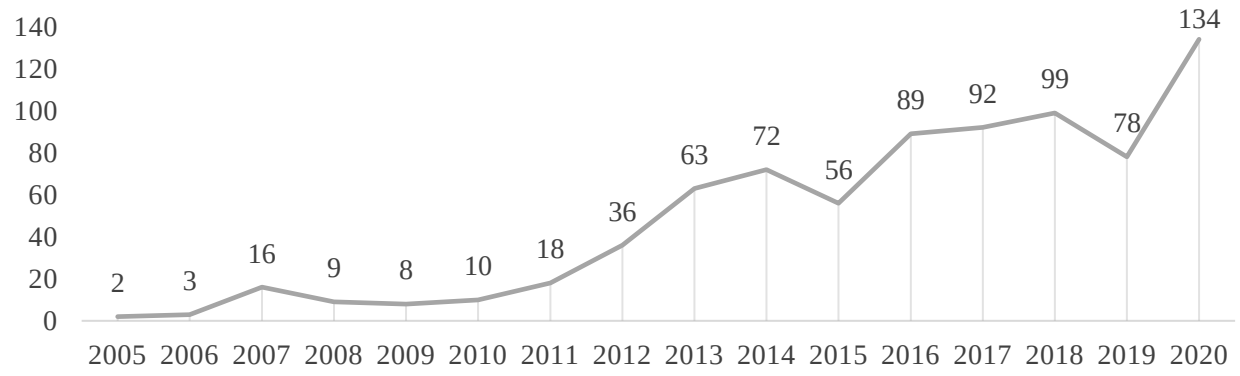


Рисунок 1.5 – Динаміка значущих кіберінцидентів у світі протягом 2005-2020 років

Джерело: складено автором на основі база даних Європейського репозитарію кіберінцидентів [51]

Дані рисунку 1.5 наочно демонструють, що у 2020 році у світі було зафіксовано 134 кіберінциденти, які ймовірно заподіяли суттєвої шкоди об’єктам критичної інфрастурктури, що майже вдвічі більше порівняно з 2019 роком (78 кіберінцидентів).

У період з 2005 по 2020 роки 41,8% кіберіндидентів здійснено резидентами з Китаю, при цьому 40% з них були направлені на об’єкти критичної інфраструктури у сфері публічного управління та 36% – на об’єкти приватного сектору (рисунок 1.6).

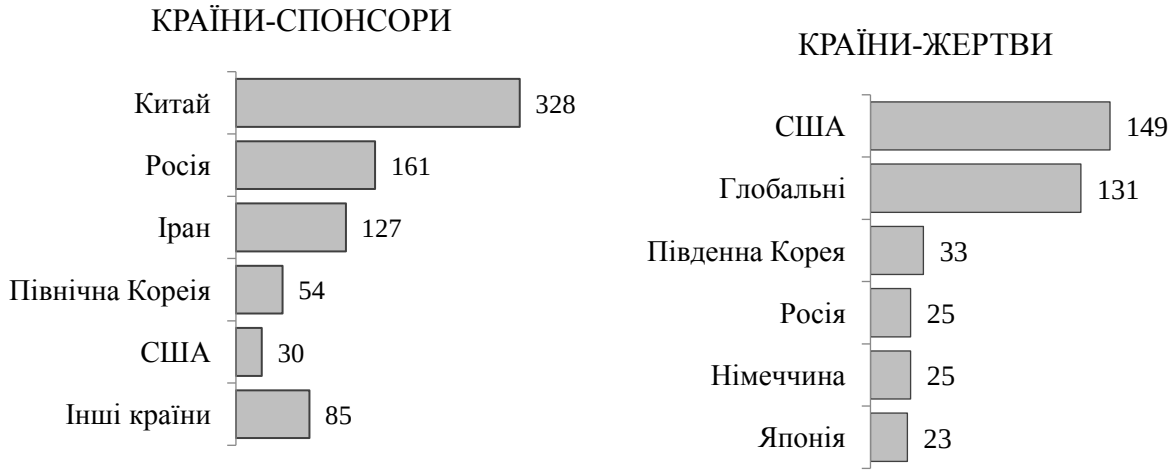


Рисунок 1.6 – Топ країни, які є найбільшими спонсорами та жертвами кібернцидентів у світі

Пріоритетними країнами-цілями для Китаю є США (питома вага – 25%), світ (13%). Крім Китаю, найбільшими спонсорами кібератак у світі є росія та Іран, сукупно на ці три країни припадає 78,5% від всіх кіберінцидентів. Рівень концентрації кіберінцидентів у розрізі країн-жертв є значно нижчим порівняно з країнами-спонсорами. Так, найбільше атакуються у кіберпросторі об'єкти критичної інраструктури США (149 інцидентів або 18,9% від загального обсягу).

Стосовно України, то протягом 2005-2020 рр. зафіксовано 22 кіберінциденти, ініціатором яких виступала росія, 10 з яких були направлені на злам урядових структур та 9 – на об'єкти приватного сектору.

Переважна більшість кібератак були здійснені у формі шпіонажу, що передбачає здійснення розвідувальної діяльності для збору конфіденційної інформації у публічному та приватному секторах (рисунок 1.7).

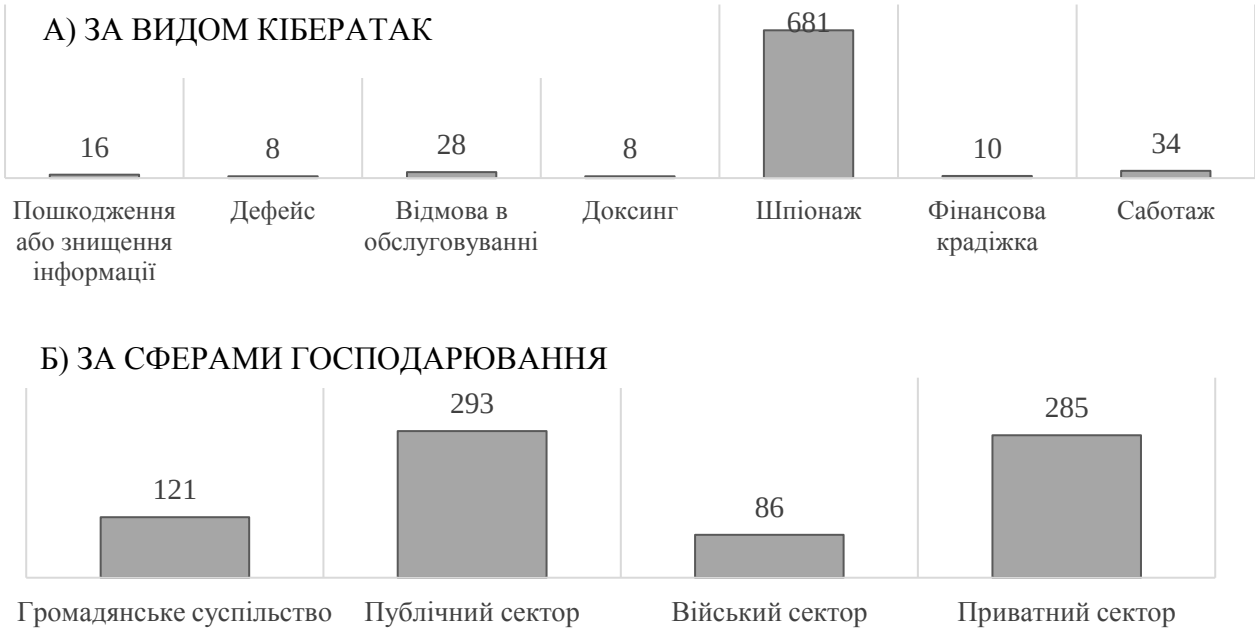


Рисунок 1.7 – Структура кіберінцидентів у період з 2005 по 2020 роки (а – за видом кібератак; б – за сферами господарювання)

У межах даного дослідження також вирішено більш детальніше проаналізувати дати здійснення кібератак (рисунок 1.8). Це обумовлено тим,

що у багатьох працях [52] вже емпірично доведено, що часова концентрація є стійкою ознакою різних видів злочинності.

Дані, що представлені на рисунку 1.8, засвідчують про достатню однорідність розподілу кіберіндицентів. Найбільша кількість кіберінцидентів у світі була реалізована у вівторок, при цьому фіксуючи збільшення даних протиправних дій у такі дні як 19,24,25. Найменша кількість кіберінцидентів була здійснена у суботу. Стосовно місяців, то найбільш інтенсивно кіберзлочинці здійснювали атаки у травні, жовтні, червні та липні. Щодо днів тижня, то збільшення кількості кіберінцидентів фіксувалося 16 та 28 числа.

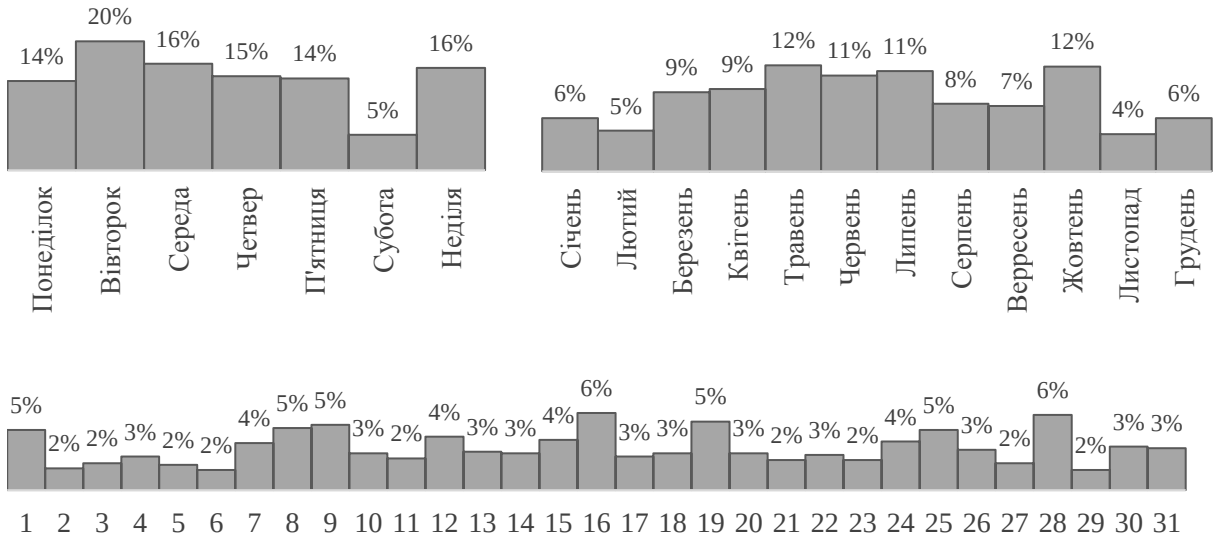


Рисунок 1.8 – Часова концентрація кіберзагроз у розрізі місяців, днів тижня та днів

Для виявлення, знешкодження, мінімізації та попередження кіберризиків, науково-практичним світовим співтовариством вживаються різноманітні заходи для боротьби з можливими кібератаками. А ефективність вжиття механізмів протидії кібершахрайствам напряму залежить, в першу чергу, від виявлення закономірностей здійснення кібератак з досвіду країн світу.

На сьогоднішній день при виявленні певних закономірностей фахівцями проводиться обробка баз даних великих розмірів, що потребує розробки

певних моделей, здатних опрацьовувати суттєві інформаційні ресурси. А одним з найефективніших вирішень цього питання є використання асоціативних правил та їх пристосування до вивчення досліджуваних питань.

Асоціативні правила – це дуже потужна технологія, що дозволяє виявляти взаємозв'язки між пов'язаними подіями або елементами. Вони описуються у вигляді: $X \to Y, X \cap Y \to \emptyset$. При чому, будь-яке асоціативне правило можна представити двома основними характеристиками [55]:

- 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;

- 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.

Асоціативні правила, що виникають при аналізі багатовимірних даних класифікуються за наступними видами:

– міжвимірні асоціаціативні правила, тобто правила між атрибутами різних вимірів (формула 1.1) [56]:

$$(A_I^x \in D_I) \wedge \ldots \wedge (A_J^y \in D_J) \to A_K^z \in D_K, \qquad (1.1)$$

де I, J, K - певні індекси розмірів, що включені в асоціативне правило, причому I, J, K = 1 ...n; де n - кількість розмірів,

$D_I - I^{th}$ - є розмірністю;

x, y, z - певні атрибути розмірності, при чому x, y, z = 1 ... m_i;

m_i - кількість атрибутів I^{th}-виміру;

A_I^X - певний атрибут I^{th}-виміру.

– внутрішньовимірної асоціаціативні правила, тобто правила асоціації в межах одного виміру (формула 1.2) [56]:

$$(A_I^x \in D_I) \wedge \ldots \wedge (A_I^y \in D_I) \rightarrow (A_I^z \in D_I) \wedge \ldots \wedge (A_I^v \in D_I), \quad (1.2)$$

де I = 1 ...n;

n - кількість розмірів;

x, y, z, v - певні атрибути розмірності, при чому x, y, z, v = 1 ... m_i;

m_i - загальна кількість атрибутів I^{th}-виміру.

– гібрідні асоціативні правила, тобто можливі залежності між вимірами, при чому певні операнди можуть представляти атрибути одного виміру (формула 1.3):

$$(A_I^x \in D_I) \wedge \ldots \wedge (A_J^y \in D_J) \rightarrow (A_J^v \in D_J) \wedge \ldots \wedge (A_K^z \in D_K), \quad (1.3)$$

Формування асоціативних правил використовується для наступного: виявлення та вивчення вразливих місць у досліджуваних процесах, що дозволить у майбутньому на ранніх етапах мінімізувати, чи, навіть, уникнути додаткових матеріальних витрат; надання можливості керівній ланці визначити необхідну оптимальну кількість потрібних ресурсів та їх ефективний розподіл; автоматичної ідентифікації, виправлення, вирішення проблемних аспектів та вдосконалення досліджуваних процесів.

Розглянемо отримані закономірності здійснення кібератак в країнах ЄС на основі використання асоціативних правил у вигляді наступної послідовності етапів [57]:

1 етап. Формування вхідної структури даних здійснення кібератак на основі застосування методу логічного узагальнення. На даному етапі проводиться збір та систематизація даних щодо характеристик кібератак протягом 2005-2020 рр. (таблиця 1.4).

Таблиця 1.4 – Фрагмент вхідної структури даних здійснення кібератак

Назва	Дата	Країна-жертва	Країна-ініціатор	Вид кіберзлочину	Сфера галузі
Атака на Міністерство закордонних справ Австрії	2020	Австрія	Росія	шпіотаж	публічна
Атака на Польський університет військових досліджень	2020	Польща	Росія	дефейс	публічна
Атака на Польський університет військових досліджень	2020	Польща	Росія	дефейс	військова
Атака на центрально європейські аерокосмічні та оборонні компанії	2020	ЄС	Північна Корея	шпіотаж	приватна
Атака на RedDelta	2018	Італія	Китай	шпіотаж	Публічна
…	…	…	…	…	…
Атака на Avast	2019	Чехія	Китай	шпіотаж	приватна
Атака на аналітичні центри США та Європи	2019	ЄС	Росія	шпіотаж	приватна
Атака на Міністерство закордонних справ Чехії	2019	Чехія	Росія	шпіотаж	публічна

Таким чином, на основі зібраних даних щодо здійснення кібератак можна констатувати наступне. До країн, які постраждали від кібератак відносяться Австрія, Польща, Італія, Німеччина, Литва, Латвія, Чехія, Норвегія, Франція, Бельгія, Люксембург, Нідерланди, Швейцарія, Болгарія, Туреччина3, Данія, Швеція, Данія, Фінляндія, Угорщина, Іспанія. До країн-ініціаторів здійснення кібератак на території Європейського Союзу віднесено Росію, Китай, Північна Корея, В’єтнам, Ліван, Іран, Казахстан, США. Крім цього, виявлено наступні типи кібератак: шпіонаж, пошкодження або знищення інформації, дефейс, саботаж, доксинг, фінансова крадіжка, відмова в обслуговуванні. Дані кібератаки були здійснені на об’єкти різних сфер: публічний та приватний сектор, військовий сектор, громадянське суспільство.

Наступним кроком є проведення поглибленого аналізу кібератак на території Європейського Союзу на основі використання асоціативних правил. Для реалізації даного етапу використано програмний продукт STATISTICA 10. Отримані результати представимо у вигляді рисунку 1.9.

	Summary of association rules (cyber-operations (EC).sta) Min: support = 20,0%, confidence = 10,0% Max. size of an itemset = 10					
	Body	==>	Head	Support(%)	Confidence(%)	Lift
1	Governmen	==>	Russia	40,3225	64,1025	1,13553
2	Russia	==>	Governmen	40,3225	71,4285	1,13553
3	Governmen	==>	Russia, Espionage	30,6451	48,7179	1,11870
4	Espionage	==>	Russia, Governmen	30,6451	36,5384	0,90615
5	Espionage, Governmer	==>	Russia	30,6451	59,3750	1,05178
6	Russia	==>	Espionage, Governmer	30,6451	54,2857	1,05178
7	Russia, Governmen	==>	Espionage	30,6451	76,0000	0,90615
8	Russia, Espionage	==>	Governmen	30,6451	70,3703	1,11870
9	Espionage	==>	Russia	43,5483	51,9230	0,91978
10	Russia	==>	Espionage	43,5483	77,1428	0,91978
11	Germany	==>	Espionage	24,1935	88,2352	1,05203
12	Espionage	==>	Germany	24,1935	28,8461	1,05203
13	China	==>	Espionage	24,1935	93,7500	1,11778
14	Espionage	==>	China	24,1935	28,8461	1,11778
15	Private sector	==>	Espionage	35,4838	84,6153	1,00887
16	Espionage	==>	Private sector	35,4838	42,3076	1,00887
17	Governmen	==>	Espionage	51,6129	82,0512	0,97830
18	Espionage	==>	Governmen	51,6129	61,5384	0,97830

Рисунок 1.9 – Результати аналізу кібератак на території Європейського Союзу за допомогою асоціативних правил

Джерело: розрахунки автора

На основі даних, отриманих шляхом побудови асоціативних правил, представлених на рисунку 1.9, можна зробити наступні висновки: в 77,14% випадків шпіонаж здійснюється зловмисниками з Росії, у 88,24% - з Німеччини, у 93,75% - з Китаю. Встановлено, що 84,62% шпіонажу спостерігається у галузі приватного сектору, 82,05% - у публічній сфері. При цьому частка спостережень, для яких шпіонаж здійснюється з Росії, складає 43,55%. Частка спостережень, для яких шпіонаж здійснюється як з Німеччини, так і з Китаю, становить 24,19% вибірки. У 76% випадків шпіонаж здійснюється зловмисниками з Росії в сфері публічної діяльності. Переходячи до аналізу частоти виявлених випадків здійснення кібератак, що є суттєвим доповненням до наведених вище асоціативних правил (рисунок 1.10).

	Frequent itemsets computed (cyber-operations (EC).sta) Min: support = 10,0%, confidence = 10,0% Max. size of an itemset = 10			
	Frequent itemsets	Number of items	Frequency	Support(%)
1	(Espionage	1,00000	52,0000	83,8709
2	(Government	1,00000	39,0000	62,9032
3	(Military	1,00000	9,0000	14,5161
4	(EU)	1,00000	7,0000	11,2903
5	(Private sector	1,00000	26,0000	41,9354
6	(Civil society	1,00000	9,0000	14,5161
7	(Germany	1,00000	17,0000	27,4193
8	(France)	1,00000	7,0000	11,2903
9	(Espionage, France	2,00000	7,0000	11,2903
10	(Espionage, Germany	2,00000	15,0000	24,1935
11	(Espionage, Private sector, Germany	3,00000	7,0000	11,2903
12	(Espionage, Government, Germany	3,00000	8,0000	12,9032
13	(Espionage, Civil society	2,00000	7,0000	11,2903
14	(Espionage, Private sector	2,00000	22,0000	35,4838
15	(Espionage, Government, Private secto	3,00000	6,0000	9,6774
16	(Espionage, EU	2,00000	7,0000	11,2903
17	(Espionage, Military	2,00000	7,0000	11,2903
18	(Espionage, Government	2,00000	32,0000	51,6129
19	(Government, Germany	2,00000	9,0000	14,5161
20	(Government, Civil society	2,00000	6,0000	9,6774
21	(Government, Private sector	2,00000	7,0000	11,2903
22	(Government, Military	2,00000	7,0000	11,2903
23	(Private sector, Germany	2,00000	8,0000	12,9032

Рисунок 1.10 – Частота виявлених випадків здійснення кібератак

Аналіз рисунку 1.10 дозволяє констатувати, що найбільша частка кіберзлочинів (62,90%) відбувається в державних структурах, наступна за частотою галузь – приватний сектор (41,94%). Найменші частки кіберзлочинів відбуваються у військовій та суспільній сферах і становить 14,52%.

Графічне представлення причинно-наслідкових зв’язків між кібератаками проведено на основі застосування методів візуалізації та графічного дизайну. У рамках даного етапу побудовано граф виявлених на другому етапі асоціативних правил, представлений на рисунках 1.11-1.12, які дозволяють 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).

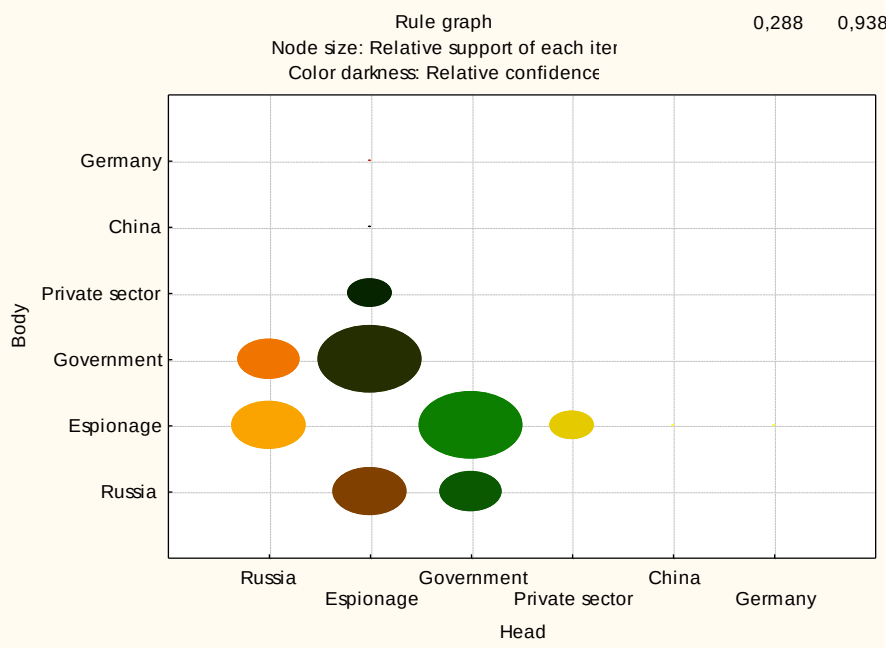


Рисунок 1.11 – Граф асоціативних правил

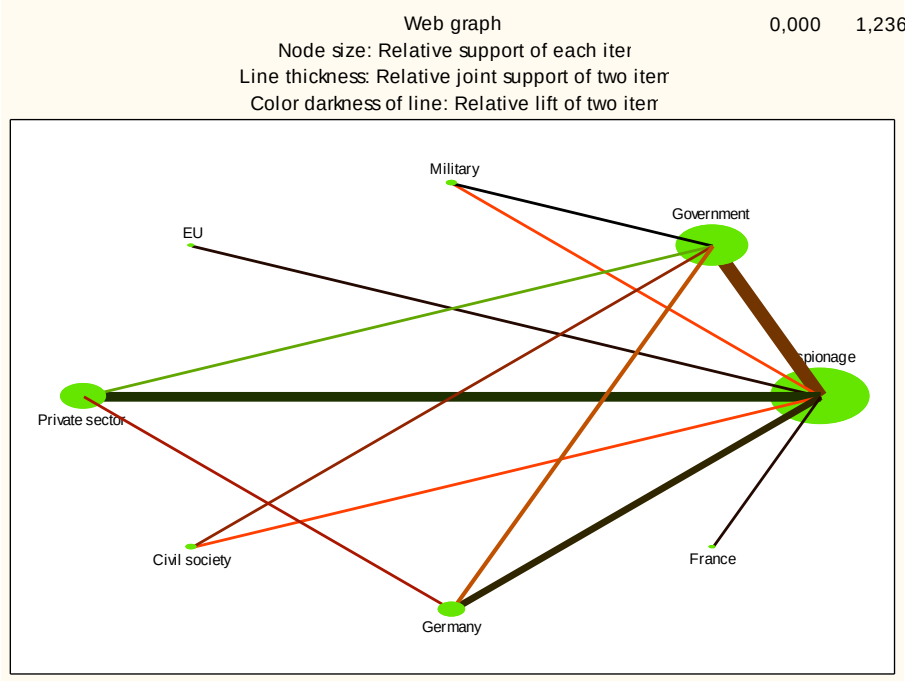


Рисунок 1.12 – Веб-граф підтримки виявлених асоціативних правил в розрізі здійснення кібератак в межах країн ЄС

Переходячи до аналізу рисунку 1.11 та 1.12 то найбільшою за частотою виявлених випадків здійснення кібератак (83,87%) є шпіонаж. Серед країн, які стали жертвами кіберзлочинів, необхідно відмітити Німеччину, на частку якої

припадає 27,42% випадків, в той час як для Франції даний показник на рівні 11,29% (що відбулось за рахунок шпіонажу). У середньому 11,29% країн ЄС стали постраждали від здійснення кібератак у період з 2005 по 2020 рр.

Зазначимо, що кібератаки, в яких втрачається особиста, комерційна, фінансова інформація, спричиняють вагомі збитки учасників фінансово-економічної системи. А за відсутності новаційних, удосконалених заходів протидії таким кіберзлочинам, масштаби даних протиправних діянь у світі неспинно зростає, і завдає серйозних загроз економічній безпеці країн.

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. Це в подальшому надасть можливість країнам приймати ефективні рішення для передбачення кіберзагроз, протидії кібератакам та забезпечення національної безпеки країн ЄС.

Забезпечення безпеки інформаційних технологій установ та їх баз даних є постійно зростаючим викликом для топ-менеджменту установ, так і національного регулятора. Хоча програмне забезпечення поступово стає все більш безпечним, а розробники створюють нові підходи до кібербезпеки, зловмисники також удосконалюють технології здійснення зловмисних діянь. Найбільш поширеними формами здійснення кібератак є програма – фішинг, експлуатація загальнодоступних програм, програми-здирники. У таблиці 1.5 наведено найбільш поширені способи здійснення кібератак у світі у розрізі сфер господарювання.

Дані таблиці 1.5 засвідчують, способи здійснення атак кіберзлочинцями не різноманітними залежно від приналежності об'єкта до відповідної сфери господарювання. Проте найбільш розповсюдженою формою кібератаки є різні види фішингу, який передбачає викрадення важливої інформації за допомогою електронних листів із застосуванням соціальної інженерії та обману.

Таблиця 1.5 – Найбільш поширені види кібератак у розрізі сфер господарювання

Сфери діяльності	Види кібератак	Географія поширення
Фінансові послуги	Фішингові вкладення – 53% атак, експлуатація загальнодоступних програм – 18%, а фішингові посилання – 12%.	Європа – 33% усіх атак, Азіатсько-Тихоокеанський регіон – 31%, Латинська Америка – 15%, Північна Америка – 10%, Близький Схід і Африка – 10%.
Виробництво	Фішингові вкладення – 28%, експлуатація загальнодоступних програм – 28%, атаки з боку зовнішніх віддалених служб – 14%, фішингові посилання –10.	Азіатсько- Тихоокеанський регіон – 61%, Європа – 14%, Північна Америка – 14%, Латинська Америка – 8%, Близький Схід і Африка – 4%.
Енергетика	Фішингові посилання – 20%, атаки з боку зовнішніх віддалених служб – 20%. ботнети – 19%, а програми-здирники та BEC-атаки – 15%	Північна Америка – 46%, Європа – 23%, Латинська Америка – 23%, Азіатсько- Тихоокеанський регіон – 4%, Близький Схід і Африка – 4%.
Роздрібна торгівля	Програми-здирники – 18%, бекдори – 18%, BEC-атаки – 18%, «хробак» –10.	Північна Америка – 39%, Латинська Америка – 39%, Європа – 22%.
Професійні послуги	Програми-здирники – 18%, бекдор-атаки – 18%, експлуатація загальнодоступних програм – 23%, атаки з боку зовнішніх віддалених служб –23%, фішингові вкладення та дійсні локальні облікові записи – 15%	Європа – 47%, Північна Америка – 33%, Азіатсько- Тихоокеанський регіон – 10%, Близький Схід і Африка – 7%. Латинська Америка – 3%.

* експлуатація загальнодоступних програм виникає коли зловмисник використовує вразливість загальнодоступної програми для отримання несанкціонованого доступу до цільової мережі; BEC-атаки – компроментація ділової електронної пошти

Джерело: розроблено автором на основі [40]

Одним з найбільш розповсюджених методів для викрадення грошей безпосередньо з рахунків компаній - це BEC-афера (business email compromise). Принцип роботи BEC-афери наступний: кіберзлочинець вводить в оману співробітника компанії, який має доступ до конфіденційної інформації, з вимогою зробити переказ коштів на рахунок, який начебто належить клієнту, або контрагенту компанії, проте кошти перенаправляються на рахунок кримінальної організації. У 2020 році збитки від BEC-афер та EAC-афер (компрометація облікового запису, email account compromise), які є аналогом BEC-афер для фізичних осіб, у США оцінені на рівні 1,8 млрд дол

США (або 36% від загальної суми збитків від кіберзлочинів), тоді як у 2019 році – 1,7 млрд дол США (або 48,57% від загальної суми) [58].

Динамічна цифровізація економіки робить банківські та небанківські фінансові установи більш вразливими до кіберзлочинності. По-перше, банки – це фактично «кровоносна система» національної економіки, через яку здійснюється обслуговування інтересів держави (виконання Державного і місцевих бюджетів, отримання міжнародної допомоги, надання субсидій тощо), суб'єктів господарювання різних галузей економіки, а також громадян суспільства. По-друге, доволі поширеною практикою є передача управління інформаційною системою фінансових установ спеціалізованим компаніям, що вимагає від останніх здійснення додаткових заходів щодо захисту своїх ресурсів від кібератак.

Шахрайство у банківській сфері є достатньо різноманітним. Існує безліч видів шахрайства в банківській сфері і серед них можна виділити чотири основні групи. Першу групу утворюють схеми розкрадання грошових коштів шляхом їх отримання за підробленими банківськими документами і цінними паперами, наприклад: розрахунковими чеками, векселями, депозитними сертифікатами і т.д. Другу групу складають розкрадання грошових коштів вкладників і інвесторів, отриманих під обіцянку виплати високих відсотків або виконання інших зобов'язань (за принципом фінансових пірамід чи інших «пірамід»). Суть такого шахрайства полягає в тому, що зобов'язання перед новими вкладниками виконуються на першому етапі за рахунок надходження коштів нових інвесторів і їх обману. До наступної групи відноситься кредитне шахрайство, яке представляє собою розкрадання грошових коштів шляхом отримання різних кредитів з наданням підробленої документації. В цьому випадку обман полягає в: поданні завідомо неправдивих відомостей; поданні завідомо недостовірних відомостей; поданні завідомо неправдивих і недостовірних відомостей. Даний вид шахрайства в банківській сфері є найпоширенішим і зловмисники використовують його частіше за інших. Потенційний позичальник надає банку або іншому кредитору завідомо

неправдиві і (або) недостовірні відомості у вигляді документів, що підтверджують його уявну платоспроможність, які в подальшому повинні бути ретельно перевірені кредитною організацією. Четверту групу утворює шахрайство з використанням банківських карт (чужих або підроблених кредитних, розрахункових чи інших платіжних). Даний вид шахрайства є порівняно новим і активно розвивається.

Найбільш розповсюдженими шахрайствами у сфері фінансових послуг є саме методи соціальної інженерії. Ці методи спираються на здійснення психологічного впливу на жертву з метою підштовхування останньої до здійснення необхідних для зловмисників дій. За даними ЄМА (Української міжбанківської асоціації членів платіжних систем) на кінець 2018 р. близько 70% – це шахрайські операції, пов’язані з соціальною інженерією та здійснені за допомогою мережі Інтернет [59]. Банкоматне шахрайство складає приблизно четверту частину від усієї кількості шахрайських операцій та має тенденцію до зниження своєї частки у зв’язку з удосконаленням банківських технологій захисту банкоматів. Протягом 2017–2018 рр. значно зменшилася й до цього незначна частка шахрайських операцій через POS-термінали та дещо зросла частка випадків шахрайства при дистанційному банківському обслуговуванні. Не варто виключати і можливостей співучасті в тій чи іншій шахрайській схемі з боку працівників банків. Це – ще один з напрямків «роботи» шахрайських схем. Працівники банку можуть не лише надавати зловмисникам дані клієнтів за грошову винагороду, але й бути активними учасниками схем, а подекуди – й організаторами. Величезним сегментом шахрайства є технологічний сегмент. Тобто, за допомогою застосування технологічних рішень зловмисники отримують дані клієнтів банків, або й безпосередній доступ до банківських рахунків жертв (цю «задачу» виконують, як правило, фішингові технології) [60]. З 2016 р. VISA і MasterCard ввели принцип нульової відповідальності в Україні та на глобальному рівні. Це означає, що якщо власник карт цих платіжних систем став жертвою шахраїв і зміг це довести, то банки повинні компенсувати йому кошти. Це ставить

проблему запобігання шахрайським операціям з боку банків. Отже, даний аспект є позитивним для клієнтів банків не лише з огляду на можливість компенсації навіть безнадійно втрачених коштів, а й, що найбільш важливо, з огляду на те, що інвестиції банків у технології захисту від шахрайства є вже об'єктивно обумовленими інтересами самих банків. Отже, постійна робота з боку банків над удосконаленням систем безпеки транзакцій та систем захисту даних своїх клієнтів буде тривати й надалі.

Щодо можливостей протидії шахрайським операціям, варто відзначити, що існує два напрямки: технічний та соціальний, в залежності від сфери застосування шахрайських технологій. Технічний шлях запобігання банківському шахрайству активно удосконалюється, постійно розвиваються технічні інструменти безпеки банківських транзакцій, розкриваються нові шахрайські схеми. Цей напрямок «приречений» на постійну еволюцію. З наведених вище даних щодо тенденцій шахрайства можна бачити, що невдовзі варто очікувати збільшення обсягу шахрайства в сфері електронної комерції. Також вкрай важливо звернути увагу на сегмент мобільних і безконтактних платежів.

З урахуванням постійно зростаючих загроз у кіберпросторі, національні регулятори розробляють стратегії щодо підвищення кіберзахисту національних економік, обмінюються кращими практиками протидії кіберзагрозам з іншими країнами та розробляються міжнародні рекомендації для підвищення кіберрезильєнтності економічних суб'єктів та урядових структур. Для моніторингу поточного стану готовності України та інших країн світу до запобігання кіберзагрозам та управління кіберінцидентами проаналізуємо Національний індекс кібербезпеки (National Cyber Security Index), що розраховується естонською Академією електронного урядування. У 2018 році експертами було оцінено кібербезпеку в Україні на рівні 58% з поміж 100%, проте вже у 2022 році – 75% за рахунок удосконалення кібербезпеки у військовій сфері, кіберзахисту у сфері надання цифрових послуг, системи управління кіберризиками тощо.

На сьогодні кіберзахист критично важливих об’єктів інфраструктури є пріоритетним завданням для держави, оскільки використання шкідливих програм є елементом сучасної стратегії гібридної війни. За даними Оперативного центру реагування на кіберінциденти Державного центру кіберзахисту Державної служби спеціального зв’язку та захисту інформації України у 2022 році отримано 58 млрд подій, які опрацьовані за допомогою засобів моніторингу. За результатами первинного та вторинного аналізу підозрілих подій для інформаційної безпеки у 2022 році офіційно зареєстровано 415 кіберінцидентів, що в 2,8 рази більше порівняно з 2021 роком [61]. За підсумками І кварталу 2023 року зафіксовано та оброблено безпосередньо аналітиками безпеки 202 кіберінциденти, що у 5 разів більше порівяно з аналогічним періодом 2022 року (40 кіберінцидентів) [62].

Отже, збільшення частоти та масштабів кібершахрайств у фінансовому секторі може призвести до несанкціонованого розповсюдження персональної фінансової інформації про клієнтів, отримання значних збитків та репутаційних втрат фінансовими установами і навіть мати системні наслідки для економіки країни, оскільки загрози можуть швидко поширюватися по різних секторах економіки. За цих умов вчасно ідентифікувати ознаки кібершахрайства та швидко прийняти рішення щодо їх нейтралізації.

1.3 Методичний підхід до визначення детермінантів поширення кібершахрайств

Карантинні заходи, спричинені пандемією, спровокували збільшення розрахунків в мережі Інтернет, зростання обсягів електронних фінансових послуг, нарощення використання криптовалют та альткоїнів як платіжного засобу та інвестиційного інструменту. Дані тенденції вказують на прискорення темпів цифровізації економіки та трансформації підходів до організації бізнес-процесів. За цих умов цифрова трансформація відкриває як нові можливості для підвищення ефективності суб’єктів господарювання і

зниження їх витрат за рахунок оптимізації транзакцій, так і загрози для стабільного їх функціонування – поширення кібератак та зростання частоти їх здійснення. У 2020 році в Україні зафіксовано близько мільйона випадків, пов'язаних з кіберзагрозами, сформовано достатньо сприятливі умови для "відмивання" брудних грошей (67 позиція з поміж 141 країни світу за даними Базельського індексу протидії легалізації), що має значущий дестабілізаційний ефект на функціонування національної економіки та враховуючи швидке перетікання із одної галузі господарювання до іншої, що в кінцевому підсумку виступає загрозою для національної безпеки держави [41]. Не зважаючи на велику кількість публікацій, присвячених окресленій проблематиці, у науковій літературі досі не здійснена спроба формалізації детермінант поширення кібер шахрайства у сфері фінансових послуг.

За результатами виконання науково-дослідної роботи розроблено науково-методичний підхід до формалізації факторів стрімкого поширення кібершахрайств на основі методів машинного навчання SVM. Реалізація запропонованого підходу передбачає покрокове виконання наступних етапів:

– збір та обробка статистичних даних, що характеризують обсяг кіберзлочинних операцій у розрізі різних методів здійснення кібератаки;

– приведення вхідних показників до єдиного співтавного вигляду;

– побудова інтегрального індексу кіберзагроз методом групового врахування аргументів Івахненка, де в якості опорної функції використовується адитивно-мультиплікативна згортка суми сум квадратів стандартизованих значень вхідних індикаторів;

– визначення потенційних факторів впливу на поширення кібершахрайств та збір по ним статистичних даних;

– визначення специфічних особливостей інтегрального індексу кіберзагроз та детермінант поширенння кіберзагроз на основі методів описової статистики;

– побудова SVM-моделі машинного навчання двох типів (epsilon-SVM regression та nu-SVM regression) в розрізі чотирьох специфікацій опорних

векторів: лінійні, поліноміальні, радіально-базисні функції (RBF) та сигмоподібні.

Перший етап передбачає проведення збору та систематизації статистичних даних, що характеризують фактичні кібератаки, проведені у 2020 році. Об'єктом дослідження слугували 21 країна Європи. Джерелом первинної інформації слугували дані компанії Comparitech [63]. Для відображення інтенсивності здійснення кібератак у розрізі країн Європи використано наступні індикатори: частка мобільних пристроїв, заражених шкідливим програмним забезпеченням, % (I_1); частка користувачів, атакованих вірусами троян через інтернет банкінг, % (I_2); частка користувачів, атакованих мобільними троянами-вимагателями, % (I_3); частка користувачів, атакованих банківським шкідливим програмним забезпеченням, % (I_4); частка користувачів, атакованих троянськими програмами-вимагателями, % (I_5); частка комп'ютерів, заражених принаймні однією атакою зловмисного програмного забезпечення (в Інтернеті), % (I_6); частка комп'ютерів, які стикаються принаймні з однією локальною атакою шкідливого програмного забезпечення, % (I_7); частка мобільних користувачів, атакованих через веб-джерела, % (I_8); частка атак на Telnet протокол, % (I_9); частка атак з боку криптомайнерів, % (I_{10}); частка атак на SSH протокол, % (I_{11}); частка спам-листів за країною відправника (за рік), % (I_{12}); частка країн, на які націлені зловмисні розсилки (щороку), %(I_{13}); частка комп'ютерів, атакованих фішингом (щорічно), % (I_{14}); загальна кількість виявлених шкідливих файлів, пов'язаних із Covid 19 (I_{15}).

Зведена статистична інформація щодо випадків кібершахраства у розрізі різних методів для країн Європи представлена у додатку А (таблиця А.1), а основні результати подано в таблиці 1.6.

На основі аналізованих у таблиці 1.6 видів кібератак, зауважимо, що найбільшими країнами-жертвами у 2020 році були Іспанія, Португалія та Латвія, тоді як найменша кількість кібератак зафіксована у таких країнах як Данія, Швеція та Ірландія. Зокрема, 19,73% комп'ютерів у Португалії були

атаковані таким інтернет-шахрайством як фішинг, тоді як у Данії – лише 3,26%. Перехід на дистанційний режим роботи та інтенсивне користування електронними послугами, спричиненого пандемією COVID-19, призвів до збільшення масштабів кібершахрайства у світі. Щодо країн Європи, то найбільша кількість виявлених шкідливих файлів, пов'язаних із пандемією Covid 19 виявлена у Іспанії, Італії та Німеччині.

Таблиця 1.6 – Інформація щодо стану кіберзлочинності в європейських країнах у 2020 році у розрізі методів та способів їх здійснення

	Топ-3 країн з найвищими показниками			Топ-3 країн з найнижчими показниками		
	1	2	3	1	2	3
Частка мобільних пристроїв, заражених шкідливим програмним забезпеченням (I_1)	Румунія (5,04%)	Іспанія (4,31%)	Словаччина (3,5%)	Фінляндія (1,06%)	Данія (1,33%)	Німеччина (1,63%)
Частка користувачів, атакованих банківським шкідливим програмним забезпеченням (I_4)	Португалія (0,9%)	Греція (0,5%)	Болгарія (0,5%)	Ірландія (0,1%)	Данія (0,1%)	Угорщина (0,2%)
Частка комп'ютерів, заражених принаймні однією атакою шкідливого програмного забезпечення (I_6)	Латвія (7,31%)	Франція (6,71%)	Іспанія (5,92%)	Данія (1,33%)	Ірландія (1,35%)	Швеція (1,435%)
Частка атак з боку криптомайнерів (I_{10})	Латвія (0,73%)	Болгарія (0,56%)	Словаччина (0,5%)	Данія (0,11%)	Німеччина (0,12%)	Румунія (0,14%)
Частка спам-листів за країною відправника (I_{12})	Німеччина (10,97%)	Франція (5,97%)	Нідерланди (4,00%)	Данія (0,07%)	Словаччина (0,19%)	Швеція (0,19%)
Частка комп'ютерів, атакованих фішингом (I_{14})	Португалія (19,73%)	Франція (17,9%)	Бельгія (16,4%)	Данія (3,26%)	Швеція (3,35%)	Ірландія (3,42%)
Загальна кількість виявлених шкідливих файлів, пов'язаних із Covid 19 (I_{15})	Іспанія (1825476)	Італія (578779)	Німеччина (314459)	Латвія (78)	Болгарія (301)	Словаччина (450)

Джерело: розрахунки автора

Другий етап передбачає визначення інтегрального індексу кіберзагроз методом групового врахування аргументів Івахненка, який ґрунтується на застосуванні індуктивних алгоритмів математичного моделювання багатопараметричних даних. В основі даного методу лежить рекурсивна селективна процедура здійснення відбору математичних моделей, на базі яких формалізуються більш складні моделі, при цьому точність та адекватність процесу моделювання поступово збільшується на кожному наступному кроці шляхом ускладнення вихідної моделі. Для побудови інтегрального індексу в якості опорної функції розглядається сума сум квадратів стандартизованих значень вхідних індикаторів.

Крок 2.1. Проведення стандартизації вхідних індикаторів на основі застосування програмного пакету Statistica інструментарію Data/ Standartize. В основі даного підходу обробки вхідних даних лежить метод Z-нормалізації, який передбачає зважження відхилення фактичного рівня кожного показника від середнього рівня за множиною розглянутих країн до середньоквадратичного відхилення, за наступною формулою 1.4:

$$k_{cj} = \frac{I_{cj} - \underline{I_j}}{\sigma_j} \qquad (1.4)$$

де k_{cj} – стандартизоване значення j-го індикатора поширення кіберзагроз в розрізі с-ої країни;

I_{cj} – фактичне значення j-го індикатора поширення кіберзагроз в розрізі с-ої країни;

$\underline{I_j}$ – середнє арифметичне значення j-го індикатора поширення кіберзагроз на множині значень розглянутої сукупності країн;

σ_j – середнє квадратичне відхилення в розрізі j-го індикатора поширення кіберзагроз на множині значень розглянутої сукупності країн.

Використовуючи формулу 1.4, розраховано стандартизовані значення показників, що характеризують рівень кіберзагроз в країнах Європи, подано в таблиці 1.7.

Таблиця 1.7 – Стандартизовані значення детермінант поширення кіберзагроз станом на 2020 рік

	I1	I2	I3	I4	I5	I6	I7	I8	I9	I10	I11	I12	I13	I14	I15
AUS	-0,7	-0,9	-0,5	-0,5	-0,4	-0,2	-0,3	-0,7	-0,9	-0,5	-0,5	-0,4	-0,2	-0,3	-0,7
BEL	-0,6	-0,6	-0,5	-0,5	-0,5	1,1	-0,2	-0,6	-0,6	-0,5	-0,5	-0,5	1,1	-0,2	-0,6
BGR	-0,4	1,5	-0,5	-0,4	-0,5	0,1	-0,3	-0,4	1,5	-0,5	-0,4	-0,5	0,1	-0,3	-0,4
HRV	-0,6	0,3	-0,5	-0,1	-0,5	-0,4	-0,3	-0,6	0,3	-0,5	-0,1	-0,5	-0,4	-0,3	-0,6
DNK	-0,7	-1,2	-0,6	-0,6	-0,6	-1,6	-0,3	-0,7	-1,2	-0,6	-0,6	-0,6	-1,6	-0,3	-0,7
FIN	-0,7	0,3	-0,6	-0,5	-0,6	-0,8	-0,3	-0,7	0,3	-0,6	-0,5	-0,6	-0,8	-0,3	-0,7
FRA	0,0	-0,9	2,5	1,7	-0,2	1,4	-0,3	0,0	-0,9	2,5	1,7	-0,2	1,4	-0,3	0,0
DEU	0,3	-1,1	3,0	3,6	2,4	-0,3	0,4	0,3	-1,1	3,0	3,6	2,4	-0,3	0,4	0,3
GRC	3,4	1,1	-0,5	-0,5	0,1	1,0	-0,3	3,4	1,1	-0,5	-0,5	0,1	1,0	-0,3	3,4
HUN	-0,3	0,7	-0,4	-0,3	-0,5	0,8	-0,3	-0,3	0,7	-0,4	-0,3	-0,5	0,8	-0,3	-0,3
IRL	-0,7	-0,7	-0,4	-0,5	-0,6	-1,5	-0,3	-0,7	-0,7	-0,4	-0,5	-0,6	-1,5	-0,3	-0,7
ITA	1,8	-0,5	0,4	-0,2	1,6	0,9	1,1	1,8	-0,5	0,4	-0,2	1,6	0,9	1,1	1,8
LVA	-0,6	2,5	-0,6	-0,3	-0,5	0,4	-0,3	-0,6	2,5	-0,6	-0,3	-0,5	0,4	-0,3	-0,6
NLD	-0,3	-0,7	0,8	0,9	-0,5	-1,2	-0,3	-0,3	-0,7	0,8	0,9	-0,5	-1,2	-0,3	-0,3
POL	0,2	0,4	-0,3	0,2	-0,3	0,3	-0,3	0,2	0,4	-0,3	0,2	-0,3	0,3	-0,3	0,2
PRT	-0,6	0,8	-0,5	-0,5	0,2	1,8	-0,3	-0,6	0,8	-0,5	-0,5	0,2	1,8	-0,3	-0,6
ROU	0,2	-1,0	-0,4	-0,4	-0,2	-1,0	-0,3	0,2	-1,0	-0,4	-0,4	-0,2	-1,0	-0,3	0,2
SVK	-0,6	1,1	-0,6	-0,5	-0,6	0,4	-0,3	-0,6	1,1	-0,6	-0,5	-0,6	0,4	-0,3	-0,6
ESP	0,4	0,3	-0,1	0,4	2,9	0,5	4,1	0,4	0,3	-0,1	0,4	2,9	0,5	4,1	0,4
SWE	-0,3	-0,7	-0,3	-0,5	-0,6	-1,5	-0,3	-0,3	-0,7	-0,3	-0,5	-0,6	-1,5	-0,3	-0,3
GBR	0,7	-0,6	0,7	-0,2	-0,2	-0,2	-0,3	0,7	-0,6	0,7	-0,2	-0,2	-0,2	-0,3	0,7

Джерело: розрахунки автора

Крок 2.2 Агрегування стандартизованих рівнів індикаторів поширення кіберзагроз до єдиного інтегрального показника методом групового врахування аргументів Івахненка, тобто розрахунку суми сум квадратів стандартизованих значень вхідних індикаторів за формулою 1.5:

$$IK_c = \sum_{j=1}^{J} \sum_{j=1}^{J} \left(k_{cj}\right)^2 \quad (1.5)$$

де IK_c - інтегральний індекс кіберзагроз в розрізі с-ої країни.

Результати обчислень за формулою 1.5 візуалізуємо на рисунку 1.13, де представимо динаміку індексу кіберзагроз у розрізі розглянутих країн Європи станом на 2020 рік, у тому числі з урахуванням впливу пандемії на захищеність інформаційного простору.

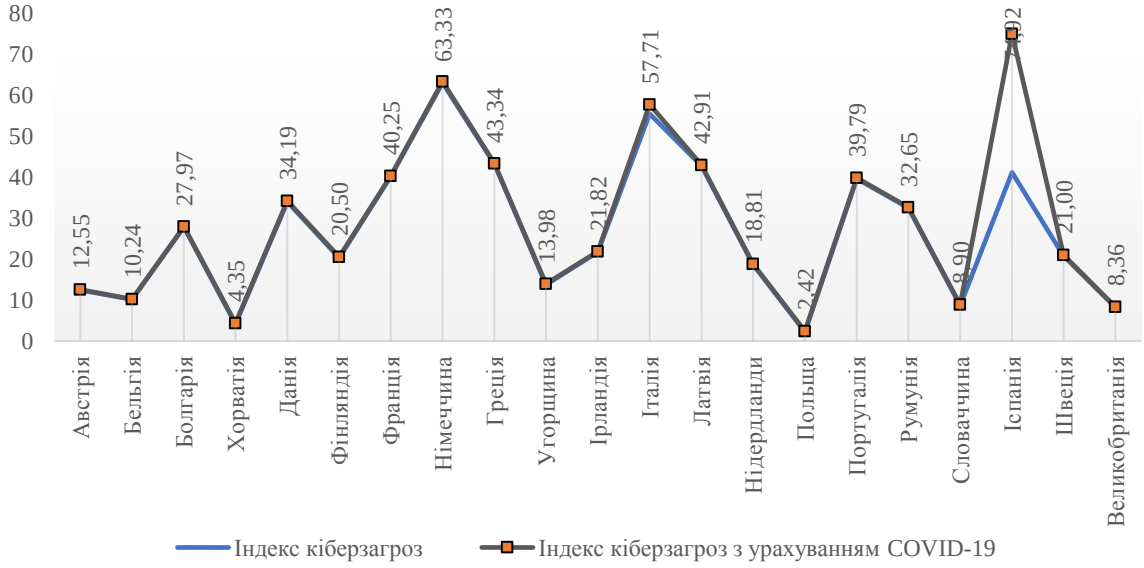


Рисунок 1.13 - Динаміка індексу кіберзагроз у розрізі країн Європи, а також з урахуванням впливу пандемії Covid 19 станом на 2020 рік

Джерело: розрахунки автора

Проведені розрахунки засвідчили, що нерівномірність здійснення кібератак у розрізі країн Європи, оскільки індекс кіберзагроз у 2020 році варіюється від 2,4 ум. од до 74,9 ум.од. На основі агрегування 15 вхідних індикаторів, що характеризують різні способи здійснення шахрайства в інформаційному просторі, отримано, що найбільший рівень кіберзагроз у 2020 році спостерігається у таких країнах як Іспанія (74,9 ум.од.), Німеччина (63,3 ум.од.), Італія (57,7 ум.од.), Латвія (42,9 ум.од.) та Франція (40,2 ум.од.).

З метою детального аналізу динаміки інтегрального оцінювання рівня кіберзагроз у розрізі країн Європи розглянемо таблицю частот (рисунок 1.14). Так, найбільша кількість країн серед розглянутої множини характеризуються рівнем індексу кіберзагроз в межах від 0 до 10, від 10 до 20 та від 20 до 30 (по 4 країни, тобто 19,05% вибірки відповідно), що свідчить про низький рівень досліджуваного показника. Лише незначна кількість країн (всього 3 серед досліджуваної множини країн Європи) з рівнями від 50 до 60, від 60 до 70 та від 70 до 80, що свідчить про високий рівень кібернебезпеки.

	Frequency table: cyber threat index (cyber threat index SVM.sta) K-S d=,15528, p> .20; Lilliefors p<,15					
Category	Count	Cumulative Count	Percent of Valid	Cumul % of Valid	% of all Cases	Cumulative % of All
-10,0000<x<=0,00000(	0	0	0,0000(	0,000(	0,0000(	0,000(
0,000000<x<=10,0000	4	4	19,0476:	19,047(	19,0476:	19,047(
10,00000<x<=20,0000	4	8	19,0476:	38,095:	19,0476:	38,095:
20,00000<x<=30,0000	4	12	19,0476:	57,142(	19,0476:	57,142(
30,00000<x<=40,0000	3	15	14,2857.	71,428(	14,2857.	71,428(
40,00000<x<=50,0000	3	18	14,2857.	85,714:	14,2857.	85,714:
50,00000<x<=60,0000	1	19	4,7619(	90,476:	4,7619(	90,476:
60,00000<x<=70,0000	1	20	4,7619(	95,238:	4,7619(	95,238:
70,00000<x<=80,0000	1	21	4,7619(	100,000(	4,7619(	100,000(
Missing	0	21	0,0000(		0,0000(	100,000(

Рисунок 1.14 – Таблиця частот індексу кіберзагроз на множині розглянутих країн світу станом на 2020 рік

Джерело: розрахунки автора

Третім етапом запропонованого підходу є визначення детермінант поширенння кіберзагроз. У межах даної роботи для математичної формалізації детермінант поширення кібершахрайств запропоновано використати наступні змінні:

– частка населення, яка користується послугами онлайн банкінгу (Z1);

– індикатор розвитку мобільного широкосмугового доступу, розрахований як середнє зважене нормалізованих показників: рівень покриття 4G (25%), рівень використання мобільного широкосмугового доступу (25%) і рівень готовності впроваджувати 5G (50%) (Z2);

– індикатор рівня навичок в Інтернеті, розрахований як середнє зважене нормалізованих показників: базові цифрові навички (33%), Вищі базові навички роботи в Інтернеті (33%) і базові навички програмного забезпечення (33%) (Z3);

– індикатор поглиблених навичок та вмінь розрахований як середнє зважене нормалізованих показників: частка фахівців у сфері інформаційно-комунікаційних технологіях (33%), частка фахівців-жінок у сфері інформаційно-комунікаційних технологіях (33%) і кількість випускників зі сфери інформаційно-комунікаційних технологій (33%) (Z4);

– індикатор онлайн діяльності розраховується як середньозважена сума нормованих показників: новини (16,6%), музика, відео та ігри (16,6%), відео на вимогу (16,6%), відеодзвінки (16,6%), соціальні мережі (16,6%)), і проведення онлайн-курсів (16,6%) (Z5);

– індикатор ділової онлайн активності, що визначається як середньо зважена сума нормалізованих показників: обмін електронною інформацією (16,7%), соціальні медіа (16,7%), великі дані (33,3%) і хмарні технології (33,3%) (Z6).

Станом на 2020 рік значення вищеперерахованих показників у розрізі країн Європи подано в таблиці 1.8.

Провести більш детальний ґрунтовний детермінант поширення кіберзагроз дозволить побудова діаграма (рисунок 1.15), яка свідчить про найбільшу волатильність індикатора Z1 (частка населення, яка користується послугами онлайн банкінгу), значення якого за 21 країнами світу коливається в межах від 11 до 95. В той же час, найменшу волатильність має індикатор Z5 (індикатор онлайн діяльності), що приймає значення в межах від 33 до 69. Зазначені висновки можна також зробити, проаналізувавши описові статистики детермінант поширення кіберзагроз у розрізі країн Європи станом на 2020 рік, представлені на рисунку 1.15.

Таблиця 1.8 – Детермінанти поширення кіберзагроз кіберзагроз на множині розглянутих країн світу станом на 2020 рік

	Banking	Mobile broadband	Internet User Skills	Advanced Skills and Development	Activities online	Business digitisation
	Z1	Z2	Z3	Z4	Z5	Z6
AUS	71,54	50,15	64,49	48,97	41,82	35,75
BEL	78,85	34,16	58,29	42,49	48,29	67,34
BGR	12,62	31,33	25,80	42,03	40,90	20,54
HRV	58,75	33,70	54,31	44,00	53,85	39,57
DNK	93,53	57,93	71,29	51,26	65,33	65,57
FIN	95,20	76,59	76,46	80,42	69,34	79,35
FRA	73,33	51,50	54,74	40,13	33,39	46,93
DEU	65,72	65,31	66,92	45,92	45,46	38,95
GRC	40,33	33,02	47,25	22,33	49,34	34,48
HUN	58,11	61,13	45,91	37,76	53,92	21,78
IRL	74,59	50,82	53,32	59,48	53,39	64,66
ITA	48,05	63,36	40,08	24,83	40,11	34,11
LVA	83,10	56,13	41,30	28,74	45,53	30,45
NLD	94,36	34,45	78,17	50,15	63,36	75,68
POL	58,76	46,32	40,93	33,61	41,46	25,03
PRT	55,67	35,42	51,80	23,73	48,53	40,50
ROU	11,35	40,73	27,23	39,08	35,70	25,41
SVK	66,11	48,81	50,15	33,47	40,57	33,25
ESP	60,50	49,39	57,06	38,06	56,31	43,44
SWE	86,59	49,43	71,90	71,55	68,78	62,11
GBR	81,30	46,77	74,46	51,55	62,98	58,61

Джерело: розроблено автором на основі [64]

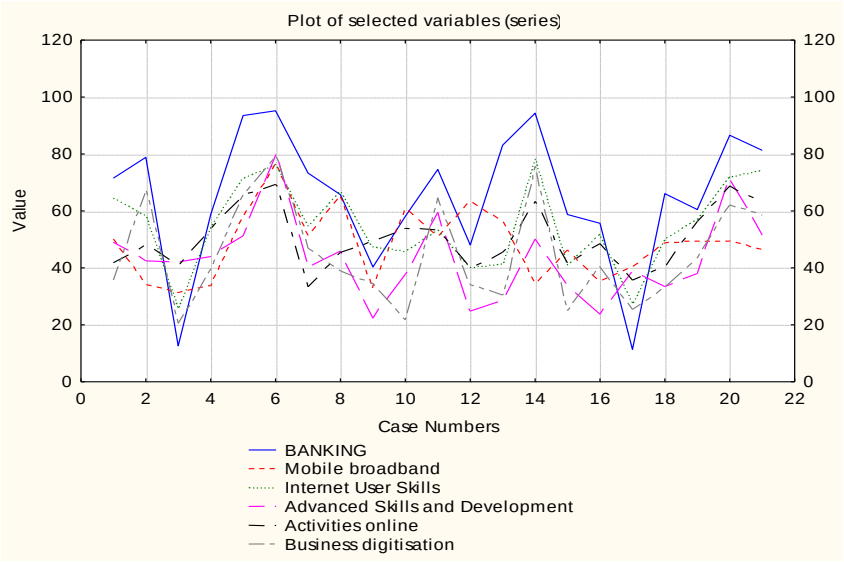


Рисунок 1.15 – Варіація значень детермінант поширення кіберзагроз на множині розглянутих країн світу станом на 2020 рік

Джерело: розрахунки автора

Variable	Descriptive Statistics (cyber threat index SVM.sta)								
	Valid N	Mean	Median	Mode	Sum	Minimum	Maximum	Std.Dev.	Coef.Var.
Banking	21	65,1594	66,1054	Multipl	1368,34	11,3482	95,2009	23,2336	35,6565
Mobile broadband	21	48,4027	49,3892	Multipl	1016,45	31,3348	76,5866	12,2742	25,3586
Internet User Skills	21	54,8506	54,3081	Multipl	1151,86	25,8010	78,1718	15,1418	27,6055
Advanced Skills and Development	21	43,3118	42,0300	Multipl	909,55	22,3295	80,4247	14,6805	33,8950
Activities online	21	50,3980	48,5308	Multipl	1058,35	33,3875	69,3385	10,7773	21,3844
Business digitisation	21	44,9281	39,5665	Multipl	943,49	20,5444	79,3486	18,1450	40,3867
cyber threat index	21	28,5714	21,8248	Multipl	600,00	2,4171	74,9243	20,0937	70,3281

Рисунок 1.16 – Описові статистики детермінант поширення кіберзагроз на множині розглянутих країн світу станом на 2020 рік

Джерело: розрахунки автора

На основі рисунку 1.16 можна стверджувати, що серед розглянутих 7 детермінант поширення кіберзагроз в розрізі лише 3 (рівень розвитку мобільного широкосмугового доступу, рівень навичок населення в Інтернеті, обсяг онлайн діяльності) спостерігається однорідність розглянутої вибірки країн, оскільки значення коефіцієнту варіації не перевищує рівня 33%. В розрізі інших детермінант, а особливо інтегрального індексу кібербезпеки спостерігається досить висока нерівномірність та різновекторність країн.

Наступним етапом запропонованого науково-методичного підходу є побудова SVM-моделей машинного навчання двох типів (epsilon-SVM

regression та nu-SVM regression) в розрізі чотирьох специфікацій опорних векторів: лінійні, поліноміальні, радіально -базисні функції (RBF) та сигмоподібні на базі даних вибіркової сукупності країн світу. Для реалізації даного етапу розглянемо спочатку математичне підґрунтя побудови та специфікацію зазначених моделей.

У регресії необхідно оцінити функціональну залежність залежної змінної y від набору незалежних змінних x. Він передбачає, як і інші задачі регресії, що зв'язок між незалежною та залежною змінними задається детермінованою функцією f з урахуванням деяких адитивних шумів (формула 1.6):

$$y = f(x) + noise \tag{1.6}$$

Завдання полягає в тому, щоб знайти функціональну форму для f, яка може правильно передбачити нові випадки, які раніше не були представлені методлм опроних векторів. Цього можна досягти шляхом навчання SVM-моделі на вибірковому наборі, що передбачає послідовну оптимізацію функції помилки. Залежно від визначення цієї функції помилки можна розпізнати два типи моделей SVM:

Тип SVM регресії 1. Для цього типу SVM модель (формула 1.7):

$$\frac{1}{2}w^T w + C\sum_{i=1}^{N} \xi_i + C\sum_{i=1}^{N} \xi_i{}^* \rightarrow min$$
$$\{w^T\phi(x_i) + b_i - y_i \leq \varepsilon + \xi_i{}^* \; y_i - w^T\phi(x_i) - b_i \leq \varepsilon + \xi_i \, \xi_i{}^*, \xi_i \geq 0, i = 1, \ldots, N \tag{1.7}$$

де C – параметр ємності (використовується для перехресної перевірки сітки);

Тип SVM регресії 2. Для цього типу SVM модель (формула 1.8):

$$\frac{1}{2}w^T w - C\left(v\varepsilon + \frac{1}{N}\sum_{i=1}^{N} (\xi_i + \xi_i^*)\right) \to min \quad (1.8)$$

$$\{w^T\phi(x_i) + b_i - y_i \le \varepsilon + \xi_i \quad y_i - w^T\phi(x_i) - b_i \le \varepsilon + \xi_i^* \, \xi_i^*, \xi_i \ge 0, i = 1, \dots, N, \varepsilon \ge 0$$

Використовуючи метод опорних векторів, можливим є побудова різних типів функціональної залежності між зімнними (лінійна, поліноміальна, радіальна базисна. Сигмовидна) (формула 1.9):

$$\phi = \{x_i \cdot x_j \; Linear \; (\gamma x_i \cdot x_j + coefficient)^d \; Polynomial \; exp\left(-\gamma\left(x_i - x_j\right)^2\right) \; RBF \; tanh(\gamma x_i \cdot x_j + coefficient) \; Sigmoid \} \quad (1.9)$$

де d - ступінь поліноміального ядра;

γ - гамма-параметр для поліномінального, RBF і сигмоподібного ядер;

коефіцієнт - коефіцієнт для поліномінального та сигмоподібного ядер.

Отже, побудуємо 8 SVM-моделей машинного навчання: двох типів (epsilon-SVM regression та nu-SVM regression) в розрізі чотирьох специфікацій опорних векторів: лінійні, поліноміальні, радіально -базисні функції (RBF) та сигмоподібні на базі даних вибіркової сукупності країн Європи (табл. 1.9).

На базі порівняння фактичних та прогнозних рівнів досліджуваних детермінант поширення кібербезпеки та інтегрального індексу кіберзагроз для тестової вибірки країн обчислимо середнє квадратичне відхилення (остання графа таблиці 1.9). Таким чином, найбільш точною виступає сигмоїдної nu-SVM регресійна модель машинного навчання, яка має наступні характеристики: SVM: Regression type 2 (C=10,000, nu=0,500), Kernel: Sigmoid (gamma=0,167, coefficient=0,000) Number of support vectors= 9 (3 bounded).

Наступним етапом є проведення визначення детермінант поширення кіберзагроз на основі методів машинного навчання SVM за допомогою сигмоїдної nu-SVM regression моделі, яка була ідентифікована як найбільш

точна та адекватна на базі країн світу тестової сукупності. Отримані результати представимо у наведених нижче рисунках 1.17-1.19.

Таблиця 1.9 – Порівняння 8 побудованих SVM-моделей

	DEU	ITA	LVA	NLD	SVK	ESP	σ
cyber threat index	63,33	57,71	42,91	18,81	8,90	74,92	
SVM: Regression type 1 (C=10,000, epsilon=0,100), Kernel: Linear Number of support vectors= 14 (8 bounded)	23,92	32,11	9,87	36,23	19,74	32,50	21,15
SVM: Regression type 1 (C=10,000, epsilon=0,100), Kernel: Polynomial (degree=3,000, gamma=0,167, 0,000(null) Number of support vectors= 14 (11 bounded)	24,08	26,02	25,38	17,44	25,21	24,81	20,69
SVM: Regression type 1 (C=10,000, epsilon=0,100), Kernel: Radial Basis Function (gamma=0,167) Number of support vectors= 14 (9 bounded)	17,09	27,93	19,68	23,59	21,38	22,23	21,24
SVM: Regression type 1 (C=10,000, epsilon=0,100), Kernel: Sigmoid (gamma=0,167, coefficient=0,000) Number of support vectors= 15 (13 bounded)	27,69	32,03	22,62	21,15	24,34	29,82	20,15
SVM: Regression type 2 (C=10,000, nu=0,500), Kernel: Linear Number of support vectors= 10 (4 bounded)	33,39	42,77	21,84	16,20	25,87	27,74	20,51
SVM: Regression type 2 (C=10,000, nu=0,500), Kernel: Polynomial (degree=3,000, gamma=0,167, 0,000(null) Number of support vectors= 9 (5 bounded)	26,03	26,03	25,98	15,91	25,39	24,52	20,71
SVM: Regression type 2 (C=10,000, nu=0,500), Kernel: Radial Basis Function (gamma=0,167) Number of support vectors= 10 (3 bounded)	29,48	37,48	28,72	16,45	28,24	24,30	20,20
SVM: Regression type 2 (C=10,000, nu=0,500), Kernel: Sigmoid (gamma=0,167, coefficient=0,000) Number of support vectors= 9 (3 bounded)	27,84	33,34	28,04	19,77	27,46	25,30	20,00

Джерело: розрахунки автора

	Model summary (Support Vector Machi
Model specifications	Value
Number of independents	6
SVM type	Regression type 1
Kernel type	Sigmoi(
Number of SVs	9 (3 bounded

Рисунок 1.17 – Специфікація SVM-моделі кіберзагроз на множині розглянутих країн світу станом на 2020 рік

Джерело: розрахунки автора

Аналіз рисунку 1.17 дозволяє констатувати наступні характеристики сигмоїдної nu-SVM regression моделі машинного навчання: кількість незалежних змінних в моделі 6, тип моделі - nu-SVM regression, Kernel type – сигмоїдна, кількість опорних векторів, які дозволяють здійснити алгоритм розпізнавання образів – 9, серед яких граничними є 3.

	SVM model specifications (coefficients and support vectors), (cyber threat index SVM.sta) SVM: Regression type 2 (C=10,000000,nu=0,500000) Kernel: Sigmoid (gamma=0,166667,coefficient=0,000000)						
Support vector	Weights 1	Support vector Banking	Support vector Mobile broadband	Support vector Internet User Skills	Support vector Advanced Skills and Development	Support vector Activities online	Support vector Business digitisation
1	-9,9177	0,80500	0,06241	0,64130	0,34696	0,41456	0,79579
2	-10,000	0,56533	0,05236	0,56273	0,37302	0,56923	0,32348
3	9,2885	0,98002	0,58778	0,89796	0,49803	0,88858	0,76567
4	9,2038	0,73917	0,44568	0,57119	0,30632	0,00000	0,44870
5	10,000	0,34556	0,03733	0,42346	0,00000	0,44383	0,23690
6	-1,8307	0,55762	0,65842	0,39695	0,26560	0,57100	0,02102
7	-10,000	0,56547	0,33106	0,29869	0,19419	0,22445	0,07624
8	9,0077	0,52858	0,09017	0,51325	0,02408	0,42122	0,33931
9	-5,7516	0,83425	0,34099	0,96056	0,50292	0,82304	0,64734

Рисунок 1.18 – Специфікація SVM-моделі визначення детермінант поширенння кіберзагроз

Джерело: розрахунки автора

Аналіз рисунку 1.18 дозволяє констатувати наступне: серед 9 побудованих опорних векторів, найбільшу за абсолютним значенням вагу мають 2, 5 та 7 вектори. Саме тому, для визначення детермінант поширенння кіберзагроз обчислимо в розрізі кожного опорного вектора середнє арифметичне значення за трьома обраними опорними векторами. Отже, отримаємо наступний рейтинг важливості детермінант поширенння кіберзагроз:

– частка населення, яка користується онлайн банкінгом (Z1) – 0,49;
– індикатор рівня навичок в Інтернеті (Z3) – 0,42;
– індикатор онлайн діяльності (Z5) – 0,41;
– індикатор ділової онлайн активності (Z6) – 0,21;
– індикатор поглиблених навичок та вмінь (Z4) –0,18;

– індикатор розвитку мобільного широкосмугового доступу (Z2) – 0,14.

У полі «Резюме» у верхній частині діалогового вікна «Результати» наведено специфікацію SVM-моделі, включаючи кількість опорних векторів та їх типи, а також ядра та їх параметри. Крім цього, відображаються й інші специфікації, створені в діалоговому вікні «Машини опорних векторів»: список залежних і незалежних змінних, значення навчальних констант (ємність, епсилон і nu), результати перехресної перевірки (якщо застосовно), а також статистику регресії для навчальних, тестових та загальних вибірок, таких як середній квадрат помилки, коефіцієнт стандартного відхилення та коефіцієнти кореляції (рисунок 1.19).

Таким чином, побудувавши нейронну модель методом опорних векторів на основі даних країн Європейського Союзу встановлено наявність тісних функціональних залежностей між рівнем кіберзагроз та такими чинниками як частка населення, яка користується онлайн банкінгом (0,49), індикатор рівня навичок в Інтернеті (0,42), індикатор онлайн діяльності (0,41).

	Regression summary (Support Vector Machin SVM: Regression type 1 (C=10,000, nu=0,50 Number of support vectors= 9 (3 bounded)	
Regression summary	cyber threat index	
Observed mean	44,430	
Predictions mean	26,956	
Observed S.D.	26,017	
Predictions S.D.	4,412	
Sum of squared error	813,906	
Error mean	17,474	
Error S.D.	24,703	
Abs. error mean	23,981	
S.D. ratio	0,949	
Correlation	0,375	

Рисунок 1.19 – Показники точності SVM-моделі визначення детермінант поширенння кіберзагроз

Джерело: розрахунки автора

Таким чином, збільшення частоти та масштабів кібершахрайств у фінансовому секторі може призвести до несанкціонованого розповсюдження

персональної фінансової інформації про клієнтів, отримання значних збитків та репутаційних втрат фінансовими установами і навіть мати системні наслідки для економіки країни, оскільки загрози можуть швидко поширюватися по різних секторах економіки. За цих умов вчасно ідентифікувати ознаки кібершахрайства та швидко прийняти рішення щодо їх нейтралізації.

1.4 Проведення типологізації країн за рівнем участі їх резидентів у здійсненні кібернетичних та фінансових шахрайств

Протягом останніх років відбувається динамічне поширення кібершахрайств та фактично набула характеристик організованої злочинної діяльності у кіберпросторі. Враховуючи транснаціональний характер злочинів, пов'язаних із протиправним, несанкціонованим створенням, зберіганням, обробкою, пошкодженням або знищенням об'єктів інформаційної інфраструктури, ефективна протидія цим діям потребує розробки системних заходів для посилення перевірки та контролю задля протидії шахрайським операціяv у мережі Інтернет.

Для ефективної організації системи кібербезпеки на як рівні окремих суб’єктів господарювання, так і держави загалом доцільним є запровадження двостороннього підходу, який передбачає поєднання дієвих превентивних заходів та постійного моніторингу стану інформаційної системи. З одного боку в умовах постійного збільшення кількості кіберзагроз та зростання складності їх проведення та, з іншого боку, нарощення обсягів транскордонної торгівлі товарів та послуг, вкрай важливо суб’єктам господарювання проводити процедуру експрес-перевірки клієнтів та контрагентів без безпосередньої взаємодії з ним. Це може бути реалізовано шляхом розробки списку ризикових держав (юрисдикцій), резиденти яких можуть мати фактичний або потенційний несприятливий вплив через ланцюги відносин на функціонування суб’єктів національної економіки. Виходячи з цього,

запропоновано науково-методичний підхід до багатокритеріального оцінювання ступеня залученості ділового партнера до фактичного або ймовірного у перспективі несприятливого впливу на безпеку об'єктів інформаційної інфраструктури. Для вирішення поставленого завдання використано алгоритм машинного навчання без нагляду на основі змінних на рівні країн, який може класифікувати країни за рівнем їх фактичної або ймовірної участі у протиправних кібернетичних правопорушеннях.

Основними етапами розробленого науково-методичного підходу є:

– формування вхідної статистичної бази дослідження;

– приведення значень показників до єдиного співставного вигляду;

– визначення узагальненої оцінки окремим складовим протиправної діяльності в країні;

– поділ країни на кластери за рівнем їх фактичної або ймовірної участі у протиправних кібернетичних правопорушеннях;

– формалізація сутнісних характеристик кластерів країн на основі використання дерев класифікації.

Перший етап передбачає формування інформаційної та статистичної бази дослідження. Соціальні та економічні чинники відображають рівень добробуту громадян та умов для їх стабільного функціонування, слугуючи основним контекстом, у якому виникає кіберзлочинність. Людські та соціальні чинники відіграють значну роль у формуванні агломерацій кіберзлочинності [65]. Особливістю розробленого авторського підходу є розробка інтегрального показника, який буде відображати не тільки частоту й масштаби кібератак, ініційованих резидентами відповідної країни, а також врахувати стан дотримання норм доброчесності у бізнес-середовищі, доступу резидентів до анонімної мережі даркнету та інтенсивність її використання, а також загальну криміногенну ситуацію в регіоні, що в сукупності опосередковано визначають ступінь залученості громадян відповідної країни до протиправної діяльності у кіберпросторі.

Для побудови інтегрального показника рівня фактичної або ймовірної участі резидентів країни у протиправних кібернетичних правопорушеннях обрано наступні групи показників, які подані в таблиці 1.10. Дві групи показників, які характеризують різні види злочинності (X1) та активність кримінальних угруповувань (X2), визначалися на основі двоетапного опитування експертів у рамках проекту Глобальної ініціативи проти транснаціональної організованої злочинності. Дане опитування проходило у межах розрахунку Глобального індексу організованої злочинності (Global Organized Crime Index) [66].

Для апробації розробленого науково-методичного підходу використано вхідну статистичну базу 34 країн світу, яка подана в таблиці 1.11. Системне та грубе недотримання суб'єктом господарювання норм міжнародного права може призвести до запровадження міжнародних штрафних санкцій та обмежень як до окремого економічного суб'єкта, так і держави загалом.

У роботі зроблено припущення, що ті суб'єкти господарювання, які перебувають у зоні високого ризику потрапляння під міжнародні санкції, можуть функціонувати ірраціонально та здійснювати злочинну діяльність. Зауважимо, що індикатор «міжнародні санкції, які накладені на країну» визначено на основі аналізу 10 діючих режимів санкцій, спрямованих на протидію легалізації доходів, отриманих незаконним шдяхом: US OFAC, UN Security Council, EU restrictive measures, EU non-cooperative tax jurisdictions, EU high-risk third countries,UK high-risk third countries, UK financial sanctions, FATF increased monitoring (сірий список), FATF call for action (чорний список), Australian sanctions.

Оскільки для характеристики злочинності в країні використано 9 індикаторів, тому виникає об'єктивна необхідність визначення проміжного узагальненого показника для використання його в подальших розрахунках. Аналогічну процедуру доцільно провести й для оцінки узагальненого рівня активності кримінальних угрупувань, що включатиме 4 індикатори.

Таблиця 1.10– Перелік індикаторів для типологізації країн за рівнем участі їх резидентів у здійсненні фінансових кібернетичних шахрайств

Показник		Одиниця вимірювання	Умовне позначення	Межі коливання
Група показників, які характеризують різні види злочинності (X1)	контрабанда людей	бал	X1_1	0-10
	торгівля зброєю	бал	X1_2	0-10
	злочини проти флори	бал	X1_3	0-10
	злочини проти фауни	бал	X1_4	0-10
	злочини проти невідновлюваних ресурсів	бал	X1_5	0-10
	торгівля героїном	бал	X1_6	0-10
	торгівля кокаїном	бал	X1_7	0-10
	торгівля канабісом	бал	X1_8	0-10
	торгівля синтетичними наркотиками	бал	X1_9	0-10
Група показників, які відображають активність кримінальних угруповувань (X2)	мафіозні угруповання	бал	X2_1	0-10
	злочинні мережі	бал	X2_2	0-10
	державні суб'єкти	бал	X2_3	0-10
	іноземні суб'єкти	бал	X2_4	0-10
Ризик корупції та хабарів		ум.од.	X3	0-100
Питома вага кібератак у світі, ініціатором якої виступила країна		%	X4	0-100
Загальний дохід, який отримано на даркнет-ринку		євро на душу населення	X5	0;∞
Міжнародні санкції, які накладені на країну		ум.од.	X6	0-1

Джерело: розрахунки автора

Таблиця 1.11 – Вхідна статистична база для дослідження

	X1_1	X1_2	X1_3	X1_4	X1_5	X1_6	X1_7	X1_8	X1_9	X2_1	X2_2	X2_3	X2_4	X3	X4	X5	X6
Албанія	6,5	4,5	4,5	3,5	5,5	6,0	7,0	7,0	3,0	7,0	7,5	7,0	2,5	35	0,0	2,9	0,2
Білорусь	5,5	6,5	3,0	2,0	5,0	4,0	2,0	4,0	5,0	4,0	5,0	9,0	5,0	41	0,7	13,7	0,3
Хорватія	6,0	3,5	5,0	2,5	4,5	5,0	5,5	5,5	5,5	4,0	6,5	6,5	4,5	47	0,0	7,7	0,0
Кіпр	6,0	2,5	2,5	3,0	2,0	2,0	4,5	4,0	3,0	3,5	5,0	4,0	7,0	53	0,0	14,3	0,0
Чехія	5,0	4,5	3,0	5,5	3,0	4,5	4,5	6,0	6,5	3,0	5,0	5,5	4,5	54	0,0	13,6	0,0
Данія	4,5	4,0	1,5	2,0	2,0	5,0	5,5	5,0	5,0	5,0	4,0	2,0	4,5	88	0,0	9,0	0,0
Єгипет	5,5	7,0	1,0	5,0	4,0	5,5	2,0	7,0	7,0	3,0	5,5	8,0	5,0	33	0,1	0,7	0,0
Естонія	3,0	3,0	1,5	1,5	3,0	3,0	3,5	5,0	6,5	3,0	5,0	2,0	5,0	74	0,0	21,7	0,0
Фінляндія	2,5	2,5	1,0	1,5	2,0	3,5	4,0	3,5	4,5	3,0	3,0	1,5	3,0	88	0,0	18,3	0,0
Франція	6,5	6,0	4,0	5,5	4,5	6,0	6,5	6,5	5,5	6,0	6,5	3,0	7,0	71	0,1	5,8	0,0
Грузія	2,0	2,0	3,5	3,5	3,0	3,5	2,0	3,5	4,0	2,5	3,0	3,0	3,0	55	0,0	9,0	0,0
Німеччина	7,0	6,0	1,5	3,5	2,5	4,5	6,5	5,0	6,0	5,0	6,5	2,0	6,5	80	0,0	6,5	0,0
Греція	7,5	3,5	2,0	2,5	3,0	6,0	3,5	5,0	2,5	3,0	6,5	7,5	6,0	49	0,1	4,1	0,0
Угорщина	6,0	3,5	3,5	4,5	3,5	4,5	5,0	5,5	5,5	1,0	4,0	7,0	5,0	43	0,0	5,1	0,0
Італія	6,5	5,5	2,5	3,5	5,5	4,5	7,5	5,0	5,0	9,0	3,0	6,5	7,0	56	0,0	2,9	0,0
Йорданія	5,5	6,5	3,5	3,5	1,5	3,5	3,0	6,0	6,0	1,5	7,0	6,5	4,5	49	0,1	1,4	0,3
Латвія	3,5	3,5	1,0	2,0	2,0	4,5	5,0	5,5	5,0	3,5	3,5	2,0	4,5	59	0,0	30,8	0,0
Литва	2,5	2,5	1,0	2,0	2,0	4,0	4,5	4,0	4,0	3,5	4,0	4,0	3,0	61	0,0	16,4	0,0
Мальта	4,0	2,5	1,0	5,0	5,0	3,0	5,0	4,5	5,5	1,5	7,0	7,5	5,0	54	0,0	17,1	0,0
Молдова	4,0	5,0	2,5	2,0	3,0	3,0	2,5	4,5	5,0	4,0	4,0	7,0	5,0	36	0,0	14,4	0,1
Морокко	6,5	3,0	3,0	4,5	3,0	3,0	6,0	9,0	6,0	1,0	6,5	7,0	4,0	39	0,1	1,4	0,2
Нідерланди	4,5	5,0	3,0	4,0	4,0	4,0	7,0	5,5	7,5	4,5	6,0	2,5	4,5	82	0,1	16,8	0,0
Норвегія	3,5	3,5	2,5	4,0	3,5	5,0	4,5	4,0	4,5	4,5	4,0	2,0	4,0	85	0,0	16,3	0,0
Польща	4,5	3,5	2,0	2,5	5,5	4,0	4,5	5,5	6,5	2,0	5,5	3,5	3,5	56	0,1	6,4	0,0
Португалія	4,0	4,0	3,5	3,5	3,0	4,5	5,0	4,5	4,5	4,5	6,0	4,5	5,0	62	0,0	7,5	0,0
Росія	6,0	4,5	7,5	7,5	5,0	7,0	4,5	5,0	7,5	4,5	7,5	8,5	5,0	29	22,6	8,7	0,5
Сербія	6,5	7,5	4,0	4,0	4,0	7,0	5,5	6,0	6,0	6,0	7,0	8,0	6,5	38	0,0	5,1	0,3
Словенія	5,5	3,5	2,0	3,0	2,5	4,0	4,5	5,0	5,5	3,0	4,5	6,0	5,0	57	0,0	23,5	0,0
Іспанія	7,0	4,0	3,5	5,0	2,0	6,5	7,0	7,0	4,0	6,0	6,5	5,0	7,5	61	0,3	5,7	0,0
Швеція	5,5	6,0	2,0	3,5	2,0	4,0	4,5	5,0	5,5	5,5	5,5	2,5	6,0	85	0,0	19,1	0,0
Туніс	7,0	5,0	3,5	3,5	5,0	2,0	3,0	5,0	4,0	1,0	4,0	5,5	3,0	44	0,0	1,7	0,1
Турція	9,0	9,0	4,0	3,0	9,5	8,0	4,0	5,0	5,5	8,0	7,5	9,0	5,0	38	0,1	4,8	0,3
Україна	6,5	8,0	6,5	4,0	7,0	5,0	3,5	5,0	3,5	6,0	7,0	8,0	6,0	32	0,7	18,8	0,3
Великобританія	5,0	3,5	2,5	4,0	2,0	4,5	6,5	4,5	5,5	4,0	6,5	3,0	8,0	78	0,3	9,0	0,0

Джерело: розроблено автором на основі [67]

2 етап. Агрегування показників першої та другої груп в інтегральні показники за допомогою попереднього проведення нормалізації за допомогою

методу Харрінгтона з подальшим формуванням узагальнюючих показників шляхом застосування функції Fonseca-Fleming.

Приведення показників вхідної статистичної бази дослідження в розрізі 1-ої та 2-ої груп по співставного вигляду відбувається за допомогою застосування методу Харрінгтона, тобто наступного співвідношення (формула 1.10):

$$P_{qi}^{N} = \frac{2 \cdot P_{qi} - \left(\{P_{qi}\} + \{P_{qi}\}\right)}{\{P_{qi}\} - \{P_{qi}\}} \tag{1.10}$$

де P_{qi}^{N} – нормалізоване значення і-го показника для q-ої країни;

P_{qi} – фактичне значення і-го показника для q-ої країни.

На основі формули 1.10 визначено нормалізовані показники, які подані в додатку Б, таблиця Б.1.

З метою згортки нормалізованих показників в єдиний інтегральний показник використовується функція Fonseca-Fleming, яка набуває наступного вигляду (формула 1.11):

$$I_q^G = \left(1 - exp\left(-\sum_{i=1}^{n} \left(P_{qi} - \frac{1}{\sqrt{n}}\right)^2\right) 1 - exp\left(-\sum_{i=1}^{n} \left(P_{qi} + \frac{1}{\sqrt{n}}\right)^2\right)\right) \tag{1.11}$$

де I_q^G – інтегральний показник для q-ої країни в розрізі G-ої групи показників;

n- кількість показників в розрізі G-ої групи.

Результати розрахунку інтегральних показників для відображення загального рівня злочинності в країні та активності криміногенних

угрупувань, використовуючи формулу Fonseca-Fleming (1.11), подано в таблиці 1.12.

Таблиця 1.12 – Інтегральні показники рівня злочинності та активності криміногенних угрупувань в окремих країнах світу

Країна	Рівень злочинності (X1)	Рівень активності криміногенних угрупувань (X2)	Країна	Рівень злочинності (X1)	Рівень активності криміногенних угрупувань (X2)
Albania	0,9203	0,8965	Lithuania	0,8404	0,2489
Belarus	0,7942	0,6872	Malta	0,8152	0,8517
Croatia	0,7738	0,5309	Moldova	0,6215	0,5300
Cyprus	0,8380	0,6290	Morocco	0,9771	0,8488
Czech Republic	0,7955	0,2140	Netherlands	0,9583	0,4787
Denmark	0,7588	0,3615	Norway	0,4694	0,3242
Egypt	0,9761	0,6617	Poland	0,7391	0,3817
Estonia	0,8769	0,3432	Portugal	0,3502	0,4313
Finland	0,8919	0,6839	Russia	0,9436	0,6734
France	0,5111	0,6391	Serbia	0,7215	0,3156
Georgia	0,8513	0,5664	Slovenia	0,5751	0,3100
Germany	0,9370	0,8011	Spain	0,9592	0,3633
Greece	0,8798	0,5590	Sweden	0,6731	0,6074
Hungary	0,6049	0,6966	Tunisia	0,7066	0,5889
Italy	0,9241	0,9011	Turkey	0,9739	0,7113
Jordan	0,8109	0,8614	Ukraine	0,9362	0,3080
Latvia	0,7592	0,3858	United Kingdom	0,8348	0,8183

Джерело: розрахунки автора

Наступним етапом є кластеризація країн за рівнем участі їх резидентів у фінансових кібершахрайствах. Крім вищерозрахованих двох індикаторів загального рівня злочинності та активності криміногенних угрупувань, поділ країн на кластери буде здійснюватися також з урахуванням даних про рівень корупції, рівень участі країни в кібератаках, обсягу доходу, який закумульвано на площадках даркнет-ринку, а також про рівень включення країни до міжнародних санкційних списків.

Для кластеризації країн використано агломеративні методи мінімальної дисперсії (ітеративний дівізівний метод k-середніх). Використання методу k-середніх передбачає розрахунок та аналіз наступних показників: середні величини для кожного кластера (усереднення проводиться всередині кластера), евклідові відстані та квадрати евклідових відстаней між кластерами. У розрізі початкових центрів кластерів запропоновано обрати підхід сортування відстані і вибору спостереження на постійних інтервалах. Для розрахунків використано програмний статистичний продукт Statistica 8.

Ключовим моментом кластерного аналізу є визначення обґрунтованої кількості груп країн світу (дві або три), що здійснюється на основі результатів дисперсійного аналізу. У таблиці 1.13 та 1.14 представлені значення міжгрупових (Between SS) та внутрішньогрупових (Within SS) дисперсій ознак.

Таблиця 1.13 – Результати дисперсійного аналізу кластеризації країн світу на 2 групи

	Between SS	df	Within SS	df	F	sign. p
X1	0,063	1	0,749	32	2,70462	0,109848
X2	0,143	1	1,571	32	2,91429	0,097485
X3	7211,954	1	3244,164	32	71,13775	0,000000
X4	11,468	1	482,139	32	0,76117	0,389462
X5	409,008	1	1389,547	32	9,41908	0,004352
X6	0,139	1	0,462	32	9,63993	0,003968

Джерело: розрахунки автора

Таблиця 1.14 – Результати дисперсійного аналізу кластеризації країн світу на 3 групи

	Between SS	df	Within SS	df	F	sign. p
X1	0,033	2	0,779	31	0,6615	0,523226
X2	0,147	2	1,566	31	1,4582	0,248179
X3	9548,153	2	907,964	31	162,9980	0,000000
X4	24,114	2	469,494	31	0,7961	0,460094
X5	406,276	2	1392,279	31	4,5230	0,018899
X6	0,284	2	0,317	31	13,8818	0,000050

Джерело: розрахунки автора

Про якість даної кластеризації свідчить виконання наступних критеріїв:

– мінімізація значення внутрішньогрупової дисперсії та максимізація значення міжгрупової дисперсій. Виконання даної умови засвідчує рівень належності країн до відповідного кластеру в розрізі кожного індикатора, а також якість проведеної кластеризації;

– максимізація значення критерію Фішера (F) та спрямування до нульового значення ймовірності відхилення нульової гіпотези (p), тобто недоцільність використання певного індикатора для визначення ступеня належності країни до відповідного кластеру.

Таким чином, аналіз результатів групування країн на 2 кластери свідчить про якісно проведену кластеризацію, оскільки значення p-значення в розрізі трьох індикаторів (X1, X2, X4) перевищує допустимий для економічних досліджень рівень 0,05, а для всіх інших інтегральних показників характеристики груп приймає граничний до допустимого рівень. Перехід від двох до трьох кластерів призводить до погіршення якості кластеризації. Отже, неадекватність групування країн світу на 3 кластери призводить до необхідності розгляду 2-кластерного групування досліджуваних об’єктів.

Обґрунтувавши доцільність виділення саме 2 кластерів країн, визначимо склад кожного із виділених кластерів (таблиця 1.15).

Таким, структура країн за кластерами представлена наступним чином: 1 кластер – 14 країн; 2 кластер – 20 країн. Візуалізацію проведеної процедури групування країн світу представлено на рисунку 1.20.

Переходячи до аналізу описових статистик виділених 2 кластерів (рисунок 1.21 – 1 фрагмент) в розрізі середніх значень прослідковуються наступні характерні особливості: середні значення за індикаторами в країнах 1-го кластеру є вищими у порівнянні з 2-им кластером країн.

Таблиця 1.15 – Розподіл країн у розрізі 2 виокремлених кластерів

Кластер 1		Кластер 2	
Країна	Відстань від центру кластера	Країна	Відстань від центру кластера
Данія	6,304783	Албанія	4,21450
Естонія	2,847356	Білорусь	2,74840
Фінляндія	6,041784	Хорватія	1,30750
Франція	3,811374	Кіпр	4,57046
Німеччина	4,260769	Чехія	4,75683
Латвія	8,861327	Єгипет	5,36010
Литва	5,204945	Грузія	4,53325
Нідерланди	3,520315	Греція	2,53516
Норвегія	4,679923	Угорщина	1,25265
Португалія	5,605646	Італія	5,27588
Словенія	7,673571	Йорданія	3,30724
Іспанія	6,336485	Мальта	5,60651
Швеція	4,970037	Молдова	4,30121
Великобританія	2,956365	Мороко	3,31009
		Польща	4,93041
		Росія	10,68329
		Сербія	2,74289
		Туніс	2,48588
		Туреччина	2,76711
		Україна	6,70613

Джерело: розрахунки автора

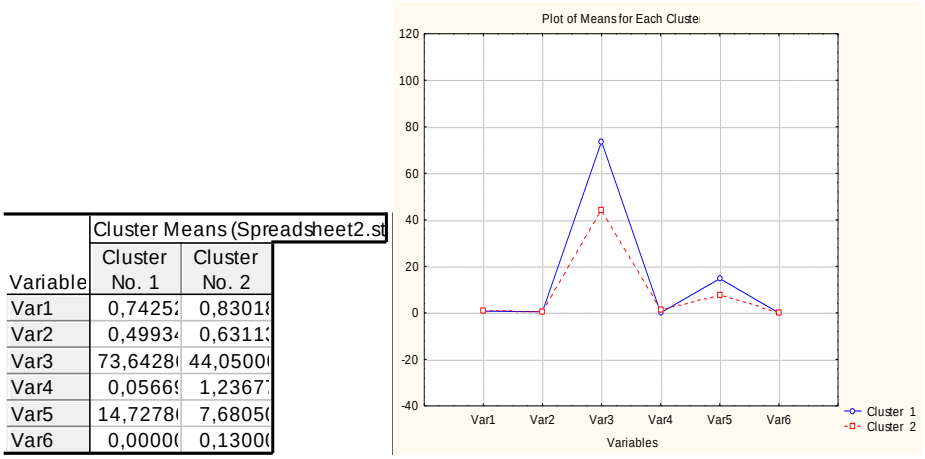


Рисунок 1.20– Скріншот фрагменту середніх значень вхідних показників кластеризації

Джерело: розрахунки автора

Variable	Descriptive Statistics for Cluster 1 (Spreadsheet2.s Cluster contains 14 cases		
	Mean	Standard Deviation	Variance
Var1	0,7425	0,1971	0,038
Var2	0,4993	0,2056	0,042
Var3	73,6428	11,6130	134,862
Var4	0,0566	0,0999	0,010
Var5	14,7278	7,6996	59,284
Var6	0,0000	0,0000	0,000

Variable	Descriptive Statistics for Cluster 2 (Spreadsheet2.s Cluster contains 20 cases		
	Mean	Standard Deviation	Variance
Var1	0,8301	0,11320	0,0128
Var2	0,6311	0,23180	0,0537
Var3	44,0500	8,85838	78,4710
Var4	1,2367	5,03675	25,3688
Var5	7,6805	5,70709	32,5709
Var6	0,1300	0,15593	0,0243

Рисунок 1.21 – Скріншот фрагменту описової статистики кластеризації європейських країн на 2 кластери

Джерело: розрахунки автора

Дані рисунків 1.20-1.21 наочно демонструють, що найбільший ефект у розподіл країн на кластери за рівнем ймовірної участі їх резидентів в протиправній діяльності в кіберпросторі є індикатор «питома вага кібератак у світі, ініціатором якої виступила країна» (X4). Зокрема, середнє значення даного показника в кластері 1 становить 0,06 %, тоді як у кластері 2 – 1,24%.

Наступний (четвертий) етап розробленого науково-методичного підходу є побудова дерев класифікації на основі методу одномірного розгалуження CART, що дозволить визначити тригерні показники та їх значення, на основі яких відбувалося поділ країн світу на кластери

Провівши кластеризацію країн, при реалізації даного етапу постає необхідність у формалізації портретів кластерів країн на основі використання дерев класифікації – методу, що дозволяє передбачати приналежність об’єктів (країн) до відповідного класу категоріальної змінної (кластер 1, 2) залежно від значень однієї чи більше незалежних вхідних предикторів.

Процес побудови дерев класифікації включає здійснення чотирьох кроків:

1.Процедура вибору критеріїв точності прогнозу на основі використання методу однакової апріорної ймовірності.

2. Процедура вибору варіантів розгалуження на основі активізації CART-методу, тобто програми дерев класифікації, яка при побудові дерева

здійснює повний перебір усіх можливих варіантів одномірного розгалуження. В якості критерія узгодженості обрано міру Джині, що представляє собою суму усіх попарних добутків відносних розмірів класів, представлених у розглянутій вершині дерев. Значення міри Джині будуть максимальними у випадку однакових розмірів усіх класів.

3. Ідентифікація тригерної точки, за якої необхідно зупинити процедуру розгалуження на основі обраної прямої зупинки процедури розгалуження за методом FACT. Так, розгалуження за предикторними змінними продовжується до того часу, коли кожна термінальна вершина не буде містити не одного неправильно класифікованого об’єкту (країни).

4. Визначення необхідного розміру дерева класифікації за методом глобальної крос-перевірки, коли кількість ітерацій встановлюється за замовчуванням рівною трьом.

Використання методичного інструментарію дерев класифікації в дослідженні здійснюється на основі програмного забезпечення Statistica. Дерева класифікації побудовано для шести ключових індикаторів (X1-X6), які використані для типологізації країн за рівнем фактичної або ймовірної участі резидентів країни у протиправних кібернетичних правопорушеннях

Першим індикатором є «рівень злочинності» (X1). На рисунку 1.22 показано результат побудови дерева класифікації для даного індикатора. Будь-яек дерево класифікації містить інформацію про номера вершин (node), номера дочірніх вершин на лівій та правій гілках, кількість об’єктів у класах та умову розгалуження (split variable).

Node	Left branch	Right branch	n in cls 2G	n in cls 1G	Predict. class	Split constant	Split variable
Tree Structure (Spreadsheet2.sta) Child nodes, observed class n's, predicted class, and split condition for each node							
1	2	3	20	14	2G	-0,590035	Var1
2			0	4	1G		
3			20	10	2G		

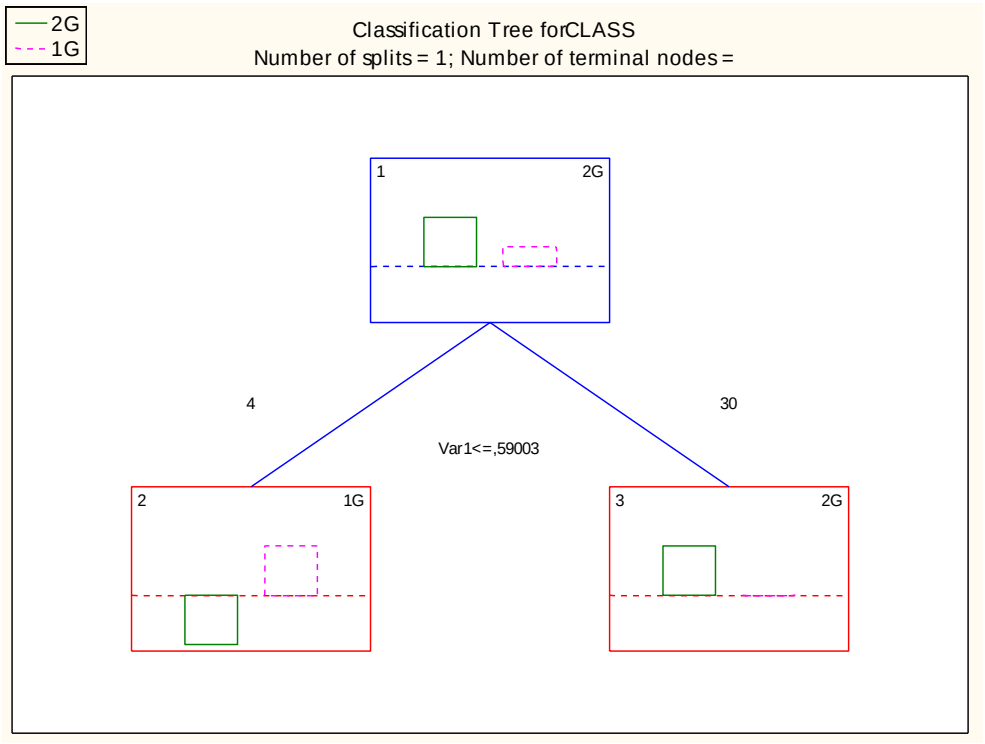


Рисунок 1.22 – Скріншот фрагменту структури дерева класифікації країн в розрізі індикатора «рівень злочинності» (X1)

Джерело: розрахунки автора

На основі аналізу рисунку 1.22 можна зробити висновок, що ліва гілка містить один вузол під номером 2, права – теж один вузол під номером 3. На основі першого рядка рисунку 5 видно, що у першій вершині 20 країн класифіковані до 2 кластеру, 14 до 1 кластеру. Для розгалуження країн за вершинами 2 і 3 використовується значення змінної інтегрального рівня злочинності, яке приймає значення більше «0,590» для країн кластеру 2 і значення не більше «0,590» для країн кластеру 1.

На рисунку 1.23 представлено дерево класифікації для індикатора «рівень активності кримінальних угруповувань» (X2).

Node	Tree Structure (Spreadsheet2.sta) Child nodes, observed class n's, predicted class, and split condition for each node						
	Left branch	Right branch	n in cls 2G	n in cls 1G	Predict. class	Split constant	Split variable
1	2	3	20	14	2G	-0,50439	Var2
2			4	9	1G		
3			16	5	2G		

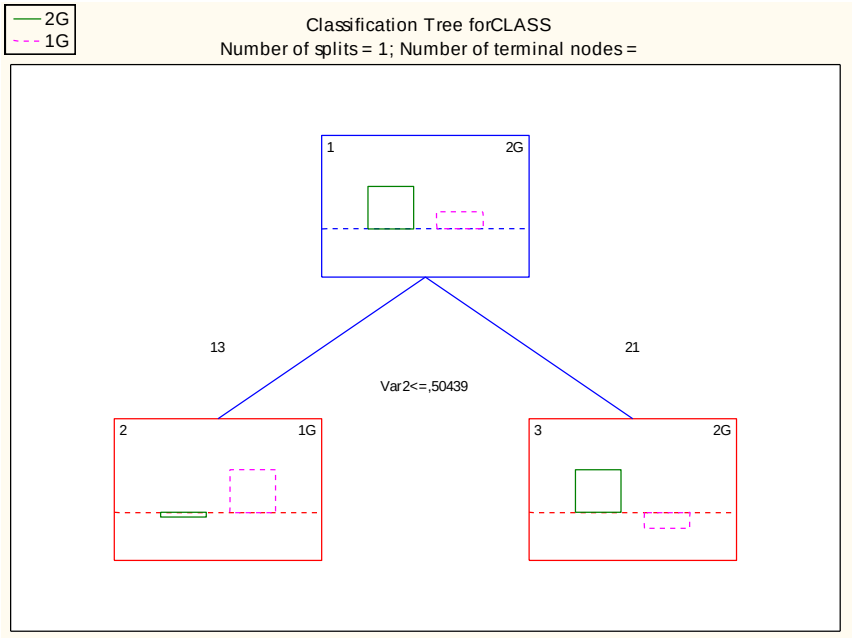


Рисунок 1.23 – Скріншот фрагменту структури дерева класифікації країн в розрізі індикатора «рівень активності кримінальних угруповувань»

Джерело: розрахунки автора

На основі аналізу рисунку 1.23 можна зробити висновок, що ліва гілка містить один вузол під номером 2, права – теж один вузол під номером 3. На основі першого рядка рисунку 5 видно, що у першій вершині 20 країн класифіковані до 2 кластеру, 14 до 1 кластеру. Для розгалуження країн за вершинами 2 і 3 використовується значення змінної інтегрального рівня активності кримінальних угруповувань, яке приймає значення більше «0,504» для країн кластеру 2 і значення не більше «0,504» для країн кластеру 1.

Розрахункові результати, що показані на рисунку 1.24, включають інформацію про дерева класифікації для індикатора «ризик корупції та хабарів» (X3).

Node	Left branch	Right branch	n in cls 2G	n in cls 1G	Predict. class	Split constant	Split variable
1	2	3	20	14	2G	-56,500(	Var3
2			20	0	2G		
3			0	14	1G		

Tree Structure (Spreadsheet2.sta)
Child nodes, observed class n's,
predicted class, and split condition for each node

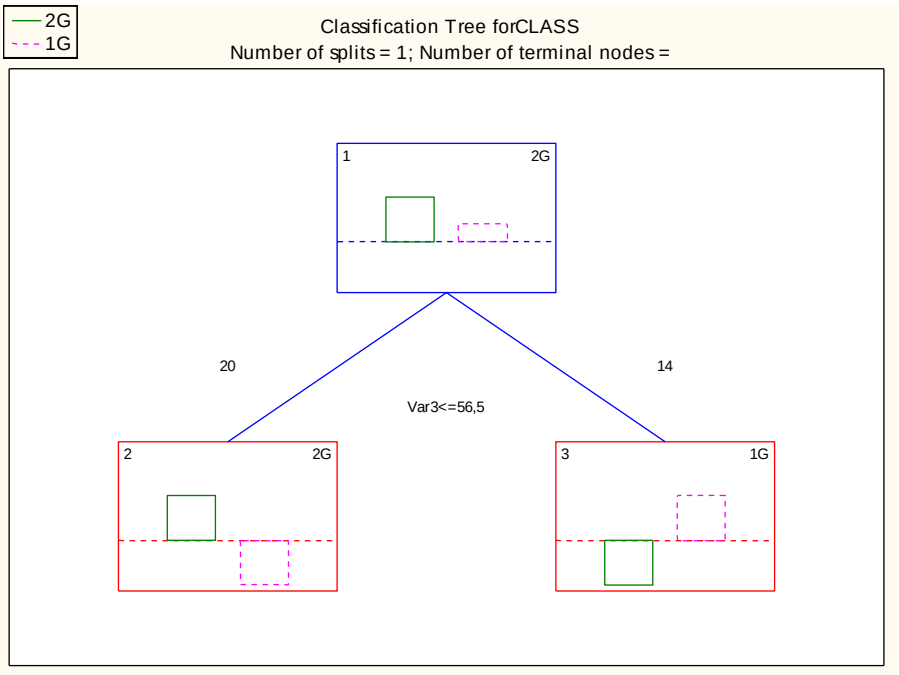


Рисунок 1.24 – Скріншот фрагменту структури дерева класифікації країн в розрізі індикатора «ризик корупції та хабарів» (X3)

Джерело: розрахунки автора

На основі аналізу рисунку 1.24 можна зробити висновок, що ліва гілка містить один вузол під номером 2, права – теж один вузол під номером 3. На основі першого рядка рисунку 5 видно, що у першій вершині 20 країн класифіковані до 2 кластеру, 14 до 1 кластеру. Для розгалуження країн за вершинами 2 і 3 використовується значення змінної «ризик корупції та хабарів», яке приймає значення не більше «56,500» для країн кластеру 2 і значення більше ««56,500» для країн кластеру 1.

Для формування профілей кластерів країн, розглянемо результати побудови дерев класифікації в розрізі індикатора «загальний дохід, який отримано на даркнет-ринку» (X5) (рисунок 1.25).

Node	Tree Structure (Spreadsheet2.sta) Child nodes, observed class n's, predicted class, and split condition for each node						
	Left branch	Right branch	n in cls 2G	n in cls 1G	Predict. class	Split constant	Split variable
1	2	3	20	14	2G	-5,4100(	Var5
2			10	0	2G		
3	4	5	10	14	1G	-0,0500(	Var6
4			6	14	1G		
5			4	0	2G		

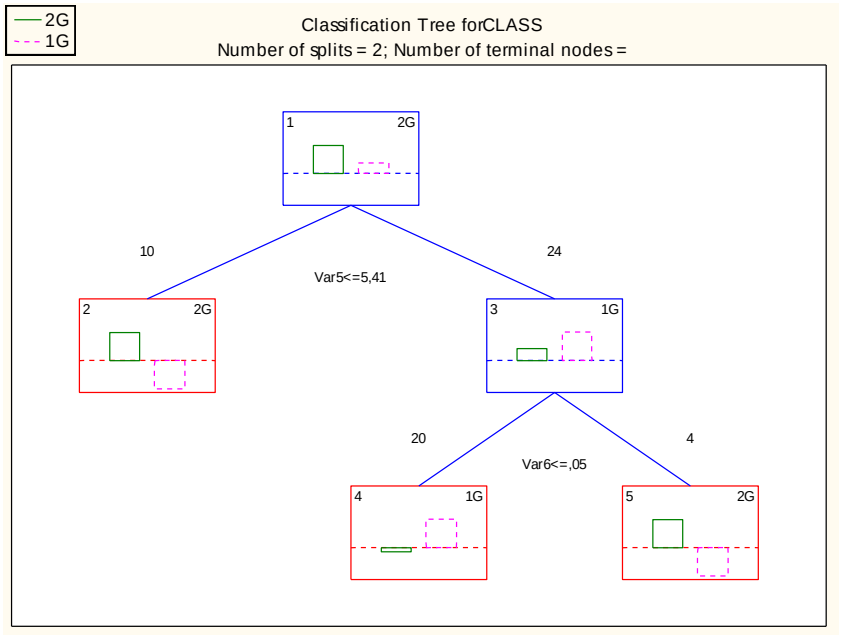


Рисунок 1.25 – Скріншот фрагменту структури дерева класифікації країн в розрізі індикаторів «загальний дохід, який отримано на даркнет-ринку» (X5) та «міжнародні санкції, які накладені на країну» (X6)

Джерело: розрахунки автора

На основі аналізу рисунку 1.25 можна зробити висновок, що ліва гілка містить один вузол під номером 2, права – теж один вузол під номером 3. Для розгалуження країн за вершинами 2 і 3 використовується значення змінної «загальний дохід, який отримано на даркнет-ринку» (X5), яке приймає значення не більше «5,4100» для країн кластеру 2 і значення більше «5,4100» для країн кластеру 1. Подальше виділення країн кластеру 1 відбувається на основі застосування змінної «міжнародні санкції, які накладені на країну» (X6), яка має приймати значення не менше «0,05», та віднесення країн до кластеру 2 в іншому випадку.

Отже, за результатами побудови дерев класифікації отримані основні результати, які представлені в таблиці 1.16.

Таблиця 1.16 – Результати побудови дерев класифікації

Назва індикатора	1 кластер	2 кластер
Рівень злочинності (X1)	< 0,590	> 0,590
Рівень активності кримінальних угруповувань (X2)	< 0,504	> 0,504
Ризик корупції та хабарів (X3)	> 56,500	< 56,500
Питома вага кібератак у світі, ініціатором якої виступила країна (X4)		
Загальний дохід, який отримано на даркнет-ринку (X5)	< 5,410	> 5,410
Міжнародні санкції, які накладені на країну (X6)	< 0,05	> 0,05

Джерело: розрахунки автора

П’ятий етап розробленого науково-методичного підходу є визначення інтегрального показника на основі згортки нормалізованих показників за допомогою методу Харрінгтона (рис. 1.26). Дані рисунку 1.26 демонструють, що з поміж 34 аналізованих країни світу найвищий рівень участі резидентів у здійсненні фінансових кібернетичних шахрайств має Молдова (0,34 ум.од.), Туніс (0,29 ум.од.) та Угорщина (0,22 ум.од.). Скандинавські країні (Данія – 0,04 ум.од, Фінляндія – 0,06 ум.од., Норвегія – 0,07 ум.од.) та інші високорозвинуті країни (Німеччина – 0,02 ум.од., Нідерланди – 0,04 ум.од., Великобританія – 0,04 ум.од.) мають низький ступінь залученості громадян до протиправних шахрайських діянь у кіберпросторі.

Варто відзначити, що розширення переліку країн світу для практичної дозволило б масштабувати цей науково-методичний підхід та отримати загальний стан рівня залученості резидентів країни в протиправну діяльність у кіберпросторі на світовому рівні.

Підсумовуючи, зазначимо, що розроблений науково-методичний підхід до визначення ступеня залученості резидентів країни до здійснення фінансових кібернетичних шахрайств дозволяє визначити перелік країн світу, з резидентами яких має бути посилений регуляторний контроль з боку контролюючих та наглядових органів. Крім цього, співпраця з резидентами

тих країн, які мають високий ступінь залученості до протиправних шахрайських дій у кіберпросторі, також несе репутаційні ризики для іншої країни.

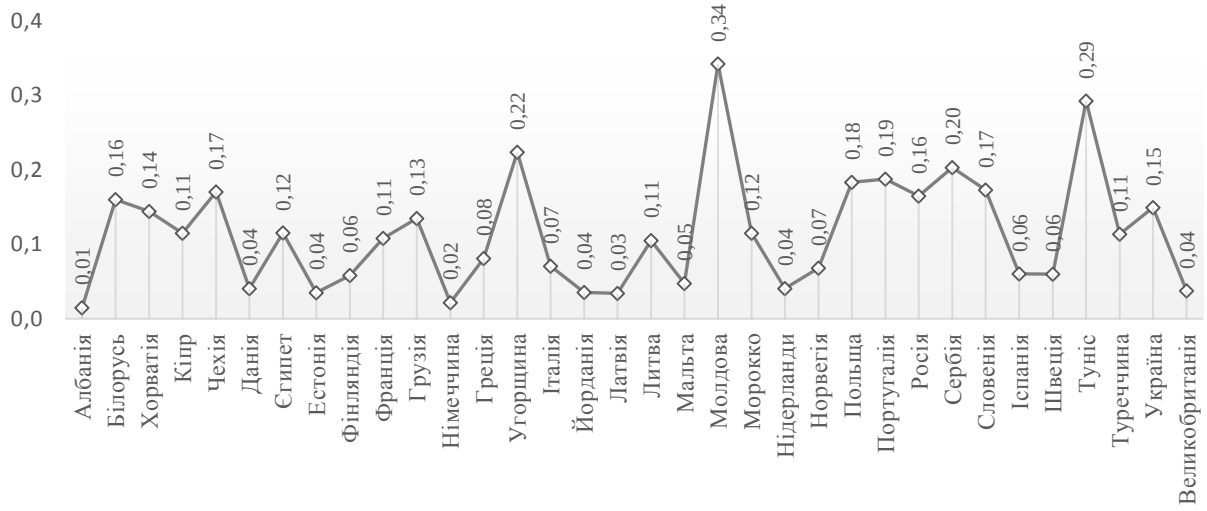


Рисунок 1.26 – Інтегральний рівень участі резидентів країни у здійсненні фінансових кібернетичних шахрайств

Джерело: розрахунки автора

2 РОЗВИТОК МЕТОДИЧНОГО ІНСТРУМЕНТАРІЮ ОЦІНЮВАННЯ ПЕРЕДУМОВ ТА ПОТОЧНОГО СТАНУ КІБЕРЗАГРОЗ В УМОВАХ ДІДЖИТАЛІЗАЦІЇ ЕКОНОМІКИ

2.1 Методичні засади до оцінювання ризику фінансових кібершахрайств

Зростання обсягів електронної комерції, використання системи онлайн-оплати рахунків сприяє збільшенню частки безготівкових розрахунків, що, з одного боку, дозволяє державі більш ефективніше контролювати джерела походження фінансових ресурсів та напрямків їх використання, а іншого – з'являються нові способи здійснення фінансових платіжних шахрайств. Протиправні дії з банківськими платіжними картками становлять підвищену небезпеку для різних верств суспільства та суб'єктів господарювання, оскільки завдають збитків широкому колу осіб, що негативно впливає на рівень довіри до сфери фінансових послуг. Незважаючи на проведення Національним банком України інформаційних кампаній з платіжної безпеки, запровадження внутрішнього моніторингу фінансових транзакцій та перевірки клієнтської бази, все ж таки шахрайства з платіжними картками залишається одним із найбільш поширених протиправних діянь у фінансовій сфері.

Кібершахрайства з платіжною карткою це використання картки іншої особи для здійснення покупок або отримання готівкових авансів без відома чи згоди власника картки у кіберпросторі. Донедавна злочинці були націлені на фізичне викрадення платіжної картки, проте сьогодні все частіше використовуються цифрові засоби для викрадення номера кредитної картки та супровідної особистої інформації для здійснення незаконних операцій. У 2021 році більше 80% банківських шахрайств з використанням платіжної картки в країнах Європейського Союзу здійснено через мережу Інтернет [68].

У 2020 році обсяг збитків від шахрайства з банківськими картками становили 32,4 млрд доларів США, що майже втричі більше порівняно з 2011

роком (9,8 млрд доларів США), при цьому 46% з цих операцій здійснені на території США [69].

Стосовно України, то кількість банківських платіжних карток в обігу динамічно збільшується з кожним роком та станом на І півріччя 2021 року становила 41,3 млн штук [70], що фактично означає 2 банківські картки у розрахунку на 1 особу економічно активного віку. У 2022 році сума збитків від незаконних дій з платіжними картками становила 481 млн грн, що на 46% більше, ніж у 2021 році. Отже, можемо зазначити, що протидія шахрайством з банківськими картками в Україні є важливим питанням як для національного регулятора, так і фінансової установи та її клієнтів. Тому виникає об'єктивна необхідність удосконалення інструментів та прийомів ідентифікації шахрайських транзакцій, визначення вразливих місць в захисті інформаційної системи фінансової установи, а також запровадження системи попереджувальних заходів для скорочення кількості та частоти здійснення шахрайських платіжних операцій.

У межах даної дисертаційної роботи запропоновано методичний підхід до багатоетапної процедури ідентифікації фінансового шахрайства з платіжними картками з використанням методів нейронного моделювання. На відміну від існуючих підходів, передбачає побудову сукупності нейромережевих моделей та оцінювання їх параметрів, що в кінцевому підсумку дозволяє знайти оптимальну нейромережеву модель для оцінювання ризику платіжного шахрайства. Для апробації запропонованого наукоко-методичного підходу використано імітовані дані про банківські транзкції банківської установи з загальнодоступного ресурсу Kaggle [71]. Через конфіденційний характер набору даних уся конфіденційна інформація була видалена.

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 [72].

У межах даного дослідження запропоновано науково-методичний підхід для визначення шахрайських фінансових операцій з використанням платіжних карток, 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.

Для проведення проміжних розрахунків використано статистичний пакет Statistica. Загальний обсяг вибірки становив 549 645 спостереження, при цьому 2141 з них – шахрайські). Аналіз кожної фінансової транзакції буде здійснюватися на основі 8 індикаторів, перелік яких наведено у таблиці 2.1.

Таблиця 2.1 – Змінні, що використовуються визначення ризиків шахрайства

№	Назва змінної	Пояснення
1	Gender	Стать власника банківської картки (0 – жінка, 1 – чоловік)
2	Birth	Вік власника банківської картки
3	CC_num	Номер банківського рахунку
4	Amt	Сума транзакції, дол США
5	Category	Вид категорій товарів/послуг, які були об'єктом фінансової транзакції. 1 – платежі, пов'язані з оплатою у сфері персонального догляду (personal_care); 2 – платежі у сфері охорони здоров'я та спорту (health_fitness); 3 – інші платежі (misc_pos); 4 – платежі, пов'язані з поїдками (travel); 5 – платежі, пов'язані з оплатою дитячих товарів та товарів для домашніх тварин (kids_pets); 6 – оплата товарів (shopping_pos); 7 – оплата харчування (food_dining); 8 – платежі, пов'язані з оплатою речей для дому (home); 9 – платежі щодо оплати палива для транспорту (gas transport); 10 – поатежі у розважальній сфері (entertainment); 11 – оплата товарів (shopping_net); 12 – інші платежі (misc_net); 13 – платежі з оплати продуктів харчування (grocery_net); 14 – платежі з оплати продуктів харчування (grocery_pos)
6	Time	Година проведення операції (від 0 до 23)
7	Week date	День тижня проведення операції (від 1 до 7)
8	Fraud	Чи є операція шахрайською (0 – ні, 1 – так)

Джерело: авторський підхід

Фрагмент вхідної статистичної бази для оцінювання ризику фінансового шахрайства з платіжними картками в таблиці 2.2.

Таблиця 2.2 – Вхідні дані характеристику ризику кібершахрайств (фрагмент)

Week_date	CC_num	Amt	Birth	Time	Gender	Category	Fraud
7	2,29116E+15	2.86	53	12	1	1	0
7	3,57303E+15	29.84	32	12	0	1	0
7	3,59822E+15	41.28	51	12	0	2	0
7	3,59192E+15	60.05	34	12	1	3	0
7	3,52683E+15	3.19	66	12	1	4	0
7	3,04077E+13	19.55	30	12	0	5	0
7	2,13181E+14	133.93	71	12	0	2	0
7	3,58929E+15	10.37	49	12	0	1	0
7	3,59636E+15	4.37	48	12	1	6	0
7	3,5469E+15	66.54	65	12	0	7	0
7	2,24254E+15	7.01	25	12	1	7	0
7	5,71465E+11	42.4	45	12	1	5	0

Джерело: розрахунки автора

Одним із основних індикаторів, які дозволить навчити нейронну мережу, для вчасної ідентифікації ризику шахрайства з банківськими платіжними картками є саме «fraud». Тому проаналізуємо більш детальніше фінансові транзакції, що мають ознаки шахрайства у розрізі виокремлених ознак. На рисунку 2.1 зображено гістограми, які відображають кількість спостережень у відповідному параметрі, за якими зафіксовано факт шахрайства.

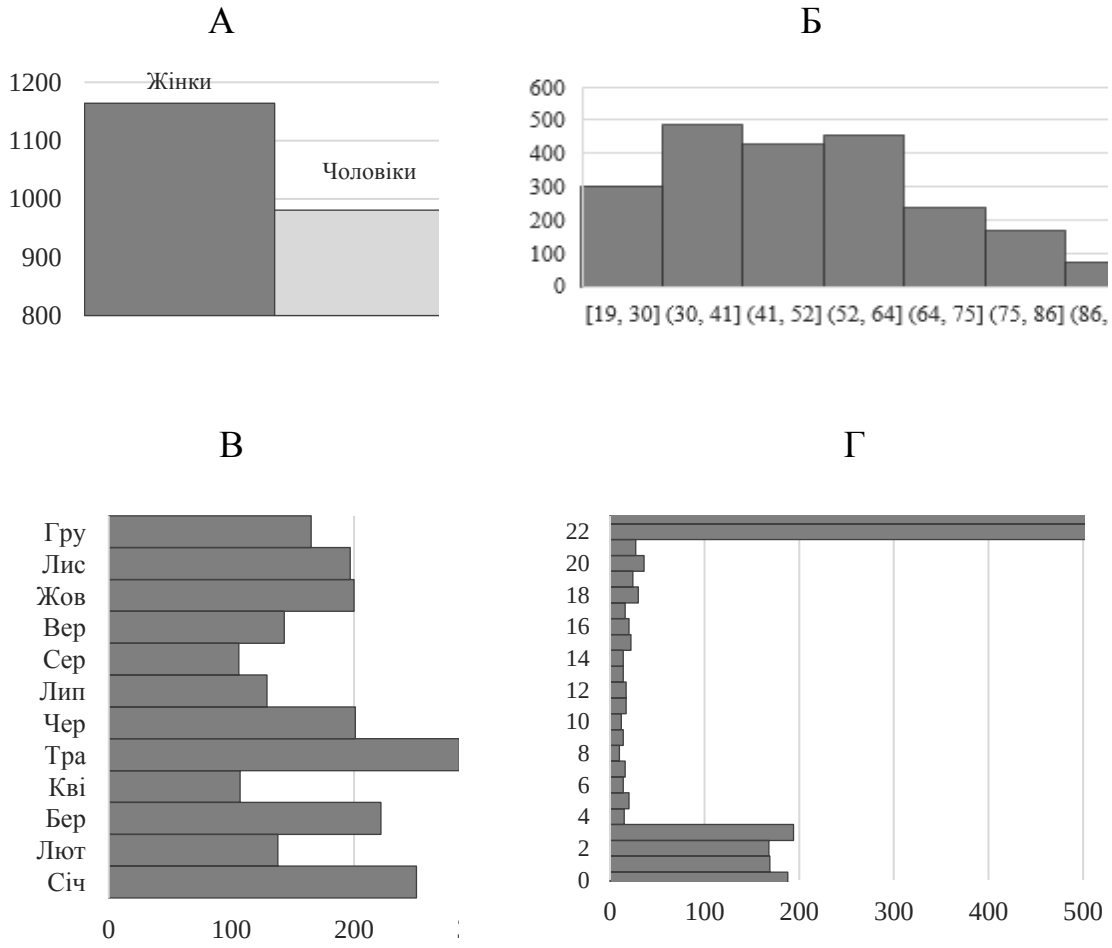


Рисунок 2.1 – Графік розподілу частоти транзакцій у розрізі досліджуваних ознак

Джерело: розрахунки автора

Дані рисунку 2.1 А наочно засвідчують, що 54.2% власників банківських карток, за допомогою яких здійснювалися шахрайські транзакції, були жінки. Середній вік держателів банківських карток, які здійснювали шахрайські фінансові транзакції, становив 50 років. Найбільший обсяг незаконних

транзакцій реалізується проходить на купівлю продуктів харчування та товарів.

Дані рисунку 2.1 Б демонструють, що найбільший обсяг шахрайських операцій було проведено у травні (286 операцій), березні (222) та січні (251). Загалом часова концентрація здійснення шахрайських фінансових операцій є досить рівномірною, проте незначний сплеск фіксується у неділю (17,4% від загального обсягу), тоді як в інші дні тижня: вівторок – 15,4%, четвер – 14,4%, понеділок – 14,1%, п'ятниця – 13,8%, середа й субота – по 12,4%). Половина 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), тоді як вночі (з 24.00 по 03.00) здійснено ще третину шахрайських транзакцій (рисунок 2.1 Б).

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 2.2.

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 7-6-1	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 7-5-1	0,59891	0,55348	0,00557	0,00582	BFGS 138	SOS	Tanh	Exponentia
4	MLP 7-5-1	0,59372	0,56108	0,00564	0,00575	BFGS 341	SOS	Exponentia	Exponentia
5	MLP 7-8-1	0,66196	0,63011	0,00489	0,00505	BFGS 338	SOS	Logistic	Tanh

Рисунок 2.2 – Результати побудови нейромережевих моделей залежності ризику кібершахрайств від факторів-складових

Джерело: розрахунки автора

Детальний аналіз даних рисунку 2.2 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 2.3).

	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	1,10	16,0000	0,0000	0,0000	1,0000	1,0000	0,0000
Maximum (Train)	4,992346E+1	12882,7	97,0000	23,0000	1,0000	16,0000	7,0000	1,0000
Mean (Train)	4,230247E+1	90,21	48,5640	13,2904	0,4028	7,8983	3,7824	0,0176
Standard deviation (Train)	1,319230E+1	171,91	17,7160	6,7401	0,4904	4,5225	2,1871	0,1318
Minimum (Test)	6,041621E+1	1,10	16,0000	0,0000	0,0000	1,0000	1,0000	0,0000
Maximum (Test)	4,992346E+1	13149,1	97,0000	23,0000	1,0000	16,0000	7,0000	1,0000
Mean (Test)	4,505042E+1	91,78	48,4880	13,2678	0,4065	7,8998	3,8178	0,0170
Standard deviation (Test)	1,356057E+1	198,21	17,6696	6,7477	0,4912	4,5268	2,2058	0,1294
Minimum (Overall)	6,041621E+1	1,10	16,0000	0,0000	0,0000	1,0000	1,0000	0,0000
Maximum (Overall)	4,992346E+1	13149,1	97,0000	23,0000	1,0000	16,0000	7,0000	1,0000
Mean (Overall)	4,285208E+1	90,52	48,5488	13,2859	0,4035	7,8986	3,7895	0,0175
Standard deviation (Overall)	1,326712E+1	177,48	17,7066	6,7416	0,4906	4,5233	2,1909	0,1313

Рисунок 2.3 – Описові статистики значень ризику кібершахрайств та факторів-складових

Джерело: розрахунки автора

Дані рисунку 2.3 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 четвер з 13.00 до 14.00 для оплати продуктів харчування.

Аналіз статистичних характеристик побудованих нейромережевих моделей, представлених на рисунку 2.4 та в додатку В, свідчить про високу якість моделей (незначну варіацію мінімальних та максимальних рівнів як в

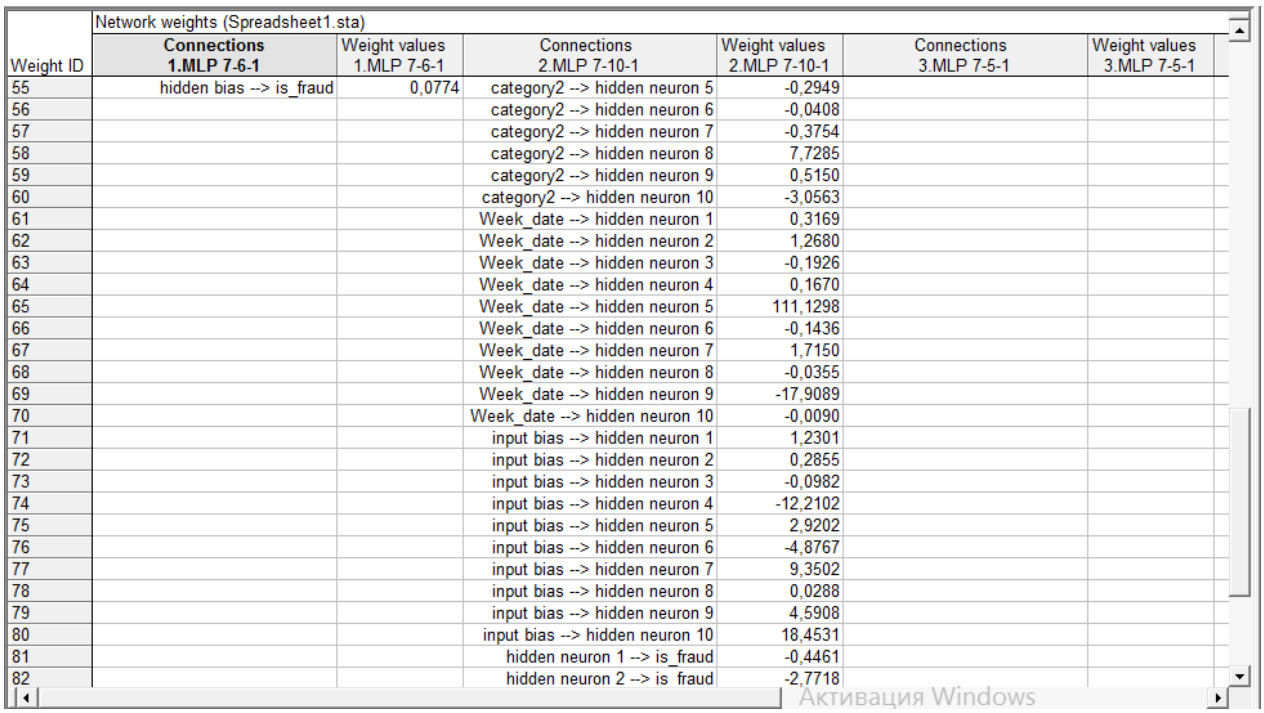
межах навчальної, так і контрольної та тестової вибірок) та незначний рівень чутливості моделей до зміни масштабу вхідних даних.

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 2.4 – 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

Джерело: розрахунки автора

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) (формула 2.1):

$$
\begin{aligned}
sn_1^{(2)} &= f(v_{11}^{(1)}p_1 + v_{12}^{(1)}p_2 + \cdots + v_{16}^{(1)}p_6 + v_{17}^{(1)}p_7 + s_1^{(1)}) \\
sn_2^{(2)} &= f(v_{21}^{(1)}p_1 + v_{22}^{(1)}p_2 + \cdots + v_{26}^{(1)}p_6 + v_{27}^{(1)}p_7 + s_2^{(1)}) \\
sn_3^{(2)} &= f(v_{31}^{(1)}p_1 + v_{32}^{(1)}p_2 + \cdots + v_{36}^{(1)}p_6 + v_{37}^{(1)}p_7 + s_3^{(1)}) \\
sn_4^{(2)} &= f(v_{41}^{(1)}p_1 + v_{42}^{(1)}p_2 + \cdots + v_{46}^{(1)}p_{16} + v_{47}^{(1)}p_7 + s_4^{(1)}) \\
sn_5^{(2)} &= f(v_{51}^{(1)}p_1 + v_{52}^{(1)}p_2 + \cdots + v_{56}^{(1)}p_6 + v_{57}^{(1)}p_7 + s_5^{(1)}) \\
sn_6^{(2)} &= f(v_{61}^{(1)}p_1 + v_{62}^{(1)}p_2 + \cdots + v_{66}^{(1)}p_6 + v_{67}^{(1)}p_7 + s_6^{(1)}) \\
sn_7^{(2)} &= f(v_{71}^{(1)}p_1 + v_{72}^{(1)}p_2 + \cdots + v_{76}^{(1)}p_6 + v_{77}^{(1)}p_7 + s_7^{(1)}) \\
sn_8^{(2)} &= f(v_{81}^{(1)}p_1 + v_{82}^{(1)}p_2 + \cdots + v_{86}^{(1)}p_6 + v_{87}^{(1)}p_7 + s_8^{(1)}) \\
sn_9^{(2)} &= f(v_{91}^{(1)}p_1 + v_{92}^{(1)}p_2 + \cdots + v_{96}^{(1)}p_6 + v_{97}^{(1)}p_7 + s_9^{(1)}) \\
sn_{10}^{(2)} &= f(v_{101}^{(1)}p_1 + v_{102}^{(1)}p_2 + \cdots + v_{106}^{(1)}p_6 + v_{107}^{(1)}p_7 + s_{10}^{(1)}) \\
\tilde{R} = h^{(3)} &= f(v_1^{(2)}sn_1^{(2)} + v_2^{(2)}sn_2^{(2)} + v_3^{(2)}sn_3^{(2)} + v_4^{(2)}sn_4^{(2)} + v_5^{(2)}sn_5^{(2)} \\
&\quad + v_6^{(2)}sn_6^{(2)} + v_7^{(2)}sn_7^{(2)} + v_8^{(2)}sn_8^{(2)} + v_9^{(2)}sn_9^{(2)} + v_{10}^{(2)}sn_{10}^{(2)} \\
&\quad + s^{(2)}
\end{aligned}
\tag{2.1}
$$

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 (формула 2.2):

$$OUT = tanh\,(net) \tag{2.2}$$

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

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 $h_1^{(2)}$.

Переходячи до опису моделі (2.1) на основі реальних даних отримаємо (формула 2.3):

$$\begin{gathered}
sn_1^{(2)} = f(0.0525p_1 + 1.8963p_2 + 0.1272p_3 + 0.6689p_4 + 0.9557p_5 \\
+ 0.8043p_6 + 0.3169p_7 + 1.2301) \\
sn_2^{(2)} = f(25.3785p_1 + 0.2291p_2 + 1.4357p_3 - 2.0158p_4 - 0.1579p_5 \\
- 0.8911p_6 + 1.2680p_7 + 0.2855) \\
sn_3^{(2)} = f(-1.1746p_1 + 0.4390p_2 + 9.3003p_3 + 0.3150p_4 - 0.0946p_5 \\
- 1.7476p_6 - 0.1926p_7 - 0.0982) \\
sn_4^{(2)} = f(-2.1610p_1 + 0.0998p_2 - 2.6001p_3 + 7.5426p_4 + 23.6766p_5 \\
- 0.2712p_{16} + 0.1670p_7 - 12.2102) \\
sn_5^{(2)} = f(-0.3174p_1 - 0.0434p_2 + 6.8840p_3 - 0.0640p_4 - 0.7207p_5 \\
- 0.2949p_6 + 111.1298p_7 + 2.9202) \\
sn_6^{(2)} = f(-0.4648p_1 - 42.3234p_2 + 5.1097p_3 - 0.4629p_4 - 1.0377p_5 \\
- 0.0408p_6 - 0.1436p_7 - 4{,}8767) \\
sn_7^{(2)} = f(-0.0748p_1 + 1.2498p_2 - 2.6516p_3 - 6.3181p_4 - 0.1759p_5 \\
- 0.3754p_6 + 1.7150p_7 + 9{,}3502) \\
sn_8^{(2)} = f(-0.0484p_1 + 2.7336p_2 + 0.4990p_3 + 0.3152p_4 - 5.2899p_5 \\
+ 7.7285p_6 - 0.0355p_7 + 0{,}0288) \\
sn_9^{(2)} = f(-42.5145p_1 + 0.3439p_2 - 0.7694p_3 + 0.0026p_4 + 0.1286p_5 \\
+ 0.5150p_6 - 17.9089p_7 + 4{,}5908) \\
sn_{10}^{(2)} = f(0.8976p_1 + 0.5628p_2 - 62.6995p_3 + 0.3332p_4 + 0.0173p_5 \\
- 3.0563p_6 - 0.0090p_7 + 18{,}4531)
\end{gathered} \tag{2.3}$$

$$\tilde{R} = h^{(3)}$$
$$= f(-0{,}4461sn_1^{(2)} - 2{,}7718sn_2^{(2)} + 2{,}3205sn_3^{(2)} - 0{,}0568sn_4^{(2)} + 0{,}1228sn_5^{(2)} + sn$$
$$+ 6{,}2373sn_6^{(2)} + 14{,}6218sn_7^{(2)} + 1{,}4856sn_8^{(2)} - 2{,}3082sn_9^{(2)} - 2{,}4977sn_{10}^{(2)}$$
$$- 2{,}3051$$

Заключним етапом розробленого науково-методичного 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 2.5.

	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	6,60	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 2.5 – Прогнозні значення ризику кібершахрайств

Джерело: розрахунки автора

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.

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

Таким чином, до проблеми шахрайства з платіжними картками необхідно підходити комплексно, на рівні держави із застосуванням сучасних методологій аналізу даних та залученням іноземних експертів. Оскільки великі дані стають доступними через фінансових установ, комп'ютерні алгоритми мають важливе значення для виявлення будь-якого шахрайства, та на основі цього розробити комплекс заходів для посиленого перевірки та контролю зі сторони внутрішньобанківського департаменту фінансового моніторингу.

2.2 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 [73, 74].

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 [75, 76, 77]. 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 [78]. 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 [79] 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 [80] 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 [81] 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. [82] 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. [83] 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 [84].

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 [85]. 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 (рисунок 2.6).

```
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 2.6 – 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 [86]. 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 (рисунок 2.7).

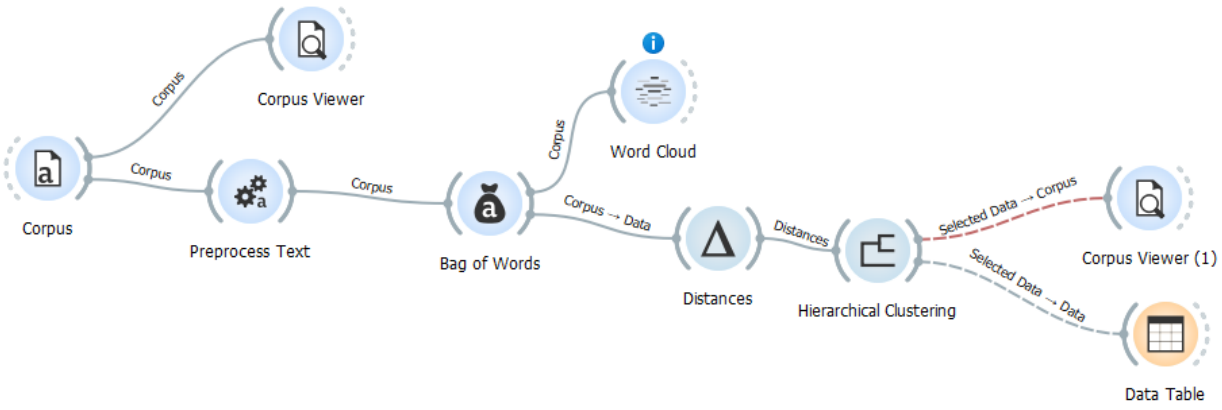


Рисунок 2.7 – Візуалізація моделі для кластеризації текстів

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 (рисунок 2.8).

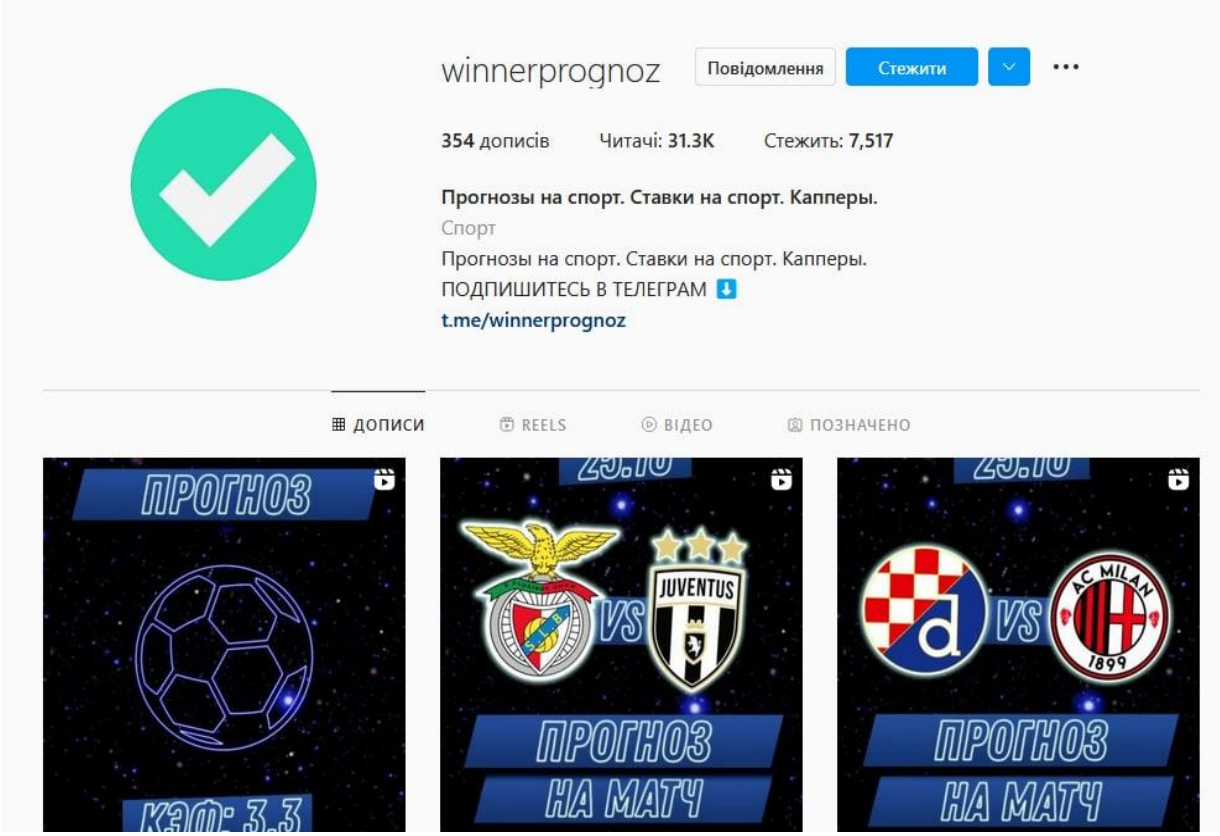


Рисунок 2.8 – Приклад арбітражної прокладки в Instagram

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 (рисунок 2.9).

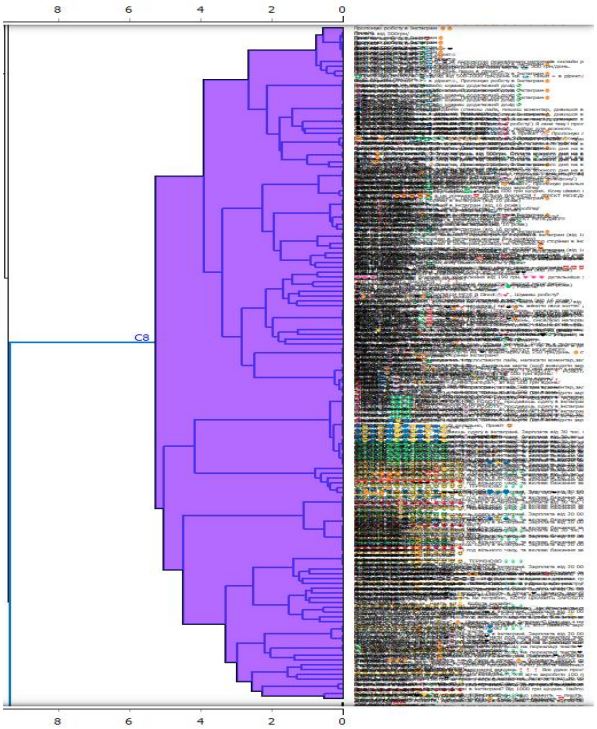


Рисунок 2.9 – Кластер зі спам-контентом

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 (рисунок 2.10).

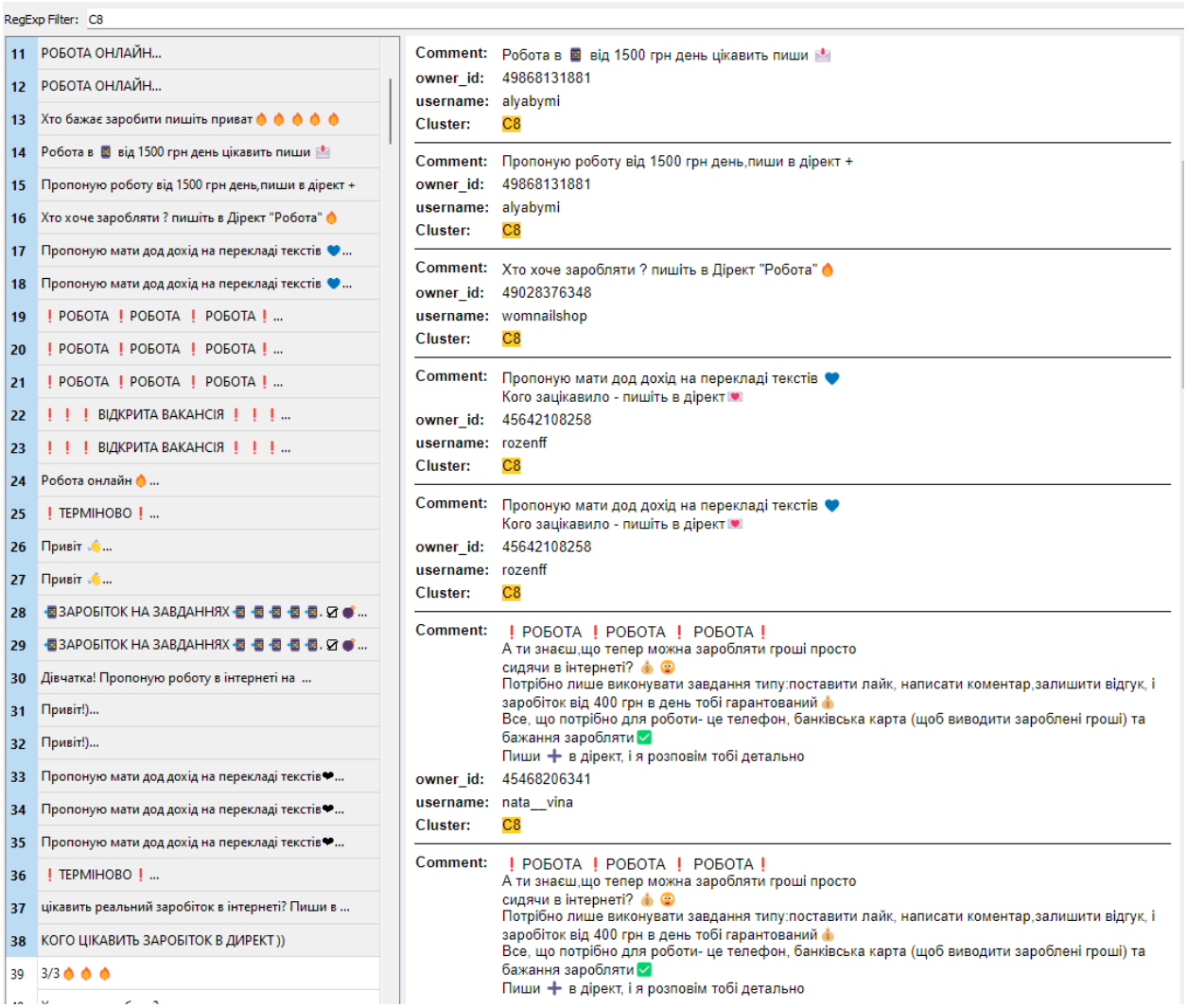


Рисунок 2.10 – Частина вмісту кластера C8

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 (рисунок 2.11).

З рисунка 2.11 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.

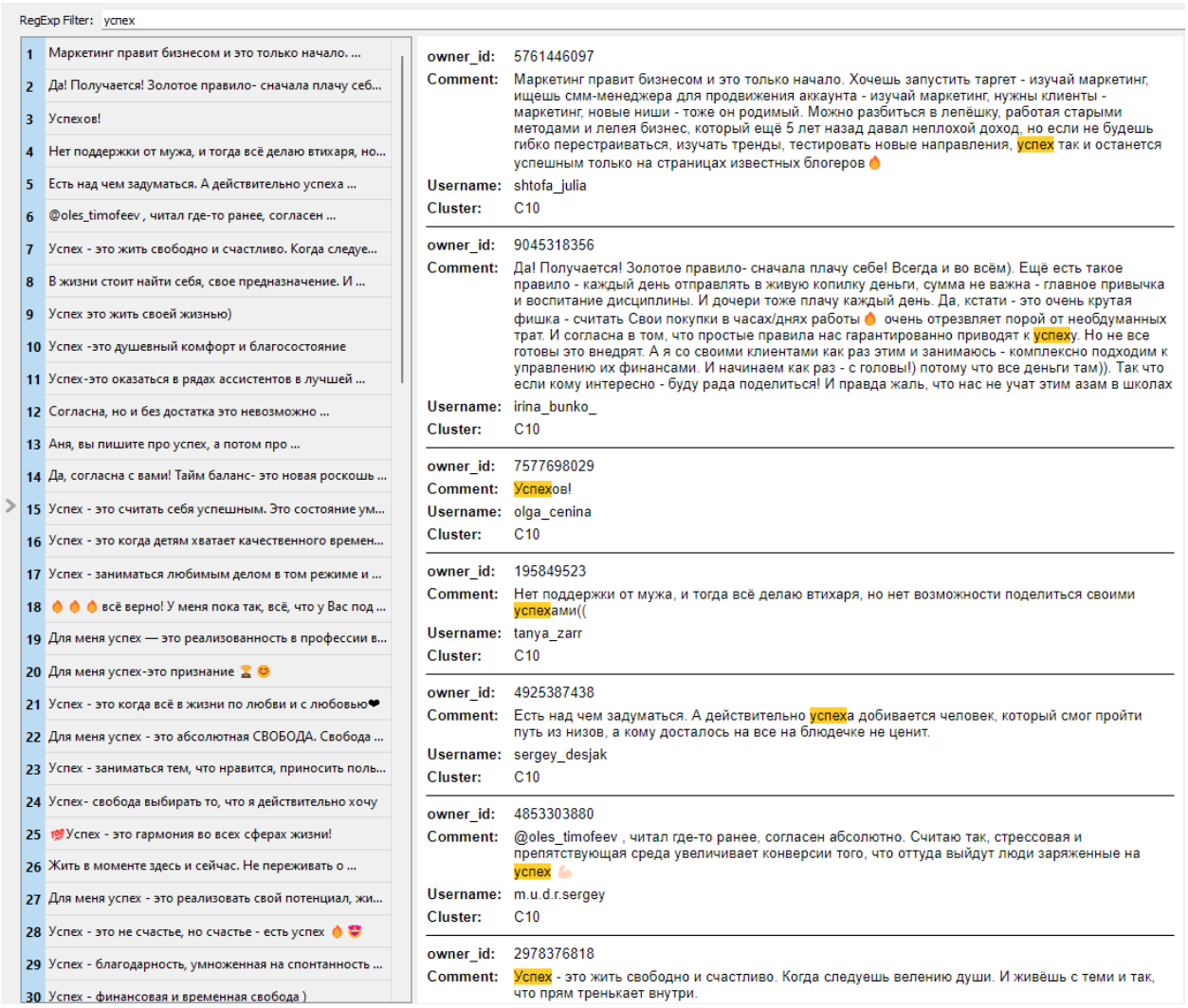


Рисунок 2.11 – Контент з ключовим словом «успех»

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.

2.3 Визначення імпульсів активізації фінансових злочинів, спричинених цифровізацією економіки

В останні роки фінансові інноваційні технології, а особливо FinTech інновацій набули особливого розвитку та поширення. Так, світові інвестиції у інновації FinTech за останнє десятиріччя зросли більш ніж у три рази. Застосування FinTech інновацій передбачає розвиток найсучасніших

технологічних можливостей: вбудовані мобільні системи обліку та обчислень даних, мобільні мережі, хмарні ресурси та обчислення, мобільна робота з великими базами даних, системи швидкого та комплексного аналізу великих масивів інформації. Важливе значення також має застосування FinTech для безперебійного вбудованого, дистанційного, online надання фінансових послуг та продуктів [87].

І хоча більшість світової спільноти вбачає в інноваціях FinTech значні переваги, не потрібно забувати і про виникаючі несприятливі наслідки використання FinTech у фінансовій сфері. Так як інноваційні досягнення можуть застосовуватись і злочинною сферою та шахраями для вчинення фінансово-економічних правопорушень. Отже, серед проблемних аспектів застосування FinTech інновацій можна виділити посилення небезпеки мережевих атак, поява загроз конфіденційності, вчинення протиправних фінансових та кібернетичних дій, а також організація та здійснення легалізації незаконних доходів, виявлення та розробка шахрайських схем обігу коштів, і навіть фінансування тероризму та розповсюдження зброї масового знищення [88, 89].

В таких умовах особливо актуальним постає питання визначення існуючих взаємозалежностей та взаємозв’язків між FinTech інноваціями, фінансовими, кібернетичними злочинами та легалізацією кримінальних доходів, для можливості вжиття відповідних регулюючих заходів.

На ряду з тим, що з питань впровадження фінансових інновацій, дослідження фінансових та кібернетичних злочинів, вже здійснено ряд вагомих внесків як зарубіжними, так і вітчизняними науковцями, але проблеми їх взаємозв’язку залишаються актуальними і сьогодні, та потребують запровадження сучасних ефективних методів їх вивчення та врегулювання.

Одним із таких методів можна виділити сплайн-моделювання - один з найефективніших сучасних способів побудови багатокомпонентних математичних функцій та рівнянь, тривимірних 3D моделей, де сплайни

представляють собою компонентні математичні функції, базові тривимірні криві, певний фундаментальний будівельний матеріал для побудови різноманітних складних функцій, тривимірних моделей. Створення сплайн-моделі передбачає побудову відповідного сплайн-каркасу, який далі виступає основою для формування почастинно заданої функції, сукупності декількох функцій, що задані множинністю значень, тривимірної геометричної поверхні, дуже складних тривимірних геометричних форм і об'єктів, тривимірних моделей [90]. Самі сплайн-лінії визначаються тривимірною сукупністю контрольних позицій точок у просторі, що задають форму та гнучкість кривої. Базовими інструментами сплайн-моделювання є алгебраїчні многочлени, математичні змінні, найпростіші функції, сплайн-примітиви (найпростіші об'єкти, з яких формується сплайн-модель), такі як: Arc, Circle, Donut, Ellipse, Helix, Line, NGon, Rectangle, Section, Star, Text та інші більш складні сплайн-елементи. Сплайн-моделювання характеризується рядом переваг: універсальність, широке застосування, можливість використання у різноманітних обчислювальних програмних комплексах, комп'ютерному моделюванні, високі обчислювальні спроможності, наявність апроксимативних властивостей, велика точність, у випадку необхідності масштабування у будь-яких межах якість сплайн-об'єкту не погіршується, гнучке налаштування, на будь-якому етапі є можливість зміни форм сплайн-об'єктів, простота реалізації обчислювальних функцій [91].

Для досягнення мети дослідження пропонується виконати три етапи.

На першому етапі науково-методичного підходу до застосування багатомірних адаптивних регресивних MAR-сплайнів до визначення впливу факторів фінансових технологій, фінансового моніторингу як банків так і страхових компаній, обсягів торгів на біржі на фінансові правопорушення, кібернетичні правопорушення та на легалізацію кримінальних доходів формується вхідна інформаційна база дослідження. Вона містить п'ять регресорів: X1 – Показник розвитку фінтех, який представлений питомою вагою кількості абонентів мережі інтернет в чисельності населення України,

X2 – Кількість повідомлень про підозрілі операції, взятих на облік Держфінмоніторингом, X3 – Загальний обсяг торгів на біржі за період, X4 – Показник діяльності страхових компаній (відношення розміру страхових виплат та страхових відшкодувань до суми страхових платежів), X5 – Показник діяльності банків (відношення грошових коштів та депозитів до розміру сукупних активів); та три регресанти: Y1 – Кількість кримінальних правопорушень за статтями 222 (Шахрайство з фінансовими ресурсами) та 222-1 (Маніпулювання на фондовому ринку України) Кримінального кодексу України, досудове розслідування у яких проводилося у звітному періоді, Y2 – Кількість кримінальних правопорушень за статтями 361 (Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп’ютерів), автоматизованих систем, комп’ютерних мереж чи мереж електрозв’язку), 361-1 (Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут), 361-2 (Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп’ютерах), автоматизованих системах, комп’ютерних мережах або на носіях такої інформації), 362 (Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп’ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї), 363 (Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється), 363-1 (Перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку) Кримінального кодексу України, досудове розслідування у яких проводилося у звітному періоді, Y3 – Кількість кримінальних правопорушень за статтею 209 (Легалізація (відмивання) доходів, одержаних

злочинним шляхом) Кримінального кодексу України, досудове розслідування у яких проводилося у звітному періоді. Для дослідження пропонується побудувати окремо сплайн-модель в розрізі кожного із зазначених регресантів, беручи в якості регресорів один і той же набір показників. В якості часового діапазону дослідження запропоновано обрати квартальні дані з 1 кварталу 2013 р. по четвертий квартал 2020 р.

На другому етапі науково-методичного підходу до застосування багатомірних адаптивних регресивних MAR-сплайнів до визначення впливу факторів фінтех, фінансового моніторингу як банків так і страхових компаній, обсягів торгів на фінансові правопорушення, кібернетичні правопорушення, легалізація кримінальних доходів проводиться дослідження динаміки поведінки як регресора, так і факторів. Для реалізації даного етапу побудуємо відповідні діаграми за допомогою інструментарію Statistics, Advanced Linear/Nonlinear Models, Time Series/Forecasting, Time Series ARIMA dialog. Даний етап виступає підготовчим для проведення безпосереднього сплайн-моделювання в розрізі визначення специфікації шуканої функціональної залежності (рисунки 2.12-2.13).

На третьому етапі науково-методичного підходу до застосування багатомірних адаптивних регресивних MAR-сплайнів до визначення впливу факторів впливу факторів фінтех, фінансового моніторингу як банків так і страхових компаній, обсягів торгів на фінансові правопорушення, кібернетичні правопорушення, легалізацію кримінальних доходів безпосередньо проводиться сплайн-моделювання.

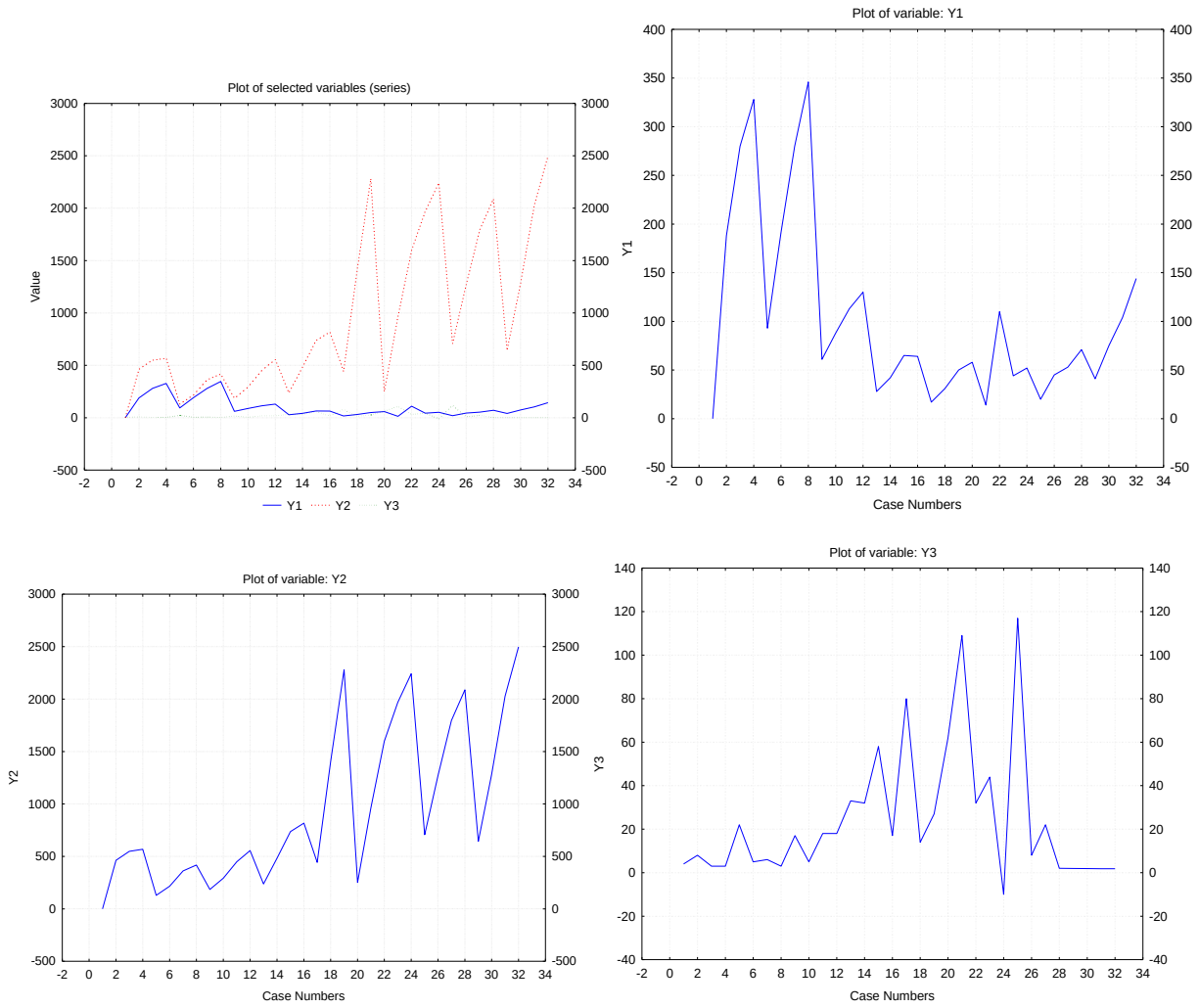


Рисунок 2.12 – Графіки динаміки регресандів визначення впливу факторів фінтех, фінансового моніторингу банків і страхових компаній, обсягів торгів на фінансові правопорушення, кібернетичні правопорушення, легалізація кримінальних доходів

Джерело: розроблено автором

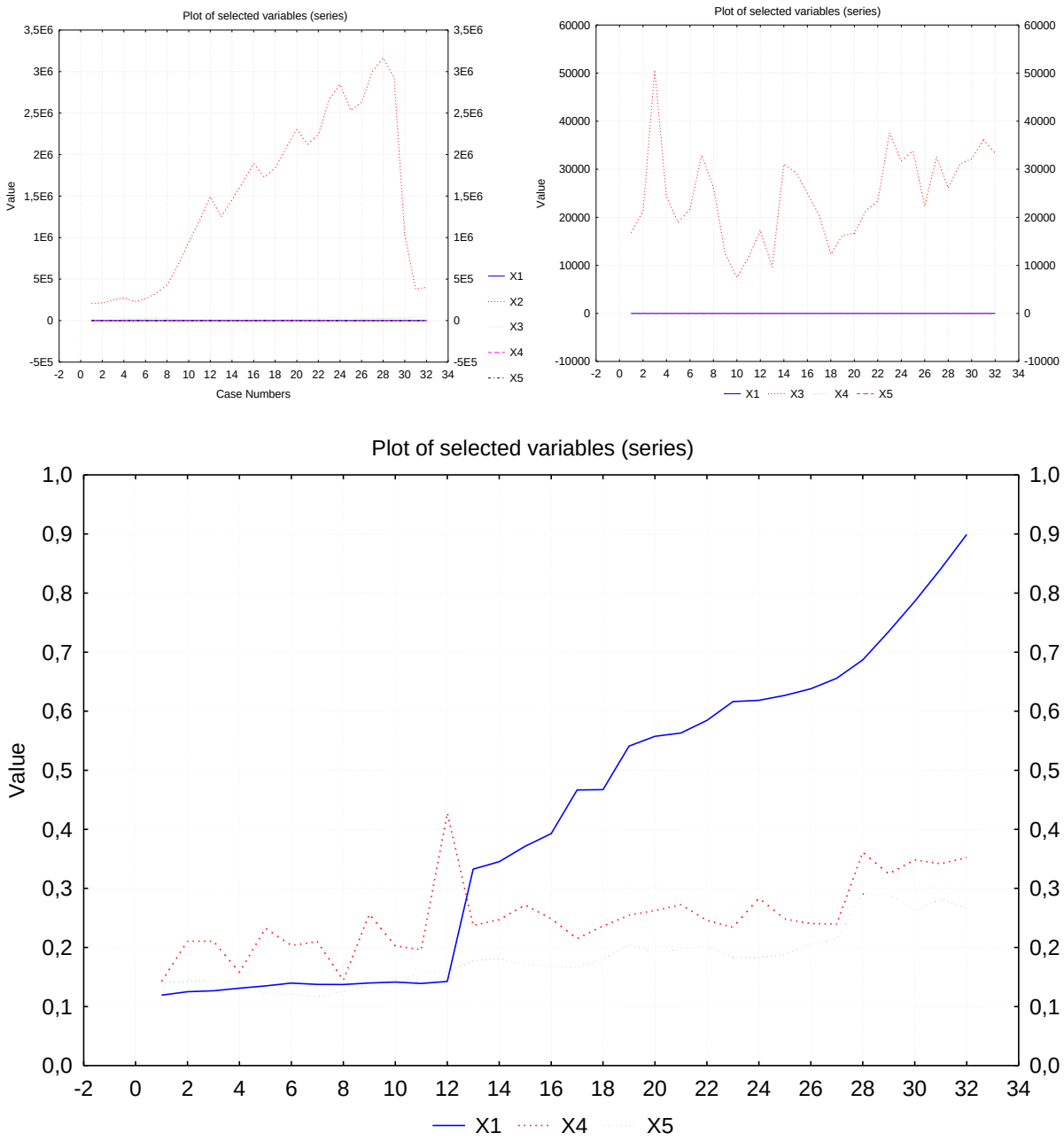


Рисунок 2.13 – Графіки динаміки регресорів визначення впливу факторів фінтех, фінансового моніторингу як банків так і страхових компаній, обсягів торгів на фінансові правопорушення, кібернетичні правопорушення, легалізація кримінальних доходів

Джерело: розроблено автором

При побудові регресивних MAR-сплайнів отримаємо наступні параметри (рисунок 2.14): кількість незалежних змінних – 5, кількість залежних змінних – 1, кількість термів – 5, кількість базисних функцій – 5, порядок взаємодії (кількість складових добутку базисних функцій) – 2, а також

кількість звернень до факторів-регресорів: найбільша – 2 до X1, X2, далі 1 – X3, крім того незначущими виявлено фактори X2 та X5. Коефіцієнти моделі відображені на рисунку 2.15.

Model specifications	Model Summary Value
Independents	5
Dependents	1
Number of terms	5
Number of basis functions	5
Order of interactions	2
Penalty	2,000000
Threshold	0,000500
GCV error	3153,123

Dependents	Number of References: References (to Basis Functions)
X1	2
X2	0
X3	1
X4	2
X5	0

Рисунок 2.14 – Параметри специфікації моделі та кількість звернень до релевантних факторів-регресорів

Джерело: розроблено автором

Coefficients, knots and basis functions	Model coefficients (Spreadsheet9.sta) NOTE: Highlighted cells indicate basis functions of type max(0, independent-knot), otherwise max(0, knot-independe: Coefficients Y1	Knots X1	Knots X2	Knots X3	Knots X4	Knots X5
Intercept	-15,34					
Term.1	-2200,1				0,23947	
Term.2	0,23			7464,63	0,23947	
Term.3	330,1	0,55754				
Term.4	250,8	0,37140				

Рисунок 2.15 – Коефіцієнти моделі та терми моделі впливу впливу факторів фінтех, фінансового моніторингу як банків так і страхових компаній, обсягів торгів на фінансові правопорушення у вигляді багатомірних адаптивних регресивних MAR-сплайнів

Джерело: розроблено автором

Таким чином, враховуючи представлені вище коефіцієнти, терми та параметри модель впливу фінтех, фінансового моніторингу як банків так і страхових компаній, обсягів торгів на фінансові правопорушення, кібернетичні правопорушення, легалізація кримінальних доходів у вигляді

багатомірних адаптивних регресивних MAR-сплайнів набуває вигляду (формула 2.4):

$$Y1 = -1{,}53418216810049e+001 - 2{,}20013777098280e+003*\max(0;\ 2{,}39473128974892e-001-X4) + 2{,}28135475716692e-001*\max(0;\ X3-7{,}46462968235000e+003)*\max(0;\ 2{,}39473128974892e-001-X4) + 3{,}30135483180817e+002*\max(0;\ 5{,}57544361572743e-001-X1) + 2{,}50799012955197e+002*\max(0;\ X1-3{,}71405276737145e-001) \quad (2.4)$$

Аналізуючи рівняння 2.4, робимо висновок, що діяльність страхових компаній веде до зменшення фінансових кримінальних правопорушень, за умови що показник діяльності страхових компаній буде менший за 0,2395, в іншому випадку, окремо діяльність страхових компаній не буде мати впливу. Мультиплікативний додатній ефект на фінансові правопорушення будуть мати загальний обсяг торгів на біржі з діяльністю страхових компаній, якщо обсяг торгів буде перевищувати 7464,63, а показник діяльності страхових компаній буде меншим за 0,2395. Додатній вплив на кількість фінансових правопорушень буде мати рівень розвитку фінтех, при тому, якщо значення показника буде від 0,3714 до 0,5575 то вплив буде у вигляді підсумку двох термів, а якщо перевищить значення у 0,5575 одиниць, то тільки одного.

В цілому, на кількість фінансових злочинів, по яких велось провадження в сторону зменшення впливає лише діяльність страхових компаній. Варто зазначити, що кількість переданих до держфінмоніторингу повідомлень та показник діяльності банків взагалі не мають впливу.

Адекватність побудованої моделі у вигляді багатомірних адаптивних регресивних MAR-сплайнів підтверджено: мінімальним значенням загального критерію якості моделі – узагальненого ковзного середнього помилки (GCV error), яке приймає значення 3153,12 (рисунок 2.14); коефіцієнт детермінації набуває значення 0,803, що свідчить про високу якість моделі (рисунок 2.16);

несуттєве відхилення фактичних та прогнозних значень кількості фінансових правопорушень, по яких було провадження у звітному періоді.

	Regression statistics (Spread
Regression statistics	Y1
Mean (observed)	100,812
Standard deviation (observed)	92,377
Mean (predicted)	100,812
Standard deviation (predicted)	82,777
Mean (residual)	0,000
Standard deviation (residual)	41,005
R-square	0,803
R-square adjusted	0,765

Рисунок 2.16 – Регресивні статистики залежності фінансових правопорушень від факторів у вигляді багатомірних адаптивних регресивних MAR-сплайнів

Джерело: розроблено автором

Переходячи до практичної реалізації моделі в розрізі залежності кібернетичних правопорушень від 5 факторів у вигляді багатомірних адаптивних регресивних MAR-сплайнів отримаємо наступні параметри (рисунок 2.17): кількість незалежних змінних – 5, кількість залежних змінних – 1, кількість термів – 8, кількість базисних функцій – 14, порядок взаємодії (кількість складових добутку базисних функцій) – 3, а також кількість звернень до факторів-регресорів: найбільша – 5 до X1, далі 4 – X3, 3 – X2, 2 – X5, крім того незначущим виявлено фактор X4.

	Model Summary
Model specifications	Value
Independents	5
Dependents	1
Number of terms	8
Number of basis functions	14
Order of interactions	3
Penalty	2,00000
Threshold	0,00050
GCV error	218725,
Prune	Yes

	Number of References to Each Predictor Number of times each predictor is referenced
Dependents	References (to Basis Functions)
X1	5
X2	3
X3	4
X4	0
X5	2

Рисунок 2.17 – Параметри специфікації моделі та кількість звернень до релевантних факторів-регресорів

Джерело: розроблено автором

Coefficients, knots and basis functions	Model coefficients (Spreadsheet9.sta) NOTE: Highlighted cells indicate basis functions of type max(0, independent-knot), otherwise max(0, knot-independ Coefficients Y2	Knots X1	Knots X2	Knots X3	Knots X4	Knots X5
Intercept	397,1					
Term.1	33871,(	0,37140				
Term.2	110777,:					0,18313
Term.3	-0,0	0,37140	183693			
Term.4	0,0	0,37140	183693	7464,6		
Term.5	-0,0		20944	7464,6		0,18313
Term.6	-1,8	0,37140		7464,6		
Term.7	-1,4	0,37140		26173,1		

Рисунок 2.18 – Коефіцієнти моделі та терми моделі впливу факторів фінтех, фінансового моніторингу як банків так і страхових компаній, обсягів торгів на кібернетичні правопорушення у вигляді багатомірних адаптивних регресивних MAR-сплайнів

Джерело: розроблено автором

Отримуємо таку математичну інтерпретацію моделі на основі коефіцієнтів рисунку 2.18 (формула 2.5):

$$Y2 = 3{,}97130455471352e{+}002 + 3{,}38716423357658e{+}004*\max(0;\ X1-3{,}71405276737145e{-}001) + 1{,}10777191998577e{+}005*\max(0;\ X5-1{,}83132301034698e{-}001) - 3{,}44120331174238e{-}002*\max(0;\ X1-3{,}71405276737145e{-}001)*\max(0;\ X2-1{,}83693800000000e{+}006) + 2{,}11976578551327e{-}006*\max(0;\ X1-3{,}71405276737145e{-}001)*\max(0;\ X2-1{,}83693800000000e{+}006)*\max(0;\ X3-7{,}46462968235000e{+}003) - 2{,}15529085157748e{-}006*\max(0;\ X2-2{,}09449000000000e{+}005)*\max(0;\ X3-7{,}46462968235000e{+}003)*\max(0;\ X5-1{,}83132301034698e{-}001) - 1{,}78240383752107e{+}000*\max(0;\ X1-3{,}71405276737145e{-}001)*\max(0;\ X3-7{,}46462968235000e{+}003) - 1{,}37560299832438e{+}000*\max(0;\ X1-3{,}71405276737145e{-}001)*\max(0;\ 2{,}61731749103700e{+}004-X3) \quad (2.5)$$

Аналізуючи детермінанти кіберзлочинів, констатуємо наступне. Показник розвитку фінтех буде мати додатній вплив у випадку набуття

значення більше 0,3714. При цьому, показники розвитку фінтех та кількості повідомлень про підозрілі операції в сукупності будуть впливати на зменшення результуючої ознаки, якщо перший буде більше 0,3714 а другий – більше 1836938. В разі до попередньої умови кількість торгів на біржі перевищить 7464,6297, то мультиплікативний ефект трьох показників буде впливати на зростання результуючої ознаки. Показник діяльності банків буде впливати на збільшення кіберзлочинів, якщо перевищить значення 0,1813. Мультиплікативний ефект одночасно показників X2, X3 та X5 за визначених умов буде впливати на зменшення кількості кіберзлочинів.

Адекватність побудованої моделі у вигляді багатомірних адаптивних регресивних MAR-сплайнів підтверджено: мінімальним значенням загального критерію якості моделі – узагальненого ковзного середнього помилки (GCV error), яке приймає значення 218725 (рисунок 2.17); коефіцієнт детермінації набуває значення 0,886, що свідчить про високу якість моделі (рисунок 2.19); несуттєве відхилення фактичних та прогнозних значень кіберзлочинів.

	Regression statistics (Spread
Regression statistics	Y2
Mean (observed)	935,093
Standard deviation (observed)	746,464
Mean (predicted)	935,093
Standard deviation (predicted)	702,487
Mean (residual)	0,000
Standard deviation (residual)	252,431
R-square	0,885
R-square adjusted	0,845

Рисунок 2.19 – Регресивні статистики залежності фінансових правопорушень від факторів у вигляді багатомірних адаптивних регресивних MAR-сплайнів

Джерело: розроблено автором

Переходячи до практичної реалізації моделі в розрізі залежності обсягів легалізації кримінальних доходів від 5 факторів у вигляді багатомірних адаптивних регресивних MAR-сплайнів отримаємо наступні параметри (рисунок 2.20): кількість незалежних змінних – 5, кількість залежних змінних

– 1, кількість термів – 3, кількість базисних функцій – 3, порядок взаємодії (кількість складових добутку базисних функцій) – 2, а також кількість звернень до факторів-регресорів: найбільша і однакова – 1 до X1, X2, X3, незначущими виявлено фактори X4 та X5.

Model specifications	Model Summary (Spreadsheet9.s Value
Independents	5
Dependents	1
Number of terms	3
Number of basis functions	3
Order of interactions	2
Penalty	2,00000
Threshold	0,00050
GCV error	767,732
Prune	Yes

Dependents	Number of References to Each Predictor (Spread Number of times each predictor is referenced (us References (to Basis Functions)
X1	1
X2	1
X3	1
X4	0
X5	0

Рисунок 2.20 – Параметри специфікації моделі та кількість звернень до релевантних факторів-регресорів

Джерело: розроблено автором

Coefficients, knots and basis functions	Model coefficients (Spreadsheet9.sta) NOTE: Highlighted cells indicate basis functions of type max(0, independent-knot), otherwise max(0, knot-independe Coefficients Y3	Knots X1	Knots X2	Knots X3	Knots X4	Knots X5
Intercept	32,9291					
Term.1	-0,0000		183693			
Term.2	15,0318	0,55754		22330,4		

Рисунок 2.21 – Коефіцієнти моделі та терми моделі впливу факторів фінтех, фінансового моніторингу як банків так і страхових компаній, обсягів торгів на кібернетичні правопорушення у вигляді багатомірних адаптивних регресивних MAR-сплайнів

Джерело: розроблено автором

Таким чином, враховуючи представлені вище коефіцієнти, терми та параметри модель впливу фінтех, фінансового моніторингу як банків так і страхових компаній, обсягів торгів на фінансові правопорушення, кібернетичні правопорушення, легалізація кримінальних доходів у вигляді багатомірних адаптивних регресивних MAR-сплайнів набуває вигляду (формула 2.6):

$$Y3 = 3{,}29291807569567e+001 - 1{,}77427285069972e-005*\max(0;\ 1{,}83693800000000e+006-X2) + 1{,}50318465753288e+001*\max(0;\ X1-5{,}57544361572743e-001)*\max(0;\ 2{,}23304254185900e+004-X3) \quad (2.6)$$

На кількість правопорушень з метою легалізації кримінальних доходів від'ємний вплив має кількість повідомлень про підозрілі операції, якщо вони менші за 1836938 одиниць, натомість додатній вплив буде мати мультиплікативний ефект фінтех та обсягів торгів на біржі, за умови що перший показник буде мати значення більше 0,5575 а другий – менше 22330,4254. Вплив інших показників не доведений.

Адекватність побудованої моделі у вигляді багатомірних адаптивних регресивних MAR-сплайнів підтверджено: мінімальним значенням загального критерію якості моделі – узагальненого ковзного середнього помилки (GCV error), яке приймає значення 767 (рисунок 2.20); коефіцієнт детермінації набуває значення 0,405, що свідчить про високу якість моделі (рисунок 2.22); несуттєве відхилення фактичних та прогнозних значень кількості правопорушень з метою легалізації кримінальних доходів.

	Regression statistics (Spread
Regression statistics	Y3
Mean (observed)	23,9527
Standard deviation (observed)	30,7883
Mean (predicted)	23,9527
Standard deviation (predicted)	19,5890
Mean (residual)	-0,0000
Standard deviation (residual)	23,7526
R-square	0,4048
R-square adjusted	0,3410

Рисунок 2.22 – Регресивні статистики залежності обсягів легалізації кримінальних доходів від факторів на у вигляді багатомірних адаптивних регресивних MAR-сплайнів

Джерело: розроблено автором

Проведене моделювання виокремлює тенденції взаємозв’язків кіберзлочинів, фінансових правопорушень та легалізації кримінальних доходів з узагальненими характеристиками розвитку фінтех, кількості поданих до держфінмоніторингу повідомлень про підозрілі операції та рівня розвитку ключових сфер фінансової діяльності: банків, страхових компаній та бірж цінних паперів.

Було визначено, що на фінансові злочини не мають впливу кількість переданих до держфінмоніторингу повідомлень про підозрілі операції та діяльність банківських установ. Натомість було визначено мультиплікативний вплив торгів на біржах цінних паперів та діяльності страхових компаній.

На кіберзлочини не має впливу діяльність страхових компаній, натомість з показником фінтех всі інші показники мали мультиплікативний ефект, в тому числі потрійний. Це вказує на те, що рівень цифровізації, розвитку фінтех стимулює інші сфери фінансової діяльності та надає нові можливості для кіберзлочинців.

Кількість злочинів з метою легалізації кримінальних доходів пояснюється кількістю поданих до держфінмоніторингу повідомлень про підозрілі операції та мультиплікативним впливом торгів на біржі і рівнем фінтех, що свідчить про значну кількість схем легалізації кримінальних доходів з використанням цінних паперів.

Отже, сучасний світ однієї сторони покладає великі надії на інновації, пов’язуючи з ними з покращення добробуту суспільства, посилення конкурентоздатності, прискорення темпів економічного зростання, а з іншого потерпає від активізації протиправних дій кіберзлочинців. Для перешкоджання та протидії фінансовим і кібернетичним злочинам, їх негативним наслідкам, необхідно постійно вживати певний комплекс ефективних регулюючих заходів. Серед них вагоме місце відводиться аналітичним процесам, що ґрунтуються на використанні моделювання фінансово-економічних процесів та тенденцій.

В свою чергу, сплайн-моделі такої взаємозалежності FinTech інновацій та фінансових і кібернетичних злочинів є досить гнучкими, та виступають достойною альтернативою стандартним математичним моделям, що можуть застосовуватись фінансовими посередниками для перешкоджання настання негативних наслідків для економічної системи. Сплайн-моделі надають гарні, точні кінцеві результати, прогнози по досліджуваним даним, демонструють одні з найкращих співвідношень вивчаємих функцій. Застосування на практиці сплайн-моделі взаємозалежності FinTech інновацій та фінансовими та кібернетичними злочинами за посередництва фінансових установ принесе користь і самим фінансовим посередникам, і користувачам фінансової системи, і державним регулюючим, наглядовим органам. Така модель може бути корисною та цікавою міжнародним організаціям, інвесторам, розробникам нормативних стандартів, банківським установам, іншим вченим, що проводять дослідження в цій сфері.

Для визначення взаємозв’язків між FinTech інноваціями, фінансовими злочинами, кіберзлочинами та легалізацією кримінальних доходів обрано структурне моделювання. Структурне моделювання передбачає собою методологію перевірки значної кількості можливих паралельно існуючих гіпотез щодо наявності причинно-наслідкових зв’язків, формування різних елементів в взаємопов’язану, комплексну, систематизовану структуру. При чому структурна модель призначена для аналізу складних взаємозв’язків між категоріями, визначеними для дослідження. За допомогою структурного моделювання можливо точно врахувати складні взаємозв’язки між складовими моделі. І за умови використання належних граничних умов, структурна модель створює базу для здійснення аналізу широкомаштабних відповідей моделі з огляду локальних характеристик її структури. Тобто згруповане вивчення сукупності окремих факторів надає індивідуальні методології вирішення індивідуальних напрямів проблемних питань.

1 етап. Формування вхідних показників оцінювання взаємозалежності FinTech інновацій та фінансовими та кібернетичними злочинами за

посередництва фінансових установ в розрізі наступних груп: фінтех складова, фінансові злочини, кіберзлочини та легалізація кримінальних доходів, враховуючи, що показник співвідношення фінансових активів до ВВП (FA/GDP) буде включено до опису кожної із зазначених груп. Таким чином, для опису фінтех складової обрано наступні два показники: Fintech1 – кількість абонентів мобільного зв'язку на 1 тис. населення; Fintech2 - показник фінтех, питома вага абонентів інтернету в населенні України; фінансові злочини, відповідно: FC1 – кількість обліковано фінансових злочинів у звітному періоді (статті 222 та 222-1 ККУ); FC2 - кількість фінансових злочинів, які передано до суду з обвинувальним актом; кіберзлочини: CC1 - кількість обліковано кіберзлочинів у звітному періоді (статті 361,361-1, 361-2, 362, 363, 363-1 ККУ); CC2 - кількість фінансових злочинів, які передано до суду кіберзлочинів з обвинувальним актом; а також легалізація кримінальних доходів – такі показники, як; AML1 – кількість обліковано з легалізації кримінальних доходів (стаття 209 ККУ); AML2 – кількість фінансових злочинів, які передано до суду обвинувальних актів з легалізації кримінальних доходів. Розглянемо статистичну базу в розрізі вхідної бази дослідження у вигляді квартальних часових рядів з 2013 по 2020 рр. (таблиця 2.3).

2 етап. Структурне моделювання взаємозалежності FinTech інновацій та фінансовими та кібернетичними злочинами за посередництва фінансових установ. На основі використання змінних, введених на першому етапі при формалізації вхідної бази дослідження, виникає необхідність їх класифікації на екзогенні та ендогенні, а також визначенні на основі введених змінних латентних (неявно заданих) змінних, які і дозволять описати взаємозалежність FinTech інновацій та фінансовими та кібернетичними злочинами за посередництва фінансових установ. Так, всі приведені змінні на першому етапі – це спостережувані (явні) змінні, оскільки їх значення приведені у файлі даних [68, 69]. Але в моделі повинні бути присутні ще й латентні змінні, якими пропонується обрати: Fintech – рівень розвитку FinTech інновацій, FC – рівень розвитку фінансових злочинів, CC – рівень розвитку кібернетичних

правопорушень, AML – рівень розвитку системи протидії легалізації кримінальних доходів. Явні змінні Fintech1, Fintech2, FC1, FC2, CC1, CC2, AML1, AML2 відносяться до ендогенних. Оскільки фінтах інновації впливають на фінансові та кібернетичні злочини та легалізацію кримінальних доходів, кібернетичні злочини впливають на фінансові злочини та легалізацію кримінальних доходів, а легалізація кримінальних доходів впливає на фінансові злочини, то латентну змінну Fintech можна вважати екзогенною, а латентні змінні FC, CC, AML – ендогенними.

Таблиця 2.3 – Вхідні показники оцінювання взаємозалежності FinTech інновацій та фінансовими та кібернетичними злочинами за посередництва фінансових установ

Квартал/ Рік	FA/GDP	Fintech 1	Fintech 2	FC1	FC2	CC1	CC2	AML 1	AML2
I 2013	6,539	1,344	0,119	0	0	0	0	4	1
II 2013	5,708	1,357	0,125	188	51	463	33	8	1
III 2013	5,237	1,364	0,127	280	109	549	200	3	1
IV 2013	5,224	1,375	0,131	328	164	568	247	3	1
I 2014	7,184	1,373	0,135	93	46	129	19	22	3
II 2014	6,144	1,381	0,140	191	115	216	77	5	1
III 2014	5,635	1,410	0,138	280	165	362	157	6	0
IV 2014	5,565	1,425	0,137	346	206	418	191	3	2
I 2015	7,885	1,436	0,140	61	28	185	35	17	2
II 2015	6,105	1,442	0,141	88	43	292	90	5	0
III 2015	4,976	1,429	0,139	113	61	449	218	18	1
IV 2015	5,011	1,420	0,142	130	67	556	151	18	0
I 2016	6,704	1,339	0,333	28	8	238	109	33	0
II 2016	5,620	1,329	0,345	42	23	483	172	32	0
III 2016	4,596	1,348	0,371	65	20	736	307	58	1
IV 2016	4,419	1,332	0,393	64	26	818	455	17	1
I 2017	5,408	1,324	0,467	17	7	443	101	80	1
II 2017	4,850	1,326	0,467	31	11	1404	469	14	2
I 2019	4,160	1,277*	0,627	20	12	707	351	117	0
II 2019	3,600	1,274*	0,638	45	26	1271	796	8	2
III 2019	2,995	1,271*	0,656	53	35	1796	1142	22	1
IV 2019	3,158	1,269*	0,687	71	41	2088	1248	2	9
I 2020	4,457	1,266*	0,735*	41	31	643	301	1,947*	9,794*
II 2020	4,413	1,263*	0,786*	75	53	1283	611	1,896*	10,657*
III 2020	3,417	1,261*	0,841*	104	72	2027	990	1,846*	11,597*
IV 2020	3,344*	1,258*	0,899*	144	92	2498	1484	1,798*	12,620*

Примітка: * - значення отримане шляхом проведення прогнозування за допомогою методу середнього темпу зростання.

Для побудови моделі структурних рівнянь взаємозалежності FinTech інновацій та фінансовими та кібернетичними злочинами за посередництва фінансових установ скористаємось програмним пакетом Statistica Portable командаю Statistics/Advanced Linear/Nonlinear Models/Structural Modeling. В результат отримаємо рисунок 2.23.

На основі даних рисунку 2.23, а саме параметрів лінійних однофакторних та багатофакторних регресійних моделей залежності між латентними змінними, а також залежності між явними та латентними змінними побудуємо шукану систему структурних рівнянь (формула 2.7).

$$\begin{cases} \frac{FA}{GDP} = -16.622 \cdot Fintech \; Fintech1 = -0.047 \cdot Fintech + 0.002 \; Fintech2 \\ = 0.252 \cdot Fintech + 0.003 \; \frac{FA}{GDP} = FC + 6.146 \; FC1 \\ = 556.553 \cdot FC \; FC2 = 290.105 \cdot FC + 292.109 \; \frac{FA}{GDP} \\ = CC + 6.146 \; CC1 = 58.179 \cdot CC + 220119.130 \; CC2 \\ = 35.761 \cdot CC + 66949.988 \; \frac{FA}{GDP} = AML + 6.146 \; AML1 \\ = 0.312 \cdot AML + 939.984 \; AML2 = 0.431 \cdot AML + 7.568 \; FC \\ = -7.660 \cdot Fintech + 0.274 \cdot CC + 0.823 \cdot AML + 0.013 \; CC \\ = 10.055 \cdot Fintech + 0.234 \; AML \\ = 7.444 \cdot Fintech - 0.156 \cdot CC + 0.001 \end{cases} \quad (2.7)$$

Таким чином, на основі системи (рисунок 2.23) можна зробити наступні висновки:

− при збільшенні рівня розвитку фінтех інновацій на 1% рівень фінансових правопорушень буде зменшуватись на 7,66%, тобто між зазначеними латентними змінними спостерігається обернений зв’язок;

− зростання кібернетичних правопорушень на 1% супроводжується зростанням фінансових правопорушень на 0,274% відповідно;

	Model Estimates (Spreadsheet1.sta)			
	Parameter Estimate	Standard Error	T Statistic	Prob. Level
(Fintech)-1->[FA/GDP]	-16,622	1,812	-9,174	0,000
(Fintech)-2->[Fintech1]	-0,047	0,011	-4,477	0,000
(Fintech)-3->[Fintech2]	0,252	0,034	7,327	0,000
(DELTA1)-->[FA/GDP]				
(DELTA2)-->[Fintech1]				
(DELTA3)-->[Fintech2]				
(DELTA1)-4-(DELTA1)	0,000	0,000		
(DELTA2)-5-(DELTA2)	0,002	0,001	3,742	0,000
(DELTA3)-6-(DELTA3)	0,003	0,004	0,742	0,458
(FC)-->[FA/GDP]				
(FC)-7->[FC1]	556,553	5063,45	0,110	0,912
(FC)-8->[FC2]	290,105	2639,42	0,110	0,912
(CC)-->[FA/GDP]				
(CC)-9->[CC1]	58,179	11,500	5,059	0,000
(CC)-10->[CC2]	35,761	0,000		
(AML)-->[FA/GDP]				
(AML)-11->[AML1]	0,312	0,956	0,326	0,744
(AML)-12->[AML2]	0,431	0,112	3,853	0,000
(EPSILON1)-->[FA/GDP]				
(EPSILON2)-->[FC1]				
(EPSILON3)-->[FC2]				
(EPSILON4)-->[CC1]				
(EPSILON5)-->[CC2]				
(EPSILON6)-->[AML1]				
(EPSILON7)-->[AML2]				
(EPSILON1)-13-(EPSILON1	6,146	2,219	2,770	0,006
(EPSILON2)-14-(EPSILON2	0,000	0,000		
(EPSILON3)-15-(EPSILON3	292,109	74,196	3,937	0,000
(EPSILON4)-16-(EPSILON4	220119,13	61580,76	3,574	0,000
(EPSILON5)-17-(EPSILON5	66949,98	19388,36	3,453	0,001
(EPSILON6)-18-(EPSILON6	939,984	238,788	3,936	0,000
(EPSILON7)-19-(EPSILON7	7,568	2,005	3,776	0,000
(ZETA1)-->(FC)				
(ZETA2)-->(CC)				
(ZETA3)-->(AML)				
(ZETA1)-20-(ZETA1)	0,013	0,383	0,035	0,972
(ZETA2)-21-(ZETA2)	0,234	1,678	0,139	0,889
(ZETA3)-22-(ZETA3)	0,001	0,151	0,007	0,995
(Fintech)-23->(FC)	-7,660	0,000		
(Fintech)-24->(CC)	10,055	1,858	5,412	0,000
(Fintech)-25->(AML)	7,444	0,000		
(CC)-26->(FC)	0,274	0,000		
(CC)-27->(AML)	-0,156	0,000		
(AML)-28->(FC)	0,823	0,113	7,259	0,000

Рисунок 2.23 – Фрагмент таблиці обчислених параметрів моделі взаємозалежності FinTech інновацій та фінансовими та кібернетичними злочинами за посередництва фінансових установ

− аналогічно описаному вище прямому зв’язку між фінансовим та кібернетичними правопорушеннями, між рівнями легалізації кримінальних доходів та фінансовими правопорушеннями спостерігається прямий зв’язок: при збільшенні рівня легалізації кримінальних доходів на 1% рівень фінансових правопорушень буде збільшуватись на 0,823%;

− якщо порівнювати темпи варіації фінансових правопорушень, кібернетичних правопорушень, фінтех інновацій та легалізації кримінальних доходів, необхідно відмітити, що лише при зростанні фінтех інновацій фінансові правопорушення будуть зменшуватись значно вищими темпами. В розрізі впливу кібернетичних правопорушень та легалізації кримінальних доходів на фінансові правопорушення темпи варіації результативної ознаки будуть меншими за варіацію факторних;

− темп варіації кібернетичних правопорушень значно перевищує темп варіації фінтех інновацій, про що свідчить відповідний коефіцієнт передостаннього рівняння системи (формула 2.7), а саме при зростання рівня фінтех інновацій на 1% рівень кібернетичних правопорушень буде зростати на 10,06%;

− при збільшенні рівня фінтех інновацій на 1%, рівень легалізації кримінальних доходів буде збільшуватись значно вищими темпами, тобто на 7,44% на відміну від взаємозалежності між кібернетичним правопорушеннями та легалізацією кримінальних доходів, де зв’язок обернений і має значно менші темпи: при зростанні кібернетичних правопорушень на 1% рівень легалізації кримінальних доходів буде зменшуватись на 0,156% відповідно.

3 етап. Перевірка адекватності та точності моделі взаємозалежності FinTech інновацій та фінансовими та кібернетичними злочинами за посередництва фінансових установ. Для реалізації даного етапу визначимо базові сумарні статистики (рисунок 2.24), матрицю рефлектор (рисунок 2.25), а також перевірку відповідності залишків моделі нормальному закону розподілу (рисунок 2.26).

	Basic Summary Statistics (Spr
	Value
Discrepancy Function	5,123
Maximum Residual Cosine	0,388
Maximum Absolute Gradient	159,12(
ICSF Criterion	1,818
ICS Criterion	0,858
ML Chi-Square	158,80-
Degrees of Freedom	23,00(
p-level	0,00(
RMS Standardized Residual	0,548

Рисунок 2.24 – Показники адекватності та точності моделі

Як видно з рисунку 2.24 Maximum Residual Cosine (максимум косинуса залишків) прямує до 0, що свідчить що ітераційний процес завершився успіхом. Значення ICSF Criterion та ICS Criterion близькі до 0, що свідчить що побудована модель є стійкою до множення на постійний маштабуючий множник та до змін масштабу.

Оскільки p-level для Chi-square статистики менше за 0,05, то відхиляємо нульову гіпотезу при рівні значущості 0,95, тобто гіпотезу про відсутність структурної взаємозалежності fintech інновацій, фінансових, кібернетичних злочинів та легалізації кримінальних доходів за посередництва фінансових установ.

За допомогою Матриці-рефлектора (рисунок 2.25) проводимо перевірку моделі на інваріантність, тобто визначаємо стійкість моделі відповідно до зміни масштабу початкових даних.

	Reflector Matrix (Spreadsheet1.sta)								
	FA/GDP	Fintech1	Fintech2	FC1	FC2	CC1	CC2	AML1	AML2
FA/GDP	0,858	-0,002	0,009	6,928	3,585	56,325	37,076	-0,814	0,042
Fintech1	-2,611	0,605	0,761	-267,77:	-184,68	587,51	438,34-	48,85-	1,242
Fintech2	0,147	0,13-	0,29-	251,02	103,28:	1379,87	619,28:	-120,76	-4,799
FC1	-0,000	-0,000	0,002	-0,192	-0,169	0,689	1,108	0,055	0,022
FC2	0,007	0,000	-0,003	-0,031	0,067	-4,129	-3,807	0,23-	-0,06-
CC1	0,001	-0,000	-0,000	-0,04-	-0,018	0,067	-0,352	0,023	0,000
CC2	0,002	-0,000	-0,000	-0,080	-0,039	-1,15-	0,068	0,038	0,001
AML1	0,001	0,000	-0,001	1,201	0,706	4,55-	2,101	-0,001	0,025
AML2	-0,079	-0,001	-0,00-	-9,47-	-6,205	8,727	11,87-	3,811	0,051

Рисунок 2.25 – Матриця-рефлектор

Для стійкої моделі характерна близькість елементів даної матриці один до одного. Аналіз матриці рефлектора взаємозалежності FinTech інновацій та

фінансовими та кібернетичними злочинами за посередництва фінансових установ свідчить про стійкість побудованої моделі до зміни масштабу вимірювання початкових даних.

Проаналізувавши Normal Probability Plot - нормальний імовірнісний графік (рисунок 2.26), підтвердимо припущення про те, що залишки моделі є якісні та мають близький до нормального закон розподілу, так як на графіку вони розміщуються близько до прямої.

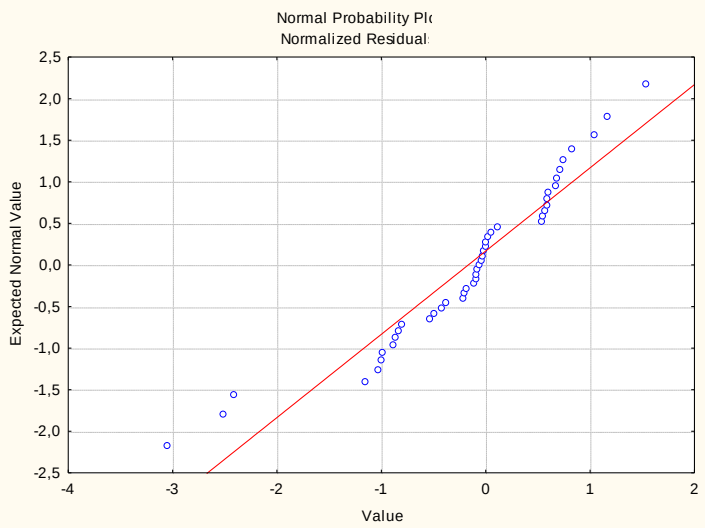


Рисунок 2.26 – Нормальний імовірнісний графік

З огляду на вищенаведений аналіз, робимо висновок про адекватність побудованої моделі.

Зазначимо, що наразі фінансовим технологіям, таким як інновації FinTech, віддається суттєва перевага. Їх використання швидко зростає. В результаті чого подальший розвито фінансово-економічних процесів потребує запровадження нових правил і методик, що зможуть поєднувати як позитивні характеристики та ефекти від FinTech інновацій, так і негативні аспекти, що пов’язують залежність FinTech інновацій з фінансовими, кібернетичними злочинами, легалізацією кримінальних доходів за посередництва фінансових установ.

2.4 Науково-методичний підхід до ідентифікації критичних зон кіберзагроз фінансовому сектору економіки України

Справедливо зауважити, що в подальшому актуальності набуває розробка методичних засад, які виступатимуть основою формування сценаріїв поведінки органів виконавчої влади та, безпосередньо, суб'єктів господарювання в залежності від рівня кіберзагроз фінансовому сектору економіки України, а також під впливом рівня діджиталізації фінансового сектору й технологічного розвитку. Починаючи опис запропонованого науково-методичного підходу доцільно зауважимо декілька базових положень. Перше, дослідження кіберзагроз в умовах цифровізації національної економіки запропоновано прослідковувати через призму фінансового сектору, оскільки цей сектор є основним каналом поширення та подальшої мультиплікації шоків в державі. Крім того, справедливо зазначити, що фінансова система України наразі є однією з найбільш діджиталізованих систем у світі та акумулює не тільки фінансову, але й персональну інформацію більшості громадян держави. Тому кібератаки зазначеної системи, призведуть не тільки до фінансових збитків, а й до втрати приватності українців. Друге, прийнято рішення розглядати стійкість економічних агентів до дії внутрішніх та зовнішніх шоків в умовах цифровізації фінансового сектору економіки України за допомогою ідентифікації взаємозв'язків у трикутнику «діджиталізація фінансового сектору–технологічний розвиток–кіберзагрози».

Обрання вище зазначених трьох складових дослідження раціональної поведінки економічних агентів в умовах цифровізації фінансового сектору національної економіки обумовлено сучасним трендом розвитку цього сектору, а саме тотальним оцифровуванням фінансової інформації з метою активізації бізнес-процесів фінансових корпорацій (віртуального банкінгу, інтернет-страхування, інтернет-трейдингу, тощо). Так, розглядаючи діджиталізацію можливо досягти розуміння про рівень цифрової трансформації фінансового сектору, тобто ступінь проникнення інноваційних

технологій до бізнес-процесів банків та інших фінансових посередників. У свою чергу, швидкість та інтенсифікація діджиталізації фінансового сектору, залежить від технологічної розвиненості інформаційної системи України. Рівень забезпеченості суспільства високоякісними та сучасними інформаційно-комунікаційними технологіями є основою розвитку будь-яких діджитал-послуг та діджитал-продуктів. Паралельно з цим, справедливо зазначити, що кіберзагрози виступають, так би мовити, похідними від діджиталізації та технологічного розвитку, оскільки до активної цифровізації усіх сфер життя суспільства кібератак не могло існувати по своїй суті. Таким чином, вершини трикутнику «діджиталізація фінансового сектору–технологічний розвиток–кіберзагрози» є не тільки взаємопов'язаними, але й взаємозалежними. Отже, розглянемо детально кожен з шести етапів розробки та практичної реалізації науково-методичного підходу до побудови сценаріїв поведінки економічних агентів в умовах цифровізації фінансового сектору національної економіки щодо забезпечення їх стійкості до зовнішніх та внутрішніх загроз.

На першому етапі охарактеризуємо окремо кожну зі складових трикутнику «діджиталізація фінансового сектору–технологічний розвиток–кіберзагрози». Так, діджиталізацію фінансового сектору опишемо за допомогою таких показників, як: частка громадян, що користуються онлайн банкінгом; співвідношення безготівкових карткових операцій до загальної кількості трансакцій; частки переказів з картки на картку; кількості депозитних рахунків на 1000 осіб дорослого населення. Перше, ніж надавати пояснення кожному з показників характеристики діджиталізації фінансового сектору зауважимо, що всі вони відносяться до банківської системи, оскільки для України характерна банкоцентрична модель фінансового ринку. Тобто банки концентрують переважну більшість вільних фінансових ресурсів суб'єктів господарювання й населення (у вигляді депозитів) та в подальшому приймають незалежні управлінські рішення щодо їх інвестування. Обсяги фінансових ресурсів, які перерозподіляються через небанківські фінансові

установи майже не впливають на фінансову безпеку України та не мають вирішального значення для розвитку національної економіки. Тобто, саме банки та їх рівень діджиталізації є рушійною силою цифровізації всієї фінансової системи України. Отже, зупиняючись на кожному з показників більш детально, зазначимо, що частка громадян, які користуються онлайн банкінгом відображає рівень залученості населення України до банківських цифрових технологій. Саме попит демонструє наскільки діджитал-послуги та діджитал-продукти банків є корисними, популярними та затребуваними, оскільки тільки якісно розроблені банківські сервіси можуть зацікавити клієнтів й збільшувати їх чисельність з кожним роком. Співвідношення безготівкових карткових операцій до загальної кількості трансакцій відображають трансформацію банківської системи у бік збільшення її діджиталізації, саме переведення операцій у безготівкову форму і є критерієм довіри клієнтів до цифрових послуг банків, їх високу якість та поширеність. Частки переказів з картки на картку, також є показником, що свідчить про становлення діджиталізації банківської системи, оскільки розвинений інтернет-банкінг спрошує цю операцію та робить її максимально зручною для клієнта. Зважаючи на той факт, що саме обсяг депозитних ресурсів для банків є основою їх інвестиційної й операційної діяльності, то фінансові посередники спрямовують значну частину власних зусиль для покращення депозитних продуктів, що в сучасних умовах неможливо без їх активної діджиталізації. Виходячи з цього, визначальним чинником для опису рівня діджиталізації фінансової системи є показник кількість депозитних рахунків на 1000 осіб дорослого населення.

Технологічний розвиток, запропоновано визначати за допомогою таких показників, як середня швидкість завантаження; кількість захищених інтернет-серверів; активні абоненти мобільного широкосмугового зв'язку на 100 жителів; особи з базовими навичками інформаційно-комунікаційних технологій (ІКТ). Отже, зупиняючись на характеристики кожного з них зауважимо, що середня швидкість завантаження, на нашу думку, є базовий

показник технологічного розвитку, його динаміка демонструє рівень інноваційного прогресу та забезпечує подальший стимул розвитку нових фінансових продуктів. Саме швидкість завантаження створила умови для формування необанків. Кількість захищених інтернет-серверів, є показником, який також характеризує рівень технологічного розвитку й прогресу в ньому. Саме рівень кіберзахисту забезпечує впевненість в успіху будь-якого продукту або послуги в інтернет просторі, в іншому випадку фінансовий посередник отримає значні збитки, а клієнти будуть ошукані. Активні абоненти мобільного широкосмугового зв'язку на 100 жителів, це критерій, який демонструє використання преваг технологічного розвитку населенням України. Увесь спектр фінансових цифрових продуктів наразі знаходиться в смартфоні, і саме якісний мобільний широкосмуговий зв'язок створює можливості для зростаючого попиту на фінансові діджитал продукти та послуги. Розглядаючи останній чинник цього напрямку, зазначимо, що яким би не був технологічний розвиток країни, якщо в державі низька цифрова грамотність населення, подальшого інноваційного розвитку не буду. Виходячи з цього, показник особи з базовими навичками ІКТ є вкрай важливим для формування сучасного цифрового суспільства в Україні та подальшого поступального становлення національної цифрової економіки.

Переходячи до аналізу ризику кіберзагроз, відмітимо, що цей напрямок описаний за допомогою таких показників, як шахрайства та кібернетичні загрози, а також суми збитків від незаконних дій з платіжними картками. Перший показник є якісним й характеризує відношення менеджменту вітчизняних фінансових посередників до ризиків, які загрожують національному фінансовому сектору, тобто він явно відображує очікування суб’єктів ринку фінансових послуг до потенційних загроз кібер атак серед усіх наявних ризиків діяльності компанії. Визначення цього показника відбувається на основі опитування топ-менеджерів провідних банків та небанківських фінансових установ України (у 2023 р. в опитуванні взяли участь керівники 22 банків, 10 страхових компаній та 3 інвестиційних

компаній). Показник суми збитків від незаконних дій з платіжними картками є кількісним та описує втрати клієнтів банків від кіберзагроз найбільш поширеному та найпопулярнішому банківському продукту серед населення України.

З метою повноцінного розуміння вхідного масиву даних реалізації науково-методичного підходу до побудови сценаріїв поведінки економічних агентів в умовах цифровізації фінансового сектору національної економіки щодо забезпечення їх стійкості до зовнішніх та внутрішніх загроз, згрупуємо показники у таблицю 2.4 та проведемо їх експрес-аналіз.

Отже, проводячи аналіз показників характеристики діджиталізація фінансового сектору, зауважимо, що усі чотири релевантні чинники протягом 2019-222 рр. мали тенденцію до зростання. Так, найбільший темп приросту прослідковується для кількості депозитних рахунків на 1000 осіб дорослого населення і складав 29,1%. Перевищення 20% значення темпу приросту за чотири роки характерно й для частки переказів з картки на картку (26,9%) та співвідношення безготівкових карткових операцій до загальної кількості трансакцій (23,4%). Частка громадян, що користуються онлайн банкінгом за 2019-2022 рр. зросла тільки на 8,3%, проте на разі в Україні вона становить 62,3%, що є доволі високим значенням зважаючи на частку людей похилого віку серед клієнтів банків.

Найбільше зростання протягом останнього періоду (2022-2021 рр.) відбувалось в межах частки переказів з картки на картку, так цей показник за рік зріс більше ніж на 22,2% (минулі роки середній темп приросту склав 1,9%). Усе вище зазначене, свідчить про те, що фінансовий сектор України активно діджиталізується з акцентом на удосконалення вже існуючих цифрових банківських послуг та продуктів, які можна реалізувати через смартфон.

Таблиця 2.4 – Вхідні статистичні дані характеристики діджиталізації фінансового сектору, технологічного розвитку та ризику кіберзагроз за 2019–2022 рр.

Умовні позначення показників	Назва групи	Показник	Рік			
			2019	2020	2021	2022
DFS1	Діджиталізація фінансового сектору	Частка переказів з картки на картку, %	42,0	42,8	43,6	53,3
DFS2		Частка громадян, що користуються онлайн банкінгом,%	57,5	60,8	60,6	62,3
DFS3		Співвідношення безготівкових карткових операцій до загальної кількості трансакцій, %	54,8	57,5	61,4	67,6
DFS4		Кількість депозитних рахунків на 1000 осіб дорослого населення	3191,5	3360,3	3853,1	4120,0
TR1	Технологічний розвиток	Середня швидкість завантаження, Мбіт/с	7,7	15,1	25,3	47,7
TR2		Кількість захищених інтернет-серверів (на 1 мільйон осіб)	7,9	9,0	9,3	9,7
TR3		Активні абоненти мобільного широкосмугового зв'язку на 100 жителів	77,3	85,3	80,1	82,9
TR4		Особи з базовими навичками ІКТ (%)	23,9	31,9	35,8	37,8
RC1	Ризик кіберзагроз	Шахрайство та кібернетичні загрози, %*	35,0	27,0	35,0	40,0
RC2		Сума збитків від незаконних дій з платіжними картками, млн грн	149,0	190,0	330,0	481,0

Примітка: * – рівень ризику, що існує у фінансовому секторі України через дію шахрайств та кібернетичних загроз (один з двадцяти одного фактору які були проаналізовані)

Джерело: Національний банк України, Cable, Світовий банк

Переходячи до показників характеристики технологічного розвитку зауважимо, що вони зростали ще швидше, ніж показники діджиталізації фінансового сектору. Так, темп приросту середньої швидкості завантаження

протягом 2019-2022 рр. складав 519,5%, а відповідний показник осіб з базовими навичками ІКТ 58,2%. Більше ніж 20% темп приросту протягом досліджуваного періоду був характерний і для кількісті захищених інтернет-серверів (на 1 мільйон осіб), а саме 22,2%. Показник, який мав не тільки найнижчий темп приросту протягом 2019-2022 рр. (7,2%), але й зменшився у 2021 р. на 5,2% порівняно до 2020 р. є активні абоненти мобільного широкосмугового зв'язку на 100 жителів. У той же час, цей показник протягом останніх трьох років дослідження складав не менше 80% від загальної чисельності абонентів мобільного зв’язку, що є доволі високим значенням. Вище наведені тенденції цілком зрозумілі, оскільки технічний прогрес повинен випереджати процеси цифровізації і щорічне значення темпів приросту середньої швидкості завантаження даних на рівні 84,1% тому підтвердження. Збільшення швидкості завантаження неможливе без розвитку технологій як самої передачі, так і відправлення й отримання даних. Тільки за таких умов, діджитал послуги та продукти у фінансовому секторі будуть безперервно розвиватись на базі нових технологій, а не змінювати форму використовуючи вже існуючу основу створення та розповсюдження.

Досліджуючи останню групу показників характеристики ризику кіберзагроз, зазначимо, що як і рівень оцінювання топ-менеджерами України ризиків, що існує у фінансовому секторі через дію шахрайств та кібернетичних загроз, так і безпосередній обсяг збитків від незаконних дій з платіжними картками неодмінно зростав протягом 2019-2022 рр. І якщо перший показник коливався протягом досліджуваного періоду в проміжку 27-40% (середній темп просту 7%), то другий зріс за чотири роки на 222,8% (середній темп приросту 49%). Це свідчить як про розуміння фахівців фінансового сектору про існування кібер ризику, так і про його руйнівну роль для стійкості фінансової системи.

Визначивши особливості розвитку показників характеристики вхідного масиву даних перейдемо до другого етапу досліджуваної методики, який полягає у приведенні обраних релевантних показників до співставного

вигляду. Виходячи з того, що отримана вибірка дослідження побудови сценаріїв поведінки економічних агентів в умовах цифровізації фінансового сектору національної економіки щодо забезпечення їх стійкості до зовнішніх та внутрішніх загроз сформована з показників стимуляторів та дестимуляторів, необхідності набуває застосування двох підходів до нормалізації. Для стимуляторів запропоновано проводити адаптивну природню нормалізацію, а для дестимуляторів адаптивну нормалізацію Севіджа з урахуванням коригування на середнє квадратичне відхилення, що дозволить привести розглянуту множину показників до співставного вигляду. Отже, проведемо дослідження механізму формалізації наведених методів нормалізації, а саме математичні співвідношення (2.8) та (2.9), які дозволяють обчислити нормалізовані значення показників ідентифікації критичних зон в поведінці економічних агентів в умовах цифровізації фінансового сектору економіки України.

Нормалізація показників за допомогою формули Севіджа для дестимуляторів:

$$n_{igj} = \frac{\max\limits_{j} a_{igj} + SD(a_{igj}) - a_{igj}}{\max\limits_{j} a_{igj} - \min\limits_{j} a_{igj} + 2 \cdot SD(a_{igj})} \tag{2.8}$$

де n_{igj} – нормалізоване значення i-го показника g-тої групи в розрізі j-го року;

a_{igj} – фактичне значення i-го показника g-тої групи в розрізі j-го року;

$\max\limits_{j} a_{igj}$ – максимальне значення i-го показника g-тої групи в межах розглянутого часового діапазону;

$SD(a_{igj})$ – середнє квадратичне відхилення;

$\min\limits_{j} a_{igj}$ – мінімальне значення i-го показника g-тої групи в межах розглянутого часового діапазону.

Нормалізація показників за допомогою формули природньої нормалізації для стимуляторів:

$$n_{igj} = \frac{a_{igj} - \min\limits_{j} a_{igj} + SD(a_{igj})}{\max\limits_{j} a_{igj} - \min\limits_{j} a_{igj} + 2 \cdot SD(a_{igj})} \quad (2.9)$$

Обчислені за допомогою застосування формул (2.8) та (2.9) нормалізовані значення показників діджиталізації фінансового сектору, технологічного розвитку та ризику кіберзагроз за період з 2019 р. по 2022 р. згрупуємо в таблицю 2.5.

Таблиця 2.5 – Нормалізовані значення показників діджиталізації фінансового сектору, технологічного розвитку та ризику кіберзагроз за 2019-2022 рр.

Умовні позначення показників	Рік			
	2019	2020	2021	2022
DFS1	0,2418	0,2783	0,3149	0,7582
DFS2	0,2282	0,5997	0,5816	0,7718
DFS3	0,2321	0,3468	0,5064	0,7679
DFS4	0,2404	0,3348	0,6104	0,7596
TR1	0,2326	0,3312	0,4670	0,7674
TR2	0,2653	0,2654	0,7148	0,7347
TR3	0,2319	0,7681	0,4210	0,6074
TR4	0,2346	0,5401	0,6890	0,7654
RC1	0,4369	0,7736	0,4369	0,2264
RC2	0,7623	0,6975	0,4763	0,2377

Джерело: розрахунки автора

Виходячи з того факту, що розглянуті показники в межах кожної групи мають різну силу впливу на потенційний результату, то на третьому етапі реалізації запропонованої методики, актуальності набуває ідентифікація їх пріоритетність. Справедливо зазначити, що доцільність реалізації даного етапу обумовлена врахуванням різного рівня значимості кожного релевантного фактору для отримання кінцевого результату. Визначення пріоритетності розглянутих показників діджиталізації фінансового сектору, технологічного розвитку та ризику кіберзагроз запропоновано здійснити за

допомогою методу головних компонент, а саме побудови графіку кам'янистого осипу та врахуванні власних значень кореляційної матриці.

Отже, формалізацію пріоритетності показників в розрізі кожної із груп дослідження доцільно проводити за допомогою ідентифікації вагових коефіцієнтів w_{ig} (для i-го показника в межах g-тої групи) змінних n_{igj} – показників діджиталізації фінансового сектору, технологічного розвитку та ризику кіберзагроз, яка має дорівнювати одиничному значенню (2.10):

$$F\left(w(n_{1gj}), \dots, w(n_{ngj})\right) = F\left(w_{1g}, \dots, w_{ng}\right) = \sum_{i=1}^{n} w_{ig} \to 1 \qquad (2.10)$$

де $F\left(w(n_{1gj}), \dots, w(n_{ngj})\right) = F\left(w_{1g}, \dots, w_{ng}\right)$ – функціональна залежність між ваговими коефіцієнтами w_{ig} змінних n_{igj};

n_{igj} – нормалізоване значення i-го показника g-тої групи в розрізі j-го року;

w_{ig} – ваговий коефіцієнт i-го показника в межах g-тої групи.

Для встановлення пріоритетності груп показників діджиталізації фінансового сектору, технологічного розвитку та ризику кіберзагроз скористаємось можливостями програмного пакету Statistica, зокрема методом головних компонент (команда Statistica/Multivariate Explanatory Techniques/Principal Components and Classification Analysis). Результати представимо на рисунках 2.27 – 2.32.

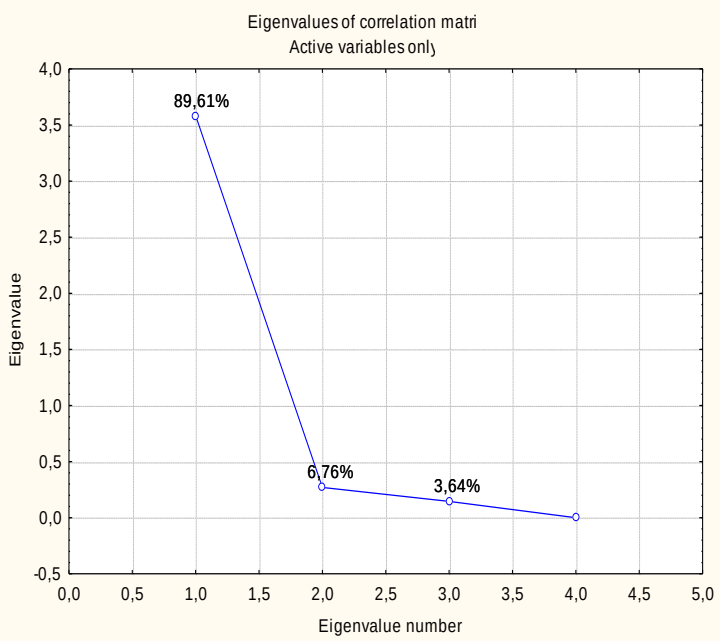


Рисунок 2.27 – Фрагмент програми Statistica графіку кам'янистого опису в розрізі першої групи показників діджиталізації фінансового сектору

Джерело: розрахунки автора

	Eigenvalues of correlation matrix, and related Active variables only			
Value numbe	Eigenvalue	% Total variance	Cumulative Eigenvalue	Cumulativ %
1	3,58424	89,6060	3,58424	89,60
2	0,27033	6,7583	3,85457	96,36
3	0,14542	3,6356	4,00000	100,00

Рисунок 2.28 – Фрагмент програми Statistica таблиці власних значень кореляційної матриці та пов'язаних статистичних показників в розрізі першої групи діджиталізації фінансового сектору

Джерело: розрахунки автора

На основі аналізу рисунків 2.27 та 2.28 для першої групи показників діджиталізації фінансового сектору можна зробити висновок про доцільність оцінювання пріоритетності зазначених показників враховувати лише першу головну компоненту, представлену першим фактором, оскільки на його варіацію припадає 89,61% загальної варіації, про це свідчить як графік кам'янистого осипу (рисунок 2.27), так і табличні значення власних значень факторів в розрізі показників (рисунок 2.28).

Безпосередньо, рівень впливу кожного з показників групи діджиталізації фінансового сектору формалізуємо за допомогою рисунку 2.29.

	Variable contributions, based on correlations (Sprea		
Variable	Factor 1	Factor 2	Factor 3
DFS1	0,23767	0,40314	0,26904
DFS2	0,22787	0,58237	0,17741
DFS3	0,27685	0,01422	0,02636
DFS4	0,25759	0,00024	0,52718

Рисунок 2.29 – Фрагмент програми Statistica таблиці вкладу змінних на основі кореляції в розрізі першої групи діджиталізації фінансового сектору

Джерело: розрахунки автора

Таким чином, на основі рисунку 2.29 можна стверджувати, що найбільш впливовим виступає показник *DFS3* – співвідношення безготівкових карткових операцій до загальної кількості трансакцій. Другим за пріоритетністю є показник *DFS4* – кількість депозитних рахунків на 1000 осіб дорослого населення. У свою чергу, майже однаковий рівень важливості мають *DFS1* – частка переказів з картки на картку та *DFS2* – частка громадян, що користуються онлайн банкінгом.

Переходячи до аналізу пріоритетності показників технологічного розвитку, зауважимо, що на основі результатів розрахунків зображених на рисунках 2.30 та 2.31 можна стверджувати, що з метою оцінювання пріоритетності показників досліджуваної групи доцільно враховувати перші дві головні компоненти, представлену першим і другим факторами. Це обумовлено тим, що на їх варіацію припадає 71,89% загальної варіації.

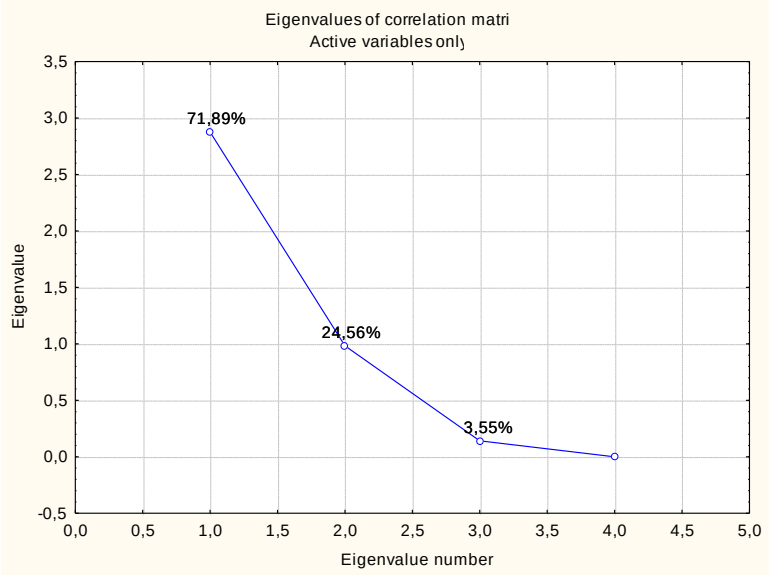


Рисунок 2.30 – Фрагмент програми Statistica графіку кам’янистого опису в розрізі другої групи показників технологічного розвитку

Джерело: розрахунки автора

	Eigenvalues of correlation matrix, and related Active variables only			
Value numbe	Eigenvalue	% Total variance	Cumulative Eigenvalue	Cumulative %
1	2,87557	71,8894	2,87557	71,88
2	0,98254	24,5637	3,85812	96,45
3	0,14187	3,5467	4,00000	100,00

Рисунок 2.31 – Фрагмент програми Statistica таблиці власних значень кореляційної матриці та пов’язаних статистичних показників в розрізі другої групи технологічного розвитку

Джерело: розрахунки автора

Зупиняючись на визначенні рівня впливу кожного з показників групи технологічного розвитку (рисунку 2.32) зауважимо, що найсуттєвіший вплив здійснюють показники TR4 – особи з базовими навичками ІКТ та TR1 – середня швидкість завантаження. Відносно менший вплив, проте теж суттєвий здійснює показник TR2 – кількість захищених інтернет-серверів, найменшу пріоритетність має показник TR3 – активні абоненти мобільного широкосмугового зв'язку на 100 жителів.

Variable	Variable contributions, based on correlations (Sprea		
	Factor 1	Factor 2	Factor 3
TR1	0,30949	0,01655	0,66080
TR2	0,26780	0,21743	0,11475
TR3	0,08892	0,75749	0,00012
TR4	0,33377	0,00852	0,22431

Рисунок 2.32 – Фрагмент програми Statistica таблиці вкладу змінних на основі кореляції в розрізі другої групи технологічного розвитку

Джерело: розрахунки автора

Виходячи з того, що у випадку з групою технологічного розвитку визначені дві головні компоненти для ідентифікації пріоритетності, то актуальності набуває проведення наступних перетворень. Враховуючи дані наведені на рисунку 2.31 та 2.32 визначимо вагові коефіцієнти показників w_{ig} на основі середньої арифметичної зваженої:

$$w_{ig} = \frac{\sum_{j=1}^{2} F_{ij} \cdot v_j}{\sum_{j=1}^{2} v_j} \tag{2.11}$$

де w_{ig} – ваговий коефіцієнт i-го показника в межах g-тої групи;

F_{ij} – значення вкладу i-тої змінної в розрізі j-того фактору (головної компоненти) на основі кореляції;

v_j – відсоток загальної варіації власних значень кореляційної матриці в розрізі j-того фактору (головної компоненти). Результати обчислень за формулою (2.11) представимо в таблиці 2.6.

Таблиця 2.6 – Вклад змінних на основі кореляції, обмеження пріоритетності та ваги показників другої групи технологічного розвитку

Факторні навантаження	71,88948	24,56374	Вагові коефіцієнти
Змінні/Фактори	Фактор 1	Фактор 2	
RT1	0,309498	0,016552	0,235
RT2	0,267801	0,217430	0,255
RT3	0,088924	0,757493	0,259
RT4	0,333776	0,008525	0,251

Джерело: розрахунки автора

Отже, пріоритетність показників: RT1, RT2, RT3 та RT4, відповідно дорівнює 0,235 од., 0,255 од., 0,259 од., 0,251 од.

Розглядаючи останню групу показників характеристики ризику кіберзагрози, зазначимо, що на основі рисунків 2.33 (графік кам'янистого осипу) та 2.34 (табличні значення власних значень факторів в розрізі показників) можна зробити висновок про доцільність оцінювання пріоритетності показників враховувати лише першу головну компоненту, представлену першим фактором (варіація дорівнює 85,99% загальної варіації).

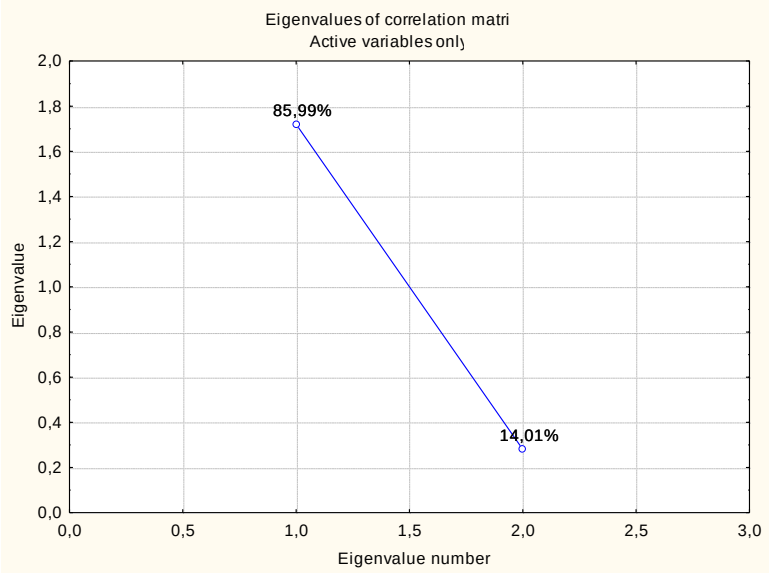


Рисунок 2.33 – Фрагмент програми Statistica графіку кам'янистого опису в розрізі третьої групи ризику кіберзагроз

Джерело: розрахунки автора

	Eigenvalues of correlation matrix, and related Active variables only			
Value numbe	Eigenvalue	% Total variance	Cumulative Eigenvalue	Cumulative %
1	1,71982	85,9914	1,71982	85,99
2	0,28017	14,0085	2,00000	100,00

Рисунок 2.34 – Фрагмент програми Statistica таблиці власних значень кореляційної матриці та пов'язаних статистичних показників в розрізі третьої групи ризику кіберзагроз

Джерело: розрахунки автора

На основі рисунку 2.35, у свою чергу, можна зазначити, що обидва розглянуті показники, а саме й шахрайство та кібернетичні загрози, а також сума збитків від незаконних дій з платіжними картками мають однакову пріоритетність – 0,5 частки одиниці.

	Variable contributions, based on correlations (Sprea	
Variable	Factor 1	Factor 2
RC1	0,50000	0,50000
RC2	0,50000	0,50000

Рисунок 2.35 – Фрагмент програми Statistica таблиці вкладу змінних на основі кореляції в розрізі третьої групи ризику кіберзагроз

Джерело: розрахунки автора

Таким чином, узагальнити отримані розрахунки рівня пріоритетності показників характеристики діджиталізація фінансового сектору, технологічного розвитку та кіберзагроз можна за допомогою таблиці 2.7.

Таблиця 2.7 – Рівень пріоритетності показників характеристики діджиталізація фінансового сектору, технологічного розвитку та кіберзагроз

Умовні позначення показників	DFS1	DFS2	DFS3	DFS4	TR1	TR2	TR3	TR4	RC1	RC2
Питома вага	0,238	0,228	0,277	0,258	0,235	0,255	0,259	0,251	0,500	0,500

Джерело: розрахунки автора

Проведені на третьому етапі реалізації науково-методичного підходу до побудови раціональних сценаріїв поведінки економічних агентів в умовах цифровізації фінансового сектору національної економіки розрахунки дозволяють знайти інтегральний показник в розрізі кожної групи окремо за допомогою трансформованої згортки Кіні (четвертий етап). Математична формалізація цього етапу має наступний вигляд:

$$K_{jg} = \frac{1}{G} \cdot \prod_{i} (1 + G \cdot w_{ig} \cdot n_{igj}) \quad (2.12)$$

де K_{jg} – інтегральний показник Кіні в розрізі j-го року в межах g-тої групи показників.

G – загальна кількість показників і розрізі g-тої групи;

n_{igj} – нормалізоване значення i-го показника g-тої групи в розрізі j-го року;

w_{ig} – ваговий коефіцієнт і-го показника в межах g-тої групи.

Провівши відповідні розрахунки на основі рівняння 2.12 практичні результати згрупуємо в таблицю 2.8.

Таблиця 2.8 – Динаміка інтегральних показників діджиталізації фінансового сектору, технологічного розвитку та ризику кіберзагроз за 2019-2022 рр.

Інтегральні показники груп	Рік			
	2019	2020	2021	2022
Діджиталізація фінансового сектору (DFS)	0,583	0,910	1,264	2,417
Технологічний розвиток (TR)	0,593	1,154	1,511	2,169
Ризик кіберзагроз (RC)	1,266	1,505	1,061	0,759

Джерело: розрахунки автора

Отже, на основі отриманих розрахунків справедливо зазначити, що протягом 2019-2022 рр. інтегральні показники досліджуваних напрямків змінювались нерівномірно. Так, інтегральний показник діджиталізації фінансового сектору та технологічного розвитку неодмінно зростали з середнім темпом приросту 62,1% та 56,4 %, відповідно. У свою чергу, для діджиталізації фінансового сектору піковий темп приросту прослідковується у 2022 р. порівняно до 2021 р. – 91,2%, а для технологічного розвитку у 2020 р. порівняно до 2019 р. – 94,6%. Зупиняючись, на ризику кіберзагроз

перш за все, зауважимо, що абсолютні значення інтегрального показника необхідно трактувати навпаки, чим воно менше тим ризик більший. Це пов'язано з тим, що в процесі нормалізації релевантні чинники, що його формували (шахрайство та кібернетичні загрози, сума збитків від незаконних дій з платіжними картками), розглядались за своєю суттю, тобто як дестимулятори. У свою чергу, ризику кіберзагроз, це також показник збільшення якого призводить до негативного ефекту. Отже, на основі даних наведених в таблиці 3.5 зауважимо, що починаючи з 2020 р. абсолютне значення інтегрального показника ризику кіберзагроз зменшувався щороку в середньому на 29%. Тобто, можна стверджувати, що інтенсифікація процесу розширення цифрових технологій в національній економіці спричиняє й збільшення кіберзагроз, тому як суб'єкти господарювання, так і державні органи контролю повинні розширювати засоби моніторингу та ліквідації кіберзагроз. Безумовно, компанії повинні постійна удосконалювати власну системи кбіербезпеки, проте конкретний набір інструментів, заважаючи на обмежений обсяг фінансових ресурсів, можна ідентифікувати розрахувавши рівень загрози у конкретний момент часу в залежності від вхідних параметрів.

На наступному (п'ятому) етапі реалізації запропонованого науково-методичного підходу, актуальності набуває визначення якісної характеристики інтегральних показників діджиталізація фінансового сектору, технологічного розвитку та ризику кіберзагроз. Для вирішення поставленої задачі, запропоновано використати підхід на основі стандартного відхилення (формули 2.13):

$$\begin{cases} [min - SD; \frac{2min-3SD+max}{3}) - \text{низький рівень для DFS й TR, високий рівень для RC;} \\ \left[\frac{2min-3SD+max}{3}; \frac{min-3SD+2max}{3}\right] - \text{середній рівень для DFS, TR та RC;} \\ (\frac{min-3SD+2max}{3}; max + SD] - \text{високий рівень для DFS й TR, низький рівень для RC;} \end{cases} \quad (2.13)$$

де *min* – мінімальне значення показника;

SD – стандартне відхилення;

max – максимальне значення показника.

Використовуючи наведений вище механізм встановимо три проміжки низького, середнього та високого рівня для інтегральних показників діджиталізація фінансового сектору, технологічного розвитку та ризику кіберзагроз. Результати проведених розрахунків згрупуємо в таблицю 2.9.

Таблиця 2.9 – Якісні характеристики інтегральних показників діджиталізація фінансового сектору, технологічного розвитку та ризику кіберзагроз

Показники	низький рівень (червона зона)		середній рівень (жовта зона)		високий рівень (зелена зона)	
	min	max	min	max	min	max
Діджиталізація фінансового сектору (DFS)	-0,217	0,395	0,395	1,007	1,007	3,217
Технологічний розвиток (TR)	-0,092	0,454	0,454	0,999	0,999	2,882
Ризик кіберзагроз (RC)	0,940	1,822	0,691	0,940	0,442	0,691

Джерело: розрахунки автора

Реалізація п’ятого етапу, дозволяє надати отриманим абсолютним значенням інтегральних показників якісну характеристику та визначити чи знаходиться показник в прийнятному стані, чи їх значення критичні для успішного розвитку процесу цифровізації національної економіки.

На завершальному шостому етапі реалізації науково-методичного підходу до побудови сценаріїв поведінки економічних агентів в умовах цифровізації фінансового сектору національної економіки щодо забезпечення їх стійкості до зовнішніх та внутрішніх загроз проведемо графічну інтерпретацію отриманих результатів (рисунок 2.36).

Отримане графічне зображення дає можливість визначити не тільки динаміку ситуації всередині трикутнику «діджиталізація фінансового

сектору–технологічний розвиток–кіберзагрози», але й з'ясувати, які практичні дії та інструменти необхідно застосовувати державним органам виконавчої влади та суб'єктам господарювання в конкретний момент часу. Так, за умови знаходження усіх трьох інтегральних показників у зеленій зоні (таблиця 2.9), справедливо стверджувати про стабільну ситуацію у фінансовому секторі економіки та рівномірний розвиток діджиталізації й технологій. У свою чергу, рівень кібер загроз, за такої ситуації, знаходиться на прийнятному рівні та не заважає безпечній роботі фінансових посередників. За умови потрапляння інтегрального показника технологічного розвитку у червону зону, а двох інших інтегральних показників у жовту та зелену зону, справедливо стверджувати про те, що з часом цифровий розвиток економіки завершиться і буде поступова стагнація. У випадку потрапляння інтегрального показника діджиталізації фінансового сектору у червону зону, а інтегрального показника технологічного розвитку та ризику кіберзагроз у зелену та жовту зони, доцільно говорити про неспроможність економічних агентів використовувати переваги існуючих технологій. У свою чергу, якщо інтегральний показник ризику кіберзагроз потрапляє у червону зону при високому рівні двох інших індикаторів, то можна стверджувати про сигнал до активного застосування як превентивних, так і радикальних заходів по ідентифікації та локалізації кібер ризиків. Якщо тільки один інтегральний показник потрапляє у зелену та жовту зони, а два інших у червоній, то в першу чергу, треба мінімізувати кібер ризики, а по-друге, шукати або інструменти реалізації наявного технологічного потенціалу (якщо інтегральний показник теологічного розвитку знаходиться у червоній зоні), або проводити активну політики по залученню інвестицій у фінтех (якщо інтегральний показник діджиталізації фінансового сектору знаходиться у червоній зоні).

Переходячи до аналізу реально отриманих результатів графічної інтерпретації таргетних індикаторів в системі: діджиталізація фінансового сектору–технологічний розвиток–кіберзагрози в Україні протягом 2019-2022 рр., зауважимо, що жоден з інтегральних показників не потрапив у критичну

червону зону. Найбільш сприятливим для цифрового розвитку фінансового сектору національної економіки був 2021 р. коли в трикутнику «діджиталізація фінансового сектору – технологічний розвиток – кіберзагрози» прослідковувалась повна рівновага й збалансованість. 2019 рік був найбільш неприйнятним в розрізі забезпечення діджиталізації фінансового сектора за допомогою впровадження технологій. Так, інтегральні індекси DFS та TR знаходились у жовтій зоні. У 2020 році ситуація покращилась і в жовтій зоні залишився тільки інтегральний показник діджиталізації. Зазначена динаміка протягом 2019-2021 рр. свідчить про ефективну та системну роботу економічних агентів в сфері цифровізації бізнес-процесів у фінансовому секторі України, а також не тільки зростанню фінтеху в Україні, але й чіткому розумінню необхідності дотримання фінансової безпеки. У 2022 р. ситуація з кібер загрозами значно погіршилась, приводом чого став початок повномасштабного вторгнення росії до України. Потенційним кібератакам були схильні усі сфери життєдіяльності країни, а особливо її фінансовий сектору.

У той же час, справедливо зауважити, що навіть не зважаючи на війну в Україні, фінансовий сектор залишається прогресивним вектором розвитку національної економіки та продовжує надавати якісні послуги українцям. Враховуючи зростання кібер ризиків, фінансовій системі вдалось їх досить успішно локалізувати та тримати високий рівень безпеки обслуговування власних клієнтів. Паралельно з цим, держава повинна продовжувати політику безперервного забезпечення цифрової безпеки як фінансової системи країни, так і громадян України. Системний характер повинні носити реформи пов’язані з удосконалення нормативного забезпечення регулювання ІТ та фінтех секторів національної економіки.

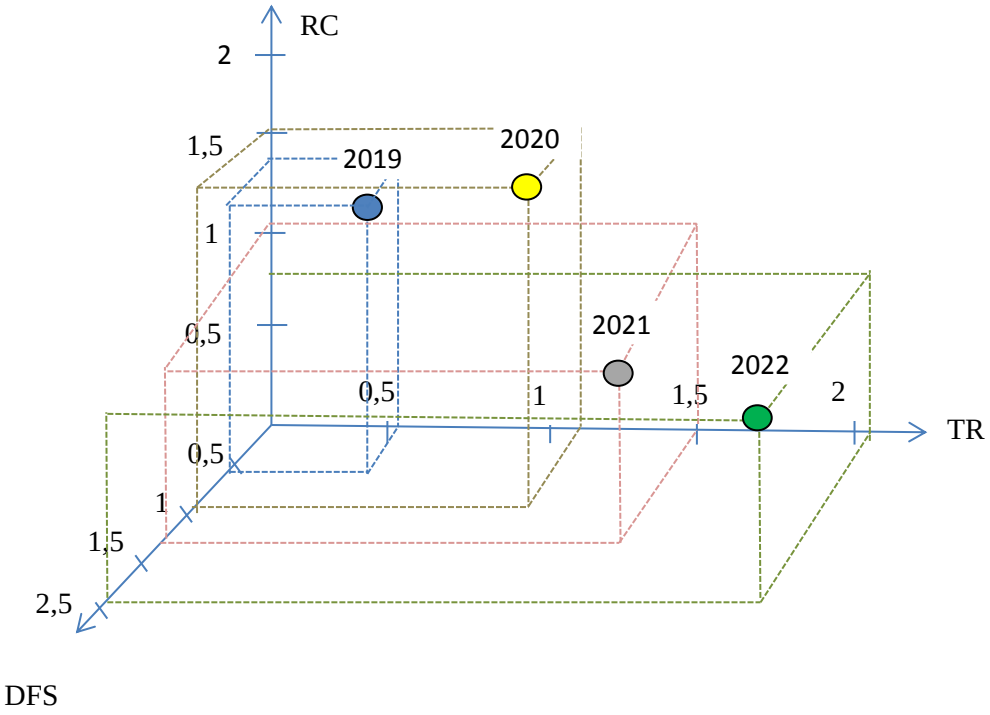


Рисунок 2.36 – Графічна інтерпретація таргетних індикаторів в системі: діджиталізація фінансового сектору–технологічний розвиток–кіберзагроз в Україні протягом 2019-2022 рр.

Джерело: розрахунки автора

3 ОСОБЛИВОСТІ ВІКТИМНОЇ ПОВЕДІНКИ СПОЖИВАЧІВ ФІНАНСОВИХ ПОСЛУГ У КІБЕРПРОСТОРІ

3.1 Науково-методичний підхід до оцінювання рівня кібервразливості економічних агентів

Розширення цифрових можливостей та покращення роботи з клієнтами є неминучим вибором для банків та фінансових установ, які прагнуть залишатися конкурентоспроможними та задовольняти потреби клієнтів протягом наступного десятиліття. У той же час це призводить до збільшення кількості атак кіберзлочинців. Insights, компанія з розвідки кіберзагроз, повідомила, що 25% усіх атак зловмисного програмного забезпечення спрямовані на банки та інші компанії, що надають фінансові послуги, що набагато більше, ніж у будь-якій іншій галузі.

Безпечне та ефективне функціонування інфраструктури фінансового ринку має важливе значення для підтримки та сприяння фінансовій стабільності, підвищення довіри населення до фінансових установ. На сьогодні питання забезпечення інформаційної безпеки суб’єктів фінансового ринку поступово стає пріоритетним вектором діяльності як національного регулятора, так і надавачів фінансових послуг. У березні 2017 року Рада керуючих Європейського центрального банку затвердила «Стратегію кіберстійкості Євросистеми для фінансових установ», метою якої є покращення інформаційної безпеки фінансових установ у Європейському Союзі та посилення співпраці між національними регуляторами, фінансовими установами та контрагентами для протидії кіберзагрозам.

Національний банк України також посилює контроль за виконанням фінансовими установами заходів із забезпечення кіберзахисту та інформаційної безпеки. З прийняттям постанови Правління Національного банку України від 16 січня 2021 року № 4 [92] фінансові установи зобов’язані щорічно проводити самооцінку з оцінювання ризиків власної інформаційної

безпеки та подавати дану інформацію до національного регулятора. Дані регуляторні заходи сприятимуть приведенню вітчизняного законодавства у сфері кіберзахисту фінансової системи до міжнародних стандартів та принципів, а саме Банку міжнародних розрахунків "Керівництво з кіберстійкості для інфраструктур фінансового ринку" [94] та Європейського центрального банку "Очікування з оверсайта щодо кіберстійкості інфраструктур фінансового ринку" [95]. Крім цього, починаючи з серпня 2021 року Національний банк України та кіберполіція співпрацюватимуть для посилення ефективності протидії кіберзлочинам у фінансовій сфері.

В умовах швидко зростаючих кіберзагроз та урізноманітнення форм їх здійснення важливою умовою ефективної боротьби з ними є розвиток комунікації, координації та партнерства у сфері кіберзахисту між фінансовими установами та національним регулятором, що передбачає обмін актуальною інформацією про кіберзагрози між банками.

У сучасних умовах фінансові установи деяких країн світу укладають попередню угоду зі своїми клієнтами, де чітко зазначається необхідний спосіб ідентифікації та аутентифікації клієнта при підтвердженні фінансової транзакції [96].

Ураховуючи масовий перехід користувачів платіжних послуг в онлайн у період карантину, важливим пріоритетом для центрального банку є необхідність максимально убезпечити їх від можливих інцидентів інформаційної безпеки. Однією з найбільш вразливих ланок в забезпеченні інформаційної безпеки фінансової системи є споживачі фінансових послуг, що й обумовило актуальність обраного напрямку дослідження.

Метою запропонованого науково-методичного підходу є оцінювання інтегрального рівня кібервразливості споживачів фінансових послуг, що передбачає реалізацію наступних етапів:

– збір та обробка статистичних даних, що прямо та опосередковано характеризують ступінь обізнаності клієнтів фінансових установ щодо

ймовірних кібершахрайств та способів захисту від кіберзагроз при здійсненні фінансових транзакцій;

– визначення пріоритетності змінних, обраних на попередньому етапі;

– обрання синтезуючої функції для визначення узагальнюючого рівня кібервразливості споживачів фінансових послуг.

Початковим етапом розробленого науково-методичного підходу є збір та систематизація індикаторів, що прямо та опосередковано характеризують вразливості споживачів фінансових послуг до кіберзагроз (проінформованість про ознаки підозрілих кібершахрайств, способи кіберзахисту, канали інформування про кібератаки). Джерелом первинних даних слугувало опитування громадян Європейського Союзу щодо їх ставлення до питань кібербезпеки, яке проводилося у 2020 році [97]. Для потреб даного дослідження відібрано 17 індикаторів, які виключно стосуються фінансових транзакцій та захисту персональних даних, а саме: частка населення, які хвилюються безпекою онлайн-платежів (R1); частка населення, які мають хвилювання щодо несанкціонованого використання їх персональних даних (R2); частка населення, які змінювали протягом останніх 12 місяців пароль до інтернет-банкінгу (R3); частка населення, які зазначають низький рівень інформованості про ризики кіберзлочинності (R16); частка населення, яким відомо хоча б один спосіб повідомлення про кіберзлочин (R17), а також група показників, що відображають превентивні заходи громадян для підвищення їх рівня захисту віртуальному просторі (R4- R15): частка населення, яка зменшила кількість банківських операцій в Інтернеті (R4); частка населення, яка рідше вводить особисту інформацію на веб-сайтах (R5); частка населення, яка змінила налаштування безпеки (наприклад, у браузері, соціальній мережі, пошуковій системі) (R6); частка населення, яка відвідуєте лише ті веб-сайти, які знаєте і яким довіряє (R7); частка населення, яка використовує різні паролі для різних сайтів (R8); частка населення, яка не відкриваєте електронні листи від незнайовим людей (R9); частка населення, яка встановила актуальне

антивірусне програмне забезпечення (R10); частка населення, яка скасувала онлайн-покупку через підозри щодо продавця або веб-сайту (R11); частка населення, яка використовує більш складні паролі, ніж раніше (R12); частка населення, яка використовує біометричні функції (наприклад, розпізнавання обличчя, відбиток пальця) (R13); частка населення, яка не підключається до Інтернету через незахищені точки доступу (R14); частка населення, яки не турбує безпека в Інтернеті (R15). Об'єктом дослідження обрано 30 країн Європи. Узагальнена інформація у розрізі 17 індикаторів станом на 2020 рік представлена в додатку Г, а основні результати подано в таблиці 3.1.

Таблиця 3.1 – Інформація щодо обізнаності громадян про кібератаки та способи захисту від них в європейських країнах у 2020 році

	Сер. знач. по ЄС	Топ-3 країн з найвищими показниками			Топ-3 країн з найнижчими показниками		
		1	2	3	1	2	3
R1	41%	Ірландія (52%)	Іспанія (49%)	Великобри-танія (46%)	Польща (24%)	Естонія (25%)	Данія (27%)
R2	46%	Кіпр (60%)	Греція (57%)	Німеччина (57%)	Угорщина (31%)	Словаччина (31%)	Польща (32%)
R3	30%	Латвія (49%)	Великобри-танія (42%)	Австрія (41%)	Румунія (10%)	Угорщина (13%)	Португалія (15%)
R16	22%	Мальта (44%)	Греція (40%)	Австрія (34%)	Румунія (14%)	Іспанія (14%)	Данія (14%)
R17	17%	Швеція (30%)	Австрія (29%)	Нідерланди (25%)	Португалія (5%)	Латвія (7%	Греція (8%)

Джерело: розрахунки автора

За даними опитування громадян Європейського Союзу щодо рівня їх обізнаності та усвідомлення важливості захисту фінансових операцій у віртуальному просторі встановлено наступні факти: близько половини населення Ірландії, Іспанії та Великобританії мають занепокоєння щодо безпечності їх онлайн платежів; у Кіпрі 60% населення мають хвилювання щодо несанкціонованого використання їх персональних даних при здійсненні розрахунків.

У країнах Європейського Союзу у середньому 22% населення зазначають низький рівень їх інформованості про ризики кіберзлочинності, тоді як найбільші значення у таких країнах як Мальта (44%), Греція (40%), Австрія (34%), а найнижчі – Румунія, Іспанія, Данії (14%).

Важливим елементом в протидії кіберзлочинності є вчасне повідомлення про факти порушення у відповідні контролюючі органи. Проте лище 17% європейців знають про хоча б один спосіб повідомлення про кіберзлочин, найвищі показники у Швеції (30%), Австрії (29%), Нідерландах (25%), а найнижчі – Португалія (5%), Латвія (7%), Греці (8%).

Наступним етапом запропонованого методичного підходу є визначення пріоритетності показників кібервразливості споживачів фінансових послуг на основі комбінації методу головних компонент (при визначенні граничних меж значень показників) та лінійного програмування методом узагальненого знижуючого градієнту. Реалізація даного етапу є комплексною, тому виникає необхідність проведення ряду проміжних кроків. Так, для постановки та вирішення задачі лінійного програмування оптимізації вагових коефіцієнтів показників кібервразливості споживачів фінансових послуг при подальшому обчисленні єдиного інтегрального індексу кіберврзарливості, проводяться наступні проміжні кроки обчислень:

Крок 2.1. Формалізація цільової функції як суми вагових коефіцієнтів змінних змінних $R_1, \dots, R_{17}$ – показників кібервразливості, яка має дорівнювати одиничному значенню (формула 3.1):

$$F(w(R_1), \dots, w(R_{17})) = \sum_{i=1}^{17} w(R_i) \to 1 \tag{3.1}$$

де $F(w(R_1), \dots, w(R_{17}))$ – функціональна залежність між ваговими коефіцієнтами $w(R_i)$ змінних $R_1, \dots, R_{17}$ – показників кібервразливості.

Крок 2.2. Формалізація обмежень задачі оптимізації вагових коефіцієнтів показників кібервразливості споживачів фінансових послуг:

- сума вагових коефіцієнтів показників наступного переліку (від 4-го до 15-го включно) не повинна перевищувати рівня 0,5 частки одиниці (формула 3.2):

$$\sum_{i=4}^{15} w(R_i) \leq 0.5 \tag{3.2}$$

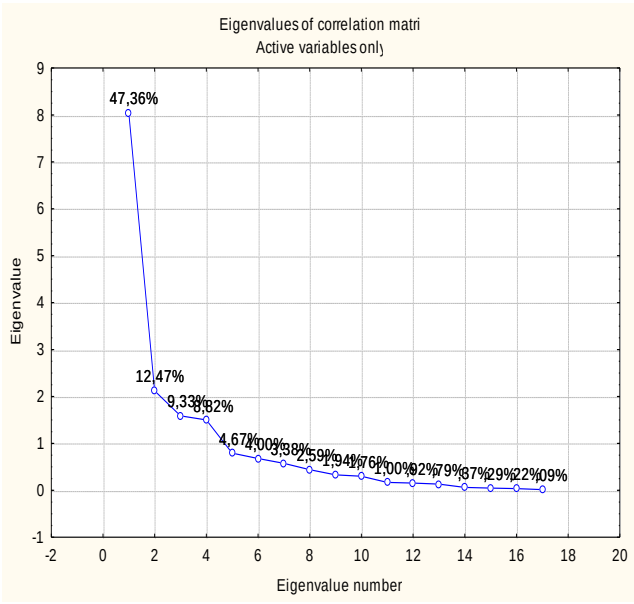
Дана умова введена в економетричну модель, оскільки вищезазначені індикатори (R4- R15) відображають ступінь використання превентивних заходів громадянами для підвищення їх рівня захисту віртуальному просторі.

- значення показників кібервразливості не повинні перевищувати і не повинні бути менше гранично допустимих рівнів (формула 3.3):

$$\begin{gathered} w(R_{i,i=4\div15}) \leq RO_i \\ w(R_{i,i=1,2,16,17}) \geq RO_i \end{gathered} \tag{3.3}$$

де RO_i – гранично допустимі межі кількісних значень для і-го показника характеристики кібервразливості.

Для встановлення гранично допустимих рівнів показників кібервразливості скористаємось методом головних компонент можливостями програмного пакету Statistica. За своєю сутністю метод полягає у виборі нової ортогональної системи координат у просторі спостережень. Як першу головну компоненту обирають напрям, вздовж якого масив спостережень має найбільшу дисперсію. Кожну наступну компоненту обирають також з умови максимізації частки дисперсії, що залишилася, вздовж неї, доповненої умовою ортогональності всім раніше обраним компонентам. При цьому із зростанням номера компоненти буде зменшуватися пов’язана з нею частка загальної дисперсії. Результати представимо на рисунку 3.1.



Value numbe	Eigenvalues of correlation matrix, and related stati Active variables only			
	Eigenvalue	% Total variance	Cumulative Eigenvalue	Cumulative %
1	8,05082	47,3577	8,0508	47,357
2	2,11958	12,4681	10,1704	59,825
3	1,58674	9,3338	11,7571	69,159
4	1,50018	8,8246	13,2573	77,984
5	0,79367	4,6686	14,0510	82,653
6	0,67927	3,9957	14,7302	86,648
7	0,57515	3,3832	15,3054	90,032
8	0,44067	2,5921	15,7461	92,624
9	0,33022	1,9424	16,0763	94,566
10	0,30000	1,7647	16,3763	96,331
11	0,16915	0,9950	16,5455	97,326
12	0,15577	0,9163	16,7012	98,242
13	0,13375	0,7867	16,8350	99,029
14	0,06303	0,3707	16,8980	99,400
15	0,04867	0,2862	16,9467	99,686
16	0,03756	0,2209	16,9842	99,907
17	0,01570	0,0924	17,0000	100,000

Рисунок 3.1 – Скріншот фрагмента програми Statistica графіку кам’янистого опису, власних значень кореляційної матриці та пов’язаних статистичних показників

Джерело: розрахунки автора

На основі аналізу рисунку 3.1 можна зробити висновок про доцільність для оцінювання граничних обмежень показників кібервразливості враховувати перші чотири головні компоненти, представлені першими чотирма факторами, на варіацію яких припадає 77,98% загальної варіації, про що свідчить як графік кам’янистого осипу (лівий фрагмент рисунку 2.8), так і табличні значення власних значень факторів в розрізі показників (правий фрагмент рисунку 3.1). Враховуючи дані рисунку 3.1 та вкладу змінних на основі кореляції показників кібервразливості споживачів фінансових послуг, визначимо обмеження для визначення пріоритетності RO_i на сонові середньої арифметичної зваженої (формула 3.4):

$$RO_i = \frac{\sum_{j=1}^{4} F_{ij} \cdot v_j}{\sum_{j=1}^{4} v_j} \quad (3.4)$$

де RO_i – обмеження, що накладається на і-ту змінну - показник кібервразливості;

F_{ij} – значення вкладу і-тої змінної в розрізі j-того фактору (головної компоненти) на основі кореляції;

v_j - % загальної варіації власних значень кореляційної матриці в розрізі j-того фактору (головної компоненти).

Результати обчислень за формулою 3.4 представимо у графі 5 таблиці 3.2.

Таблиця 3.2 – Вклад змінних на основі кореляції, обмеження пріоритетності та ваги показників кібервразливості споживачів фінансових послуг

Показник	Factor1 47,36	Factor2 12,47	Factor3 9,33	Factor4 8,82	Обмеження для визначення пріоритетності RO_i	Ваги $w(R_i)$
A	1	2	3	4	5	6
R1	0,0011	0,1829	0,2279	0,0164	0,0590	0,104
R2	0,0030	0,3253	0,0225	0,0812	0,0657	0,111
R3	0,0404	0,0043	0,0582	0,0004	0,0323	0,077
R4	0,0267	0,1753	0,0108	0,0237	0,0483	0,011
R5	0,0772	0,0331	0,0036	0,0446	0,0576	0,021
R6	0,0949	0,0032	0,0189	0,0028	0,0607	0,029
R7	0,0259	0,1418	0,1851	0,0170	0,0625	0,038
R8	0,1127	0,0007	0,0019	0,0059	0,0694	0,045
R9	0,0941	0,0100	0,0619	0,0072	0,0669	0,045
R10	0,0784	0,0040	0,0147	0,0002	0,0500	0,045
R11	0,0468	0,0239	0,1518	0,0246	0,0532	0,049
R12	0,1023	0,0008	0,0103	0,0097	0,0646	0,053
R13	0,1007	0,0264	0,0079	0,0045	0,0668	0,055
R14	0,1009	0,0020	0,0204	0,0005	0,0641	0,055
R15	0,0016	0,0188	0,1293	0,3758	0,0619	0,055
R16	0,0895	0,0064	0,0200	0,0084	0,0587	0,104
R17	0,0039	0,0411	0,0547	0,3770	0,0582	0,103

Джерело: розрахунки автора

Таким чином, враховуючи формули (3.1) – (3.4) постановка задачі оптимізації вагових коефіцієнтів показників кібервразливості споживачів фінансових послуг набуває наступного вигляду (формула 3.5):

$$F(w(R_1),\dots,w(R_{17})) = \sum_{i=1}^{17} w(R_i) \to 1$$

$$\{\sum_{i=1}^{17} w(R_i) \le 0.5\, w(R_{i,i=4\div15}) \le RO_i\, w(R_{i,i=1,2,16,17}) \ge RO_i\, w(R_i) \ge 0 \quad (3.5)$$

де $F(w(R_1),\dots,w(R_{17}))$ – функціональна залежність між ваговими коефіцієнтами $w(R_i)$ змінних $R_1,\dots,R_{17}$ – показників кібервразливості.

Вирішення задачі оптимізації вагових коефіцієнтів показників кібервразливості споживачів фінансових послуг як задачі лінійного програмування пропонується провести за допомогою інструментарію «Пошук рішення» MS Excel, зокрема методу узагальненого знижуючого градієнту. Результати проведених розрахунків представимо в графі 6 таблиці 3.2. Таким чином, найбільш впливовим при оцінюванні кібервразливості споживачів фінансових послуг є показник R2, на частку впливу якого припадає 11,1%. Наступними релевантними показниками виступають R1 та R16, вагові коефіцієнти впливу в розрізі яких сягають 10,4%.

Завершальним етапом є розрахунок інтегрального індексу кібервразливості за основі застосування мультиплікативної згортки Кіні. Враховуючи отримані на попередньому етапі вагові коефіцієнти впливу показників кібервразливості споживачів фінансових послуг, а також характер даних показників як стимуляторів чи дестимуляторів, проведемо їх згортку в єдиний інтегральний індекс кібервразливості за основі застосування мультиплікативної згортки Кіні (формула 3.6):

$$ICR_i(R_1,\dots,R_{17}) = \frac{1}{k}\left\{\prod_{i=1\div3,16}[1 + k\cdot w(R_i^+)\cdot R_i^+] \cdot \prod_{i=4\div15,17}[1 + k\cdot w(R_i^-)\cdot(1-R_i^-)] - 1\right\} \quad (3.6)$$

де $ICR_i(R_1, \dots, R_{17})$ – індекс кібервразливості для і-тої країни (абсолютна оцінка);

k – константа, яка визначає кількість показників кібервразливості;

R_i^+, R_i^- - відповідно, і-ий показник кібервразливості стимулятор та де стимулятор.

Результати проведених обчислень за формулою Кіні (3.6) систематизуємо в табличному вигляді, зокрема графах 1 та 2 таблиці 3.3.

Таблиця 3.3 – Абсолютний та відносний рівні кібервразливості споживачів фінансових послуг на множині відібраних 28 країн Європи

Країна	Абсолютний рівень кібервразливості	Країна	Абсолютний рівень кібервразливості
Бельгія	287378%	Ліхтенштейн	331317%
Болгарія	435179%	Люксембург	214931%
Чехія	349618%	Угорщина	393596%
Данія	125357%	Мальта	192096%
Німеччина	256822%	Нідерланди	120042%
Естонія	172125%	Австрія	208011%
Ірландія	366930%	Польща	309972%
Греція	336109%	Португалія	376243%
Іспанія	526414%	Румунія	491389%
Франція	299869%	Словенія	366733%
Хорватія	447456%	Словачиина	365780%
Італія	519764%	Фінляндія	148774%
Кіпр	394184%	Швеція	117005%
Латвія	361841%	Великобританія	282798%

Джерело: розрахунки автора

Абсолютне значення індексу кібервразливості споживачів фінансових послуг на множині розглянутих країн Європи не дозволяє об’єктивно оцінити та порівняти країни між собою, що призводить до необхідності визначення відносної оцінки кібервразливості споживачів фінансових послуг. Для цього визначимо відносний рівень кібервразливості споживачів фінансових послуг як співвідношення абсолютної оцінки до максимально можливого рівня, який

спостерігається на досліджуваній множині значень складових показників. Отже, максимально можливе значення абсолютного індекса кібервразливості обчислимо наступним чином (формула 3.7):

$$ICR_{max}(R_1, \dots, R_{17}) = \frac{1}{k}\left\{ \prod_{i=1\div3,16} [1 + k \cdot w(R_i) \cdot R_i] \cdot \prod_{i=4\div15,17} [1 + k \cdot w(R_i) \cdot (1 - R_i)] - 1 \right\} \quad (3.7)$$

де $ICR_{max}(R_1, \dots, R_{17})$ – максимально можливе значення абсолютного індекса кібервразливості.

Враховуючи представлені вище формули (3.6) та (3.7), а саме визначивши їх співвідношення, отримаємо шуканий відносний індекс кібервразливості споживачів фінансових послуг (формула 3.8):

$$VICR_i(R_1, \dots, R_{17}) = \frac{ICR_i(R_1, \dots, R_{17})}{ICR_{max}(R_1, \dots, R_{17})} \quad (3.8)$$

де $VICR_i(R_1, \dots, R_{17})$ - індекс кібервразливості для і-тої країни (відносна оцінка).

Представимо результати проведених обчислень за допомогою формули 3.8 на рисунку 3.2.

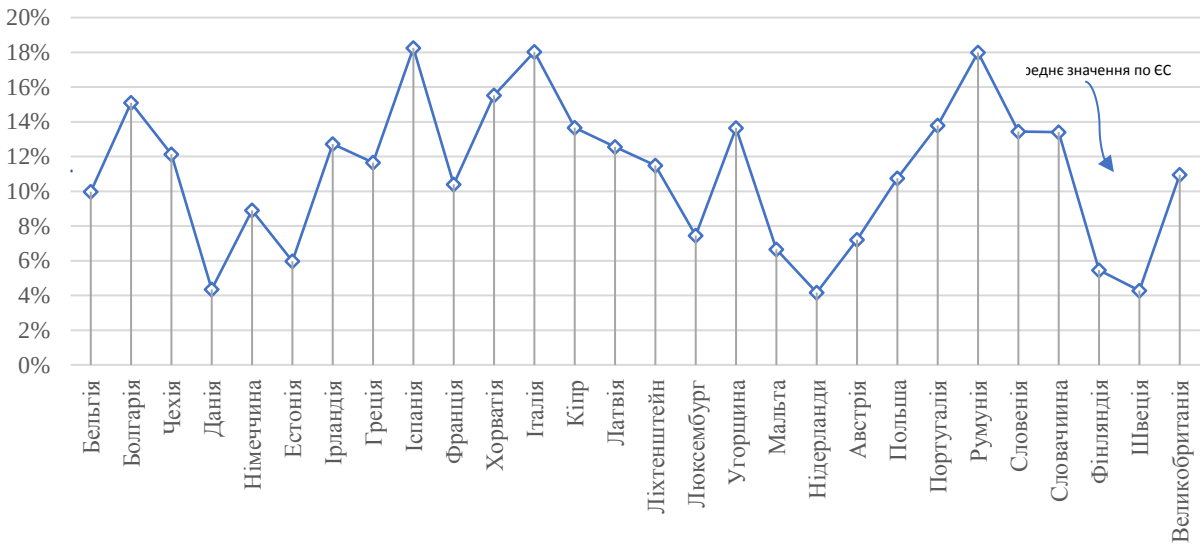


Рисунок 3.2 – Результати оцінювання рівня кібервразливості споживачів фінансових послуг у країнах Європи станом на 2020 рік

Проведене дослідження засвідчило, що рівень кібервразливості громадян ЄС становить у середньому 11%, що дозволяє стверджувати про усвідомленість населенням європейський країн наявних загроз у віртуальному просторі, способів захисту від кіберзлочинності. Проте рівень кібервразливості споживачів фінансових послуг у розрізі країн ЄС не є однорідним, а саме найменшим ризик стати жертвою кібершахрайства мають громадяни таких країн як Данія, Нідерланди, Швеція. До країн з найвищими значеннями розрахованого рівня кібервразливості споживачів фінансових послуг (18%) належать: Іспанія, Італія, Румунія.

Таким чином, проведений аналіз рівня кібервразливості споживачів фінансових послуг на прикладі країн ЄС засвідчує ефективність здійснюваних регуляторних та просвітницьких заходів з інформування населення про потенційні загрози у віртуальному просторі та способи захисту від кіберзагроз. Варто зазначити, що для моніторингу рівня кібервразливоті громадян при здійсненні ними фінансових розрахунків необхідно проводити розрахунки на щорічній основі, оскільки відбувається постійна інтелектуалізація методів та способів здійснення кібершахрайств.

3.2 Побудова фазового портрету потенційної жертви кіберзлочинності у сфері фінансових послуг

Активізація зусиль щодо зменшення кількості кібержертв від фінансових операцій неможлива у відриві від наукового забезпечення системи кіберзахисту. Сучасний розвиток інформаційних технологій дозволяє акумулювати великі масиви даних, їх обробляти та отримувати науково обґрунтовані закономірності, які доцільно враховувати при формуванні системи попередження кіберзагроз у фінансовому секторі. Одним з провідних напрямків у вирішенні цього завдання є розробка фазового портрету ймовірної жертви кібершахрайства у фінансовій системі, що дозволяє ідентифікувати ознаки кіберзагрози на ранніх етапах, відповідно відреагувати на неї, тим самим нейтралізувати або мінімізувати негативні наслідки. Використання технології профайлінгу дозволяє оцінити та спрогнозувати поведінку споживача фінансових послуг в умовах зростаючого ризику кібершахрайств на основі систематизації та встановлення причинно-наслідкових зв’язків між найбільш інформативними персоніфікованими їх ознаками. Зауважимо, що технологій профайлінгу є досить поширеною практикою в діяльності правоохоронних органів для встановлення типових психотипів злочинців.

Для його побудови використано дані соціологічного опитування громадян Європейського Союзу станом на 2020 рік. Для аналізу обрано 25 країн світу. В основі побудови фазового портрету споживача фінансових послуг є індикатор «частка населення, які стикалися з кібершахрайствами у сфері фінансових послуг» у розрізі європейських країн, динаміка якого представлена на рисунку 3.3.

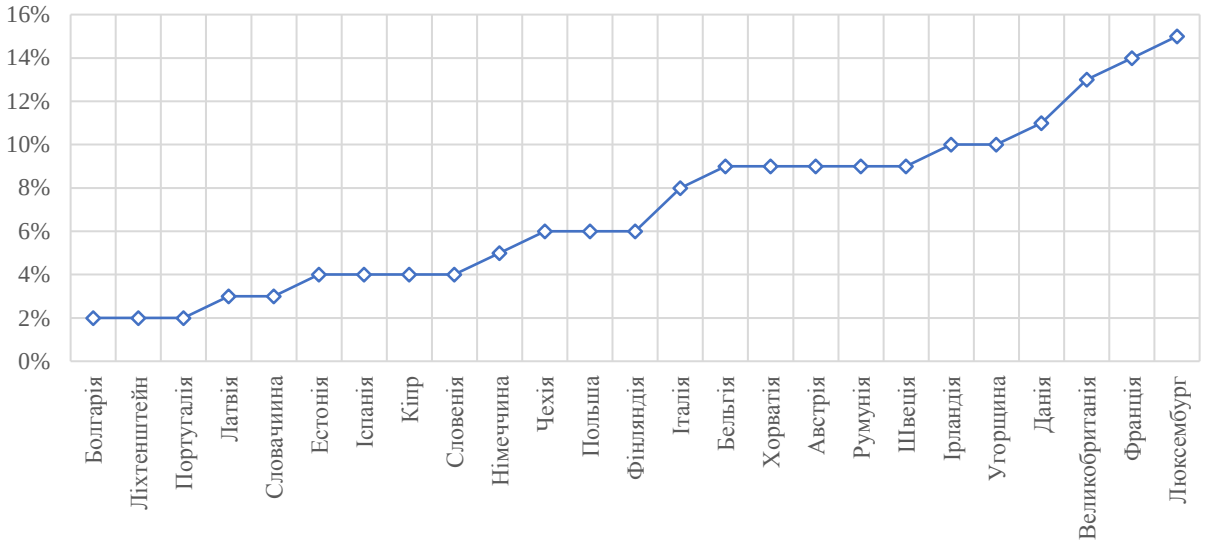


Рисунок 3.3 – Частка громадян країн Європейського Союзу, які стикалися з кібершахрайствами у сфері фінансових послуг у 2020 році, %

Дані рисунку 3.3 наочно демонструють, що до країн з найвищими показниками кібершахрайства у сфері фінансових послуг належить Люксембург (15%), Франції (14%), Великобританії (13%) та Данії (11%). У 2020 році у середньому кожний 10-й житель Європейського Союзу став кібержертвою при здійсненні фінансових транзакцій.

Для побудови портрету ймовірної кібержертви споживача фінансових послуг використано первинні дані щодо опитування у розрізі 55 інформаційних ознак (таблиця 3.4) на основі даних 25 європейських країн.

Сформована статистична база для побудови фазового портрету жертви кіберзлочинності подана в таблиці Г.1, додатку Г.

Наступним кроком є вибір найбільш релевантних індикаторів, що характеризують кібершахрайства при здійсненні фінансових транзакцій . В рамках даного етапу проведений одномірний тест значущості впливу різних інформаційних ознак на результативний показник – «особи, які стикалися з кібершахрайствами у сфері фінансових послуг» за допомогою сигма-обмеженої параметризації та діаграми Парето t-значень для коефіцієнтів GRM та ідентифіковано релевантні факторами віктимної поведінки споживача

фінансових послуг (рисунок 3.4). Для реалізації даного етапу використовується інструментарій Statistics.

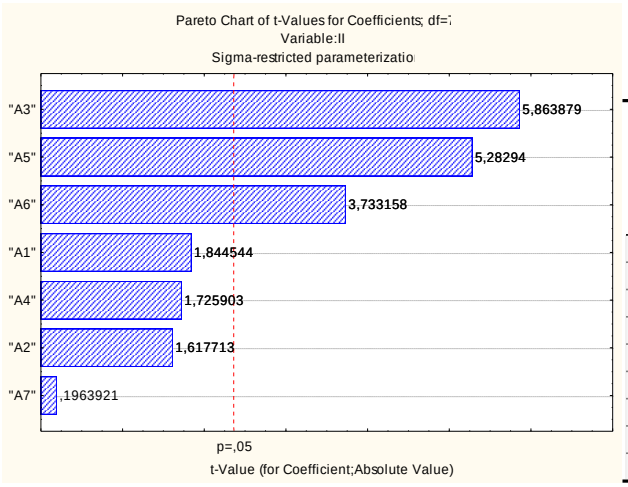
Таблиця 3.4 – Вхідні дані для побудови фазового портрету жертви кіберзлочинності

Стать	Чоловіча (G1); жіноча (G2)
Вік	від 15 до 24 років (A1); від 25 до 34 років (A2); від 35 до 44 років (A3); від 45 до 54 років (A4); від 55 до 64 років (A5); від 65 до 74 років (A6); від 75 і більше (A7).
Сфера діяльності	особа, яка навчається (SPC1); фрілансер (вільнозайнятий) (SPC2); управлінець (SPC3); інші працівники розумової праці (SPC4); працівники фізичної праці (SPC5); домогосподарства (SPC6); безробітній(-я) (SPC7); пенсіонер(-ка) (SPC8); студент(-ка) (SPC9).
Сімейний стан	Одружений/заміжня (MS1); одинокий(-а), який(-а) проживає з партнером (MS2); неодружений/незаміжня (MS3); розлучений (-а) (MS4); вдова/вдівець (MS5)
Стан сім'ї	одне домогосподарство без дітей (HS1); одне домогосподарство з дітьми (HS2); декілька домогосподарств без дітей (HS3); декілька домогосподарство з дітьми (HS4)
Склад сім'ї	одна дитина (HC1); дві дитини (HC2); три дитини (HC3); чотири дитини та більше (HC4)
Труднощі з оплатою рахунків	дуже часто (DPB1); часто (DPB2); час від часу (DPB3); майже ніколи / ніколи (DPB4)
Соціальний статус особи	робочий клас (C1); нижчий середній клас (C2); середній клас (C3); вищий середній клас (C4); вищий клас (C5).
Тип місцевості	сільська місцевість (SU1); мале/середнє місто (SU2), велике місто (SU3)
Рівень користування інтернетом	постійно (UI1); інколи (UI2)
Пристрої для доступу до Інтернету	домашній комп’ютер (DAI1); ноутбук (DAI2); планшет (DAI3); смартфон (DAI4); телевізор (DAI5); ігрова консоль (DAI6)
Канали про інформування про кіберзлочинність	веб-сайт (AEP1); адреса електронної пошти (AEP2); онлайн-форма (AEP3); контактний номер (AEP4); будь-яким іншим способом (AEP5).

Інформаційна ознака «вік особи».

Дані стосовно опитування громадян Європейського Союзу щодо їх відношення до питань кібербезпеки акумулювалися у розрізі 7 градацій вікової структури. У 2020 році найвищі значення показника кіберзлочинності у сфері фінансових послуг (21%) зафіксовано для громадян Литви у віці 25-34 роки та

громадян Італії у віці більше 75 років. Для визначення найбільш значущих інформаційних ознак «вік» з позиції стати кібержертвою побудовано діаграму Парето (рисунок 3.4).



Univariate Tests of Significance for Spreadsheet3 a
Sigma-restricted parameterization
Effective hypothesis decomposition

Effect	SS	Degr. of Freedom	MS	F	p
Intercept	0,00021	1	0,00021	10,4036	0,01454
"A1"	0,00006	1	0,00006	3,4023	0,10762
"A2"	0,00005	1	0,00005	2,6169	0,14975
"A3"	0,00069	1	0,00069	34,3850	0,00062
"A4"	0,00006	1	0,00006	2,9787	0,12801
"A5"	0,00056	1	0,00056	27,9094	0,00114
"A6"	0,00028	1	0,00028	13,9364	0,00732
"A7"	0,00000	1	0,00000	0,0385	0,84988
Error	0,00014	7	0,00002		

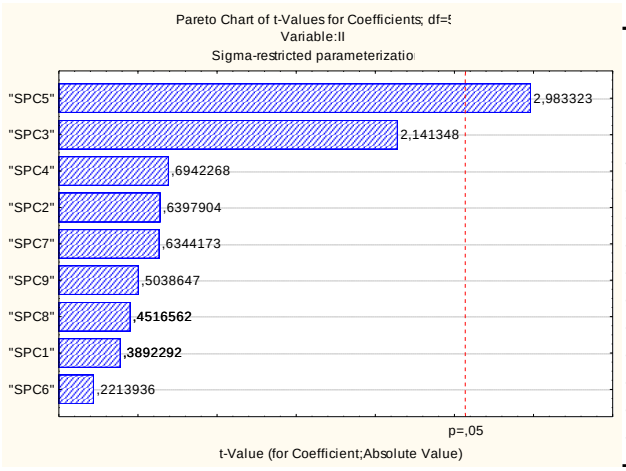
Рисунок 3.4 – Скріншот фрагменту діаграми Парето t-значень значущості (лівий фрагмент) та одномірного тесту значущості впливу інформаційної ознаки «вік» на результативний показник (правий фрагмент)

На основі даних рисунку 3.4, в правому фрагменті якого приведені одномірні результати для оцінки ступеня та характеру взаємозв'язку між рівнем кібершахрайства у сфері фінансових послуг та віковою структурою, можна стверджувати, що статистично значущими виступають такі ефекти, як: особи у віці від 35 до 44 років (A3); від 55 до 64 років (A5); від 65 до 74 років (A6), оскільки рівні значущості p критерія Фішера менше 0,05. Найбільший вклад в загальну модель вносить ефект A3, оскільки сума квадратів відхилень SS, яка приймає значення 0,000697, має найбільше значення. Далі вклад статистично значущих ефектів розподіляється наступним чином: A5 та A6. Візуальним підтвердженням значущості даних трьох ефектів виступає діаграма Парето t-значень значущості (лівий фрагмент рисунку 3.4).

Інформаційна ознака «сфера діяльності особи».

Найбільший рівень кібершахрайства серед споживачів фінансових послуг зафіксовано для наступних сфер їх діяльності: особи, які навчаються

(17% – Угорщина); фрілансер (23% – Данія); управлінець (23% – Ірландія); інші працівники розумової праці (22% – Франція); працівники фізичної праці (17% – Латвія); домогосподарства (24% – Болгарія); безробітній(-я) (23% – Данія); пенсіонер(-ка) (14% – Великобританія); студент(-ка) (17% – Угорщина). Побудова діаграми Парето дозволяє відібрати тільки значущі причинно-наслідкові зв'язки між інформаційною ознакою «сфера діяльності особи» та обсяги кібершахрайств у сфері фінансових відносин (рисунок 3.5).



Univariate Tests of Significance for (Spreadsheet3 a
Sigma-restricted parameterization
Effective hypothesis decomposition

Effect	SS	Degr. of Freedom	MS	F	p
Intercept	0,00003	1	0,00003	0,34060	0,58481
"SPC1"	0,00001	1	0,00001	0,15149	0,71313
"SPC2"	0,00004	1	0,00004	0,40933	0,55046
"SPC3"	0,00049	1	0,00049	4,58537	0,08517
"SPC4"	0,00005	1	0,00005	0,48195	0,51846
"SPC5"	0,00095	1	0,00095	8,90021	0,03068
"SPC6"	0,00000	1	0,00000	0,04901	0,83354
"SPC7"	0,00004	1	0,00004	0,40248	0,55369
"SPC8"	0,00002	1	0,00002	0,20399	0,67043
"SPC9"	0,00002	1	0,00002	0,25388	0,63576
Error	0,00053	5	0,00010		

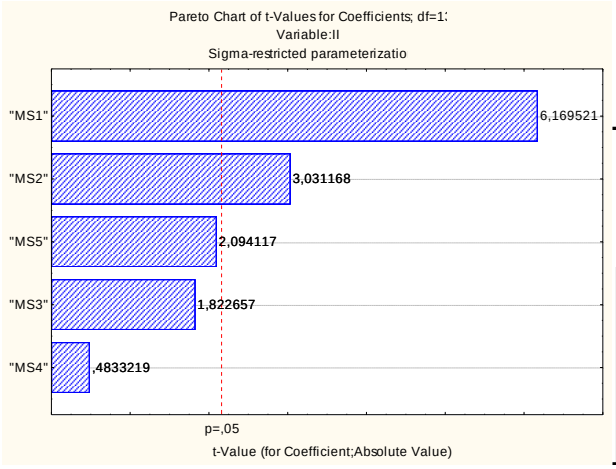
Рисунок 3.5 – Скріншот фрагменту діаграми Парето t-значень значущості (лівий фрагмент) та одномірного тесту значущості впливу інформаційної ознаки «сфера діяльності особи» на результативний показник (правий фрагмент)

Дані рисунку 3.5 наочно засвідчують, що статистично значущим виступає лише один ефект такий, як працівники фізичної праці (SPC5), оскільки рівень значущості p критерія Фішера лише для даного показника менше 0,05. Візуальним підтвердженням значущості зазначеного ефекту для індикатора SPC5 виступає діаграма Парето t-значень (лівий фрагмент рисунку 3.6).

Інформаційна ознака «сімейний статус особи».

Серед європейських країн жертвами кіберзлочинності у середньому ставали 7% одружені/заміжні особи (тоді як у Франції – 16%, Латвія – 15%);

8% одинокий(-а), який(-а) проживає з партнером (Італія, Румунія – 14%); 7% неодружений/незаміжня (Латвія – 15%, Великобританія – 13%); 7% розлучений (-а) (Великобританія – 20%, Франція – 16%); 9% вдова/вдівець (Франція – 21%). Діаграма Парето t-значень відображена на рисунку 3.6.



Univariate Tests of Significance for Spreadsheet3 a
Sigma-restricted parameterization
Effective hypothesis decomposition

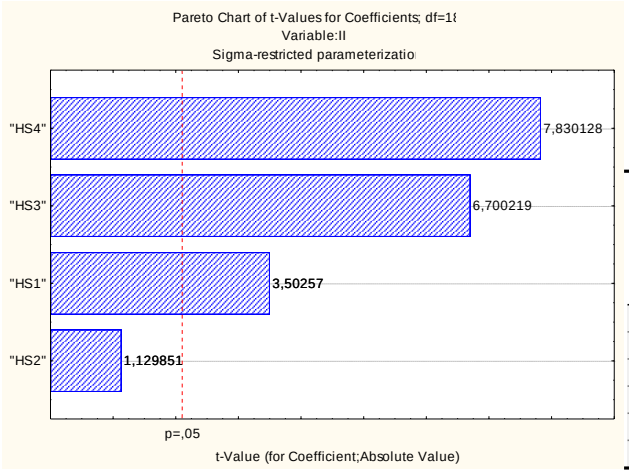
Effect	SS	Degr. of Freedom	MS	F	p
Intercept	0,00005	1	0,00005	1,0211	0,33068
"MS1"	0,00189	1	0,00189	38,0629	0,00003
"MS2"	0,00045	1	0,00045	9,1879	0,00964
"MS3"	0,00016	1	0,00016	3,3220	0,09142
"MS4"	0,00001	1	0,00001	0,2336	0,63690
"MS5"	0,00021	1	0,00021	4,3853	0,05641
Error	0,00064	13	0,00005		

Рисунок 3.6 – Скріншот фрагменту діаграми Парето t-значень значущості (лівий фрагмент) та одномірного тесту значущості впливу інформаційної ознаки «сімейний статус» на результативний показник (правий фрагмент)

Оскільки рівень значущості p критерія Фішера менше 0,05 лише для двох показників (одружені/заміжні особи (MS1), одинокий(-а), який(-а) проживає з партнером (MS2)), то можемо стверджувати про необхідність їх подальшого врахування в наступних розрахунках при побудові фазового портрету кібержертви споживача фінансових послуг. Найбільший вклад в загальну модель вносить ефект MS1, оскільки сума квадратів відхилень SS має найбільше значення (0,001898). Візуальним підтвердженням значущості даних двох ефектів виступає діаграма Парето t-значень (лівий фрагмент рисунку 3.6).

Інформаційна ознака «стан сім'ї».

Домогосподарства, які мають дітей, частіше ставало жертвою кібершахрайства при користуванні фінансовими послугами. Результати відбору значимих інформаційних чинників «стан сім'ї» подано на рисунку 3.7.



Univariate Tests of Significance for Spreadsheet3 a
Sigma-restricted parameterization
Effective hypothesis decomposition

Effect	SS	Degr. of Freedom	MS	F	p
Intercept	0,00000	1	0,00000	0,0205	0,88757
"HS1"	0,00040	1	0,00040	12,2679	0,00254
"HS2"	0,00004	1	0,00004	1,2765	0,27337
"HS3"	0,00146	1	0,00146	44,8929	0,00000
"HS4"	0,00200	1	0,00200	61,3109	0,00000
Error	0,00058	18	0,00003		

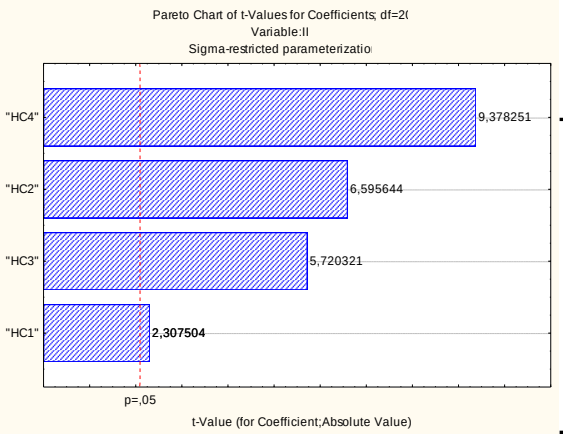
Рисунок 3.7 – Скріншот фрагменту діаграми Парето t-значень значущості (лівий фрагмент) та одномірного тесту значущості впливу інформаційної ознаки «стан сім'ї» на результативний показник (правий фрагмент)

На основі даних рисунку 3.7, зауважимо, що найбільш релевантними (рівень значущості p критерія Фішера менше 0,05) характеристиками інформаційної ознаки «стан сім'ї» є одне домогосподарство без дітей (HS1); декілька домогосподарств без дітей (HS3); декілька домогосподарство з дітьми (HS4). Найбільший вклад в загальну модель вносить ефект HS4 - Household with children оскільки сума квадратів відхилень SS, яка приймає значення 0,002, має найбільше значення. Далі вклад статистично значущих ефектів розподіляється наступним чином: HS3 - Multiple Household without children, HS1 - Single Household without children. Графічне представлення отриманих результатів відображає діаграма Парето (лівий фрагмент рисунку 3.7).

Інформаційна ознака «склад сім'ї».

До топ європейських країн, особи яких ставали кібержертвами у сфері фінансових послуг залежно від складу їх сім'ї, відзначимо наступних: громадян Литви, які мають одну дитину (22%); громадян Данії, які мають троє дітей (20%); громадян Франції, які мають чотири та більше дітей (18%). Проведений аналіз відбору найбільш значущих складових інформаційної

ознаки «склад сім'ї» підтвердив необхідність включення всіх елементів: HC1-HC4 (рисунок 3.8).



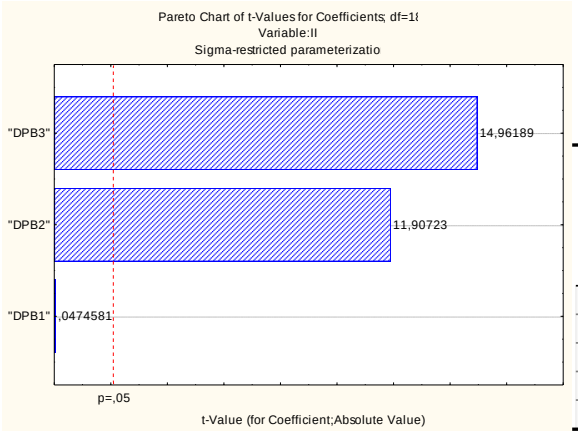
Univariate Tests of Significance for Spreadsheet3 a
Sigma-restricted parameterization
Effective hypothesis decomposition

Effect	SS	Degr. of Freedom	MS	F	p
Intercept	0,00000	1	0,00000	0,3030	0,58806
"HC1"	0,00013	1	0,00013	5,3245	0,03184
"HC2"	0,00108	1	0,00108	43,5025	0,00000
"HC3"	0,00081	1	0,00081	32,7220	0,00001
"HC4"	0,00219	1	0,00219	87,9515	0,00000
Error	0,00050	20	0,00002		

Рисунок 3.8 – Скріншот фрагменту діаграми Парето t-значень значущості (лівий фрагмент) та одномірного тесту значущості впливу інформаційної ознаки «склад сім'ї» на результативний показник (правий фрагмент)

Інформаційна ознака «труднощі з оплатою рахунків».

За результатами аналізу даних опитування встановлено, що 12% середньостатистичних європейців мали труднощі з оплатою рахунків, та відповідно вони у більшій мірі схильні стати жертвою кібершахрайства. Побудована діаграма Парето та розрахований одномірний тест значущості (рисунок 3.9) вказує, що найбільш релевантними складовими для характеристики інформаційної ознаки «труднощі з оплатою рахунків» є відповідь «часто» (DPB2) ; відповідь «інколи» (DPB3). Найбільший вклад в загальну модель вносить ефект DPB3, оскільки сума квадратів відхилень (SS) для даного показника є найбільшою (0,009393).



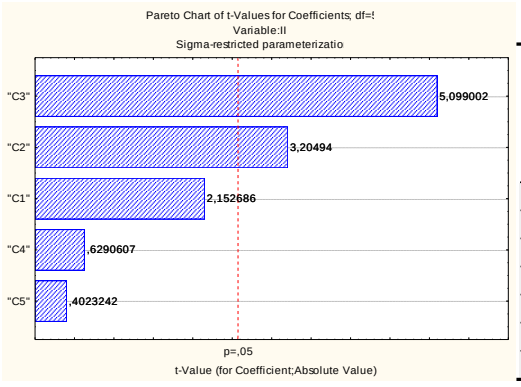
Univariate Tests of Significance for Spreadsheet3 a
Sigma-restricted parameterization
Effective hypothesis decomposition

Effect	SS	Degr. of Freedom	MS	F	p
Intercept	0,00001	1	0,00001	0,355(	0,55870
"DPB1"	0,00000	1	0,00000	0,002	0,96267
"DPB2"	0,00594	1	0,00594	141,782	0,00000
"DPB3"	0,00939	1	0,00939	223,858	0,00000
Error	0,00075	18	0,00004		

Рисунок 3.9 – Скріншот фрагменту діаграми Парето t-значень значущості (лівий фрагмент) та одномірного тесту значущості впливу інформаційної ознаки «труднощі з оплатою рахунків» на результативний показник (правий фрагмент)

Інформаційна ознака «соціальний статус особи».

Соціальний статус споживача фінансових послуг розглянуто у межах 5 градацій. Середньостатистичні європейці, які вважають себе належним до вищого класу (33%) частіше ставали жертвами протиправної діяльності у віртуальному просторі порівняно з тими особами, які ставлять себе нижче в соціальній шкалі.



Univariate Tests of Significance for Spreadsheet3 a
Sigma-restricted parameterization
Effective hypothesis decomposition

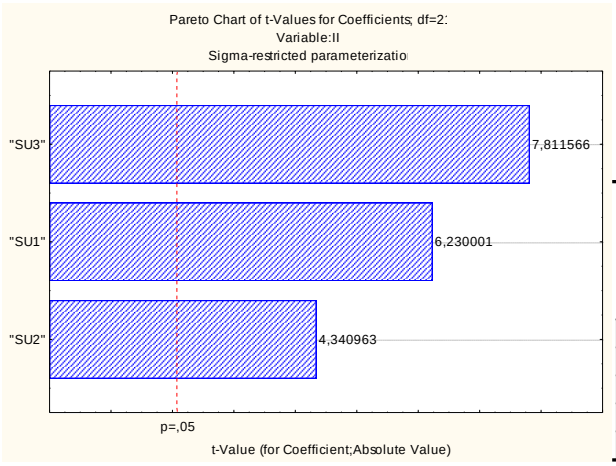
Effect	SS	Degr. of Freedom	MS	F	p
Intercept	0,00011	1	0,00011	2,7627	0,15737
"C1"	0,00018	1	0,00018	4,6340	0,08395
"C2"	0,00041	1	0,00041	10,2716	0,02386
"C3"	0,00105	1	0,00105	25,9998	0,00377
"C4"	0,00001	1	0,00001	0,3957	0,55692
"C5"	0,00000	1	0,00000	0,1618	0,70406
Error	0,00020	5	0,00004		

Рисунок 3.10 – Скріншот фрагменту діаграми Парето t-значень значущості (лівий фрагмент) та одномірного тесту значущості впливу інформаційної ознаки «соціальний статус особи» на результативний показник (правий фрагмент)

Дані рисунку 3.10 вказують, що рівень значущості критерія Фішера менше 0,05 виключно для двох індикаторів: нижчий середній клас (С2); середній клас (С3), що свідчить про їх статистично значущість.

Інформаційна ознака «тип місцевості».

Найбільша кількість правопорушень, пов'язаних із задіянням фінансової та моральної шкоди при фінансових розрахунках, пов'язана з особами, які проживають у великих містах: у Хорватії – 22% громадян, Франції – 18%, Бельгія, Австрія, Великобританія – 15%. Результати побудови графіка Парето та розрахунку одномірного тесту значущості подано на рисунку 3.11.



Univariate Tests of Significance for Spreadsheet3 a
Sigma-restricted parameterization
Effective hypothesis decomposition

Effect	SS	Degr. of Freedom	MS	F	p
Intercept	0,00000	1	0,00000	0,0001	0,98919
"SU1"	0,00293	1	0,00293	38,8129	0,00000
"SU2"	0,00142	1	0,00142	18,8439	0,00028
"SU3"	0,00461	1	0,00461	61,0205	0,00000
Error	0,00158	21	0,00007		

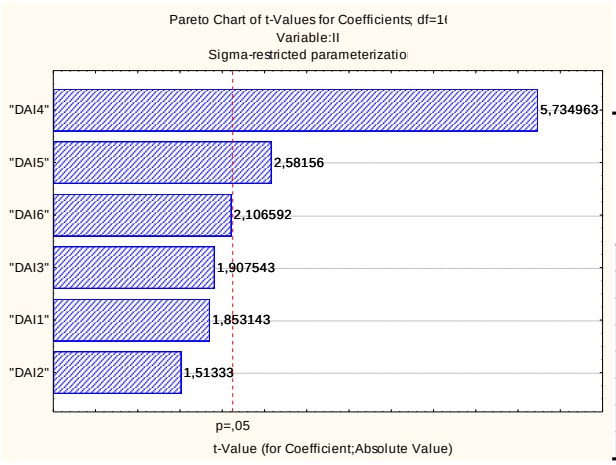
Рисунок 3.11 – Скріншот фрагменту діаграми Парето t-значень значущості (лівий фрагмент) та одномірного тесту значущості впливу інформаційної ознаки «тип місцевості» на результативний показни (правий фрагмент)

Проведені розрахунки засвідчили доцільність включення 3-х складових інформаційної ознаки «тип місцевості»: сільська місцевість (SU1); мале/середнє місто (SU2), велике місто (SU3). Найбільший вклад в загальну модель вносить ефект SU3 (сума квадратів відхилень SS = 0,004615).

Інформаційна ознака «пристрої для доступу до Інтернету»

У середньому 13% жителів європейських країн, які ставали жертвами кібершахрайства, із-за використання ігрової консолі, тоді як у деяких європейських країнах цей показник перевищує у декілька разів: Румунія – 37%, Чехія – 36%, Угорщина – 35%. Крім ігрової консолі, за результатами

опитування встановлено, що у середньому 11% європейців піддавалися кібератакам через недосконаліть системи захисту при здійсненні фінансових транзакцій через смарт-телевізори, тоді як у Румунії – 27% громадян, Угорщині – 26%, Латвія – 21%. Результати відбору значимих складових інформаційної ознаки «пристрої для доступу до Інтернету» подано на рисунку 3.12.



Univariate Tests of Significance for Spreadsheet3 a
Sigma-restricted parameterization
Effective hypothesis decomposition

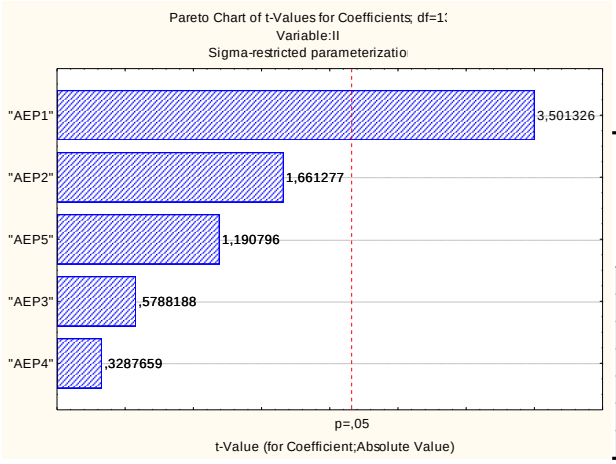
Effect	SS	Degr. of Freedom	MS	F	p
Intercept	0,00019	1	0,00019	4,7055	0,04547
"DAI1"	0,00014	1	0,00014	3,4341	0,08239
"DAI2"	0,00009	1	0,00009	2,2901	0,14969
"DAI3"	0,00015	1	0,00015	3,6387	0,07456
"DAI4"	0,00137	1	0,00137	32,8898	0,00003
"DAI5"	0,00027	1	0,00027	6,6445	0,02007
"DAI6"	0,00018	1	0,00018	4,4377	0,05129
Error	0,00066	16	0,00004		

Рисунок 3.12 – Скріншот фрагменту діаграми Парето t-значень значущості (лівий фрагмент) та одномірного тесту значущості впливу інформаційної ознаки «пристрої для доступу до Інтернету» на результативний показник (правий фрагмент)

Аналізуючи рисунок 3.12, можна зробити висновки, що на рівні 5% відхилення значущим виступає 2 показника: смартфон (DAI4); телевізор (DAI5). Візуальним підтвердженням значущості даних двох ефектів виступає діаграма Парето.

Інформаційна ознака «канали про інформування про кіберзлочинність»

Дані опитування засвідчили, що лише 13% жителів європейських країн проінформовані про способи повідомлення про кібератаку при здійсненні фінансових розрахунків. При цьому варто відзначити, що в деяких країнах Європи цей показник є критично низьким: Латвія – 1%, Іспанія, Португалія, Словаччина – 4%, Швеція – 5%. На рисунку 3.13 представимо результати побудови одномірного тесту значущості та діаграми Парето.



Univariate Tests of Significance for Spreadsheet3 a
Sigma-restricted parameterization
Effective hypothesis decomposition

Effect	SS	Degr. of Freedom	MS	F	p
Intercept	0,00320	1	0,00320	6,2278	0,02681
"AEP1"	0,00631	1	0,00631	12,2592	0,00390
"AEP2"	0,00142	1	0,00142	2,7598	0,12057
"AEP3"	0,00017	1	0,00017	0,3350	0,57260
"AEP4"	0,00005	1	0,00005	0,1080	0,74756
"AEP5"	0,00073	1	0,00073	1,4179	0,25502
Error	0,00669	13	0,00051		

Рисунок 3.13 – Скріншот фрагменту діаграми Парето t-значень значущості (лівий фрагмент) та одномірного тесту значущоості впливу інформаційної ознаки «канали про інформування про кіберзлочинність» на результативний показник (правий фрагмент)

Дані рисунку 3.13 вказують, що зі складових інформаційної ознаки «канали про інформування про кіберзлочинність» доцільно включати виключно веб-сайт (AEP1).

Крім представлених вище груп показників характеристики кібервразливості споживачів фінансових послуг, за якими проведено відбір релевантних для подальшого аналізу, залишаються дві групи в розрізі «стать особи»: чоловік (G1), жінка (G2) та «рівень користування Інтернетом»: постійно (UI1), інколи (UI2). Дані групи представлені лише двома показниками, тому відбір пріоритетності показників для них не проводився.

Відібравши релевантні показники для побудови фазового портрету потенційної кібержертви споживача фінансових послуг шляхом використання асоціативних правил виявлені причинно-наслідкові зв’язки між обраними інформаційними ознаками.

Для побудови фазового портрету споживача фінансових послуг, який став жертвою кібершахоайства використано асоціативні правила.

Побудуємо мережу асоціативних правил причинно-наслідковості зв’язків між індикаторами кібервразливості споживачів фінансових послуг. Для реалізації даного етапу використаємо програмний продукт STATISTICA:

команду Data Mining/Sequence, Association and Link Analysis. Отримані результати представимо у вигляді рисунку 3.14.

Summary of association rules (Spreadsheet3 асоц прав.sta)
Min: support = 20,0%, confidence = 10,0%
Max. size of an itemset = 10

	Body	==>	Head	Support(%)	Confidence(%)
1	0,053493<AEP1<=0,08796	==>	0,036834<HS1<=0,05361	20,0000	55,555(
2	0,036834<HS1<=0,05361	==>	0,053493<AEP1<=0,08796	20,0000	71,428(
3	0,056192<MS2<=0,07181	==>	0,053493<AEP1<=0,08796	20,0000	83,333(
4	0,053493<AEP1<=0,08796	==>	0,056192<MS2<=0,07181	20,0000	55,555(
5	0,019518<HC3<=0,04083	==>	0,053493<AEP1<=0,08796	20,0000	55,555(
6	0,053493<AEP1<=0,08796	==>	0,019518<HC3<=0,04083	20,0000	55,555(
7	0,019420<G2<=0,03933	==>	0,053493<AEP1<=0,08796	20,0000	62,500(
8	0,053493<AEP1<=0,08796	==>	0,019420<G2<=0,03933	20,0000	55,555(
9	0,023606<DPB2<=0,05112	==>	0,019420<G2<=0,03933	24,0000	75,000(
10	0,019420<G2<=0,03933	==>	0,023606<DPB2<=0,05112	24,0000	75,000(
11	0,023606<DPB2<=0,05112	==>	0,019420<G2<=0,039332, 0,019518<HC3<=0,040	20,0000	62,500(
12	0,019518<HC3<=0,04083	==>	0,019420<G2<=0,039332, 0,023606<DPB2<=0,051	20,0000	55,555(
13	0,019518<HC3<=0,040831, 0,023606<DPB2<=0,051	==>	0,019420<G2<=0,03933	20,0000	83,333(
14	0,019420<G2<=0,03933	==>	0,019518<HC3<=0,040831, 0,023606<DPB2<=0,051	20,0000	62,500(
15	0,019420<G2<=0,039332, 0,023606<DPB2<=0,051	==>	0,019518<HC3<=0,04083	20,0000	83,333(

Рисунок 3.14 – Скріншот фрагменту ідентифікованих асоціативних правил

На основі поглибленого аналізу статистичних даних щодо кібершахрайств у сфері фінансових послуг шляхом побудови асоціативних правил, представлених на рисунку 3.14 та в таблиці Г.2 (додатку Г), можна зробити наступні висновки:

– у 100% аналізованих випадків кібершахрайств у сфері фінансових послуг серед жителів європейських країн виявлено стійкі закономірності між такими параметрами: «заміжня жінка, яка виховує трьох дітей», «жінка у віці 55-64 роки, яка виховує трьох дітей», «заміжня (одружена) особа, яка періодично відчуває фінансову труднощі та виховує трьох дітей», «особа, яка проживає у сільській місцевості та виховує трьох дітей», «особа у віці 65-74 роки, яка має трьох дітей».

– ймовірність стати жертвою кібершахрайства жінці, яка виховує трьох дітей становить 87,5%;

– з ймовірністю в 83,3% прослідковуються причинно-наслідкові зв’язки між наступними параметрами: «жінка, яка періодично відчуває

фінансову труднощі та виховує трьох дітей», «жінка, яка має дитину», «жінка у віці 55-64 роки», «заміжня (одружена) особа, яка виховує двох дітей», «особа, яка проживає у невеликому місті та виховує двох (трьох) дітей»

– у 71,4% випадків кіберзлочинності у сфері фінансових послуг прослідковується тісний каузальний зв’язок з такими параметрами: «працівник фізичної праці, у якого кібератака відбулася через смартфон», «особа, яка періодично відчуває фінансові труднощі та кібератака відбулася через смартфон».

Таким чином, ідентифіковані параметри за допомогою використання алгоритму асоціативних правил дозволяють визначити найбільш вразливі категорії населення, які потребують посиленої інформаційно-консультаційної допомоги в підвищенні рівня їх інформаційної безпеки при здійсненні фінансових транзакцій.

3.3 Оцінювання впливу фінансових та кібернетичних злочинів на рівень довіри до фінансового сектору

Довіра споживачів фінансових послуг є ключовим компонентом стабільного функціонування фінансових установ в контексті постійно зростаючих викликів, спричинених збільшенням частоти та обсягів шахрайства із платіжними картками, несанкціонованого доступу до персональних даних клієнтів, незаконного списання коштів із банківських рахунків тощо.

Довіра споживачів до фінансових установ формується як рівні держави (контроль з боку національного фінансового регулятора за виконанням фінансовими установами заходів із забезпечення кіберзахисту та інформаційної безпеки, проведення просвітницьких заходів щодо підвищення рівня фінансової грамотності та цифрової гігієни) та на рівні фінансової установи (проведення внутрішнього аудиту кібербезпеки фінансової установи, постійний моніторинг інформаційного середовища платіжної інфраструктури,

інформування клієнтів про найбільш поширені способи вчинення кібершахрайств у сфері фінансових послуг). Виходячи з цього, збереження та зміцнення довіри споживачів до фінансового сектору є комплексним пріоритетним завданням як національного фінансового регулятора, так і фінансових установ. Оскільки зниження довіри громадянина до фінансової установи супроводжується відтоком коштів з депозитних рахунків, збільшення обсягу зняття готівки, закриттям банківських рахунків тощо. Дані процеси неодмінно матимуть вплив на показниках функціонування фінансових установ – зниження ліквідності банків, скорочення ресурсів банків для корпоративного та роздрібного кредитування, а також для вкладання коштів в інвестиційні проєкти.

Довіру до фінансових установ у контексті кібернетичних загроз доцільно розглядати з двох точок зору: перша – фінансові установи є ціллю кіберзлочинців, порушення інформаційної безпеки яких може призвести до фінансових збитків, порушення цілісності, доступності та конфіденційності даних як фінансової установи, так і її клієнтів, а також репутаційних ризиків; друга – клієнти фінансової установи є ціллю кіберзлочинців, у результаті чого відбувається крадіжка коштів, збір персональних даних про клієнта.

У межах даного дослідження висунуто робочу гіпотезу – зростання обсягів фінансових кібершахрайства в країні призводить до зменшення довіри населення до фінансових установ.

У межах дослідження запропоновано науково-методичний підхід до оцінювання дискретного лагового впливу фінансових кібершахрайств на рівень довіри клієнтів до фінансових установ. Для врахування часової затримки при кількісному вимірюванні взаємозв’язків між економічними процесами використано поліноміальну модель розподіленого лагу Алмона.

В умовах дефіциту офіційної статистичної інформації щодо обсягу кібершахрайств у сфері фінансових послуг у розрізі окремої країни, а також збільшення кількості цифрових слідів в інтернет просторі для дослідження запропоновано обрати дані про запити користувачів у пошуковій мережі

Google. Google Trends є одним з найпоширеніших в емпіричній економічній літературі інструментів для генерації первинного масиву даних. Популярність пошукових запитів, про які повідомляє Google, часто розглядається як непрямий метод вимірювання уваги до певної події чи теми [98]. Google Trends став важливим аналітичним інструментом для дослідників у галузі медицини [99, 100, 101, 102, 103] та соціальних наук [104, 105].

Дані у звітах Google Trends в основному є валідними. Значення певного атрибута коливається у межах від 0 до 100. Однак існують певні ситуації, в яких значення атрибута набуває нецілого значення, зокрема "<1". Це означає, що пошук певного атрибута в аналізований період часу мав достатній обсяг, щоб відобразитися у звіті Google Trends, але менше, ніж 1/100 частина від періоду з найвищою популярністю [98].

Дослідницька вибірка охоплює період з січня 2005 року по серпень 2023 року, загалом 104 щомісячні спостереження. Об’єктом для дослідження обрано Україну, Німеччину, США та Польщу. Для потреб даного дослідження сформовано 2 групи пошукових запитів, які відображають рівень зацікавленість користувачів відповідним питанням:

1 група – пошукові запити, що відображають віктимізацію споживачів фінансових послуг (кіберполіція (X1), шахрайство (X2), заблокувати картку (X3), повернення помилково перерахованих коштів (X4), інформаційна безпека (X5)). Зауважимо, що всі пошукові запити акумулювалися у сфері «фінансів»;

2 група – пошукові запити, що характеризують довіру до фінансової установи (кредитний ліміт (Y1), змінити банк (Y2), закриття рахунку (Y3), інтернет ліміт (Y4), рейтинг банків (Y5)). До пошукових запитів також було застосовано фільтр «фінанси».

Запропонований науково-методичний підхід до оцінювання впливу фінансових кібершахрайств на рівень довіри клієнтів до фінансових установ запропоновано реалізовувати на основі поетапного виконання таких завдань:

1. Акумулювання первинних даних у межах визначених пошукових запитів у розрізі аналізованих країн з о використанням інструментів пошукової системи Google Trends.

2. Нормалізацію показників за допомогою методу MPI (Mazziotta Pareto Index).

3. Визначення інтегральних показників, що характеризують рівень віктимізації споживачів фінансових послуг та рівень довіри на фінансових установ за допомогою функції Berger and Casella.

4. Ідентифікація величини лагових затримок між інтегральними показниками за допомогою автокореляційних функцій та корелограм.

5. Оцінювання впливу фінансових кібершахрайств на рівень довіри клієнтів до фінансових установ шляхом побудови поліноміальних моделей розподіленого лагу Алмона.

Перший етап науково-методичного підходу передбачає формування статистичного масиву інформацію щодо результатів пошукових запитів.

Другий етап спрямований на приведення показників вхідної статистичної бази дослідження до співставного вигляду відбувається за допомогою застосування методу MPI (Mazziotta Pareto Index), тобто наступного співвідношення (формула 3.9):

$$z_{ijg} = \left[100 + \frac{x_{ijg} - M_{x_{ig}}}{S_{x_{ig}}}\right] / 100 \qquad (3.9)$$

де z_{ijg} – нормалізоване значення і-го показника в розрізі j-го періоду для g-ої країни;

x_{ijg} - фактичне значення і-го показника в розрізі j-го періоду для g-ої країни;

$M_{x_{ig}}$ – математичне сподівання і-го показника для g-ої країни за розглянутий часовий інтервал;

$S_{x_{ig}}$ – середнє квадратичне відхилення і-го показника для g-ої країни за розглянутий часовий інтервал.

Таблиця 3.5 – Фрагмент нормалізованих значень показників на прикладі України

	X1	X2	X3	X4	X5	Y1	Y2	Y3	Y4	Y5
2015-01	0,869	0,963	0,833	0,841	0,920	0,865	0,921	0,887	1,167	1,113
2015-02	0,880	0,951	0,895	0,841	0,960	0,844	0,921	1,231	0,868	1,341
2015-03	0,869	0,835	0,929	1,195	1,017	0,833	1,098	1,049	0,868	1,363
2015-04	0,869	0,967	0,923	1,075	0,989	0,807	0,921	1,034	0,868	1,124
2015-05	0,869	0,955	0,985	0,981	1,028	0,913	1,028	1,024	0,868	1,163
2015-06	0,869	0,930	0,833	0,841	1,023	0,838	0,921	1,008	0,868	1,141
2015-07	0,869	1,033	1,025	1,244	0,920	0,870	0,921	0,897	0,983	1,335
2015-08	0,869	1,079	1,036	0,841	0,898	0,944	1,093	0,963	1,110	1,124
2015-09	0,869	1,029	0,934	0,981	0,926	0,849	0,921	0,953	0,978	1,141
2015-10	1,145	1,038	1,076	0,841	0,977	0,838	0,921	0,938	1,079	1,058
…	…	…	….	…	…	…	…	…	…	…
2022-11	1,180	1,054	1,013	1,030	1,125	1,199	1,177	0,993	1,180	0,886
2022-12	1,203	0,992	1,036	0,941	1,040	1,140	1,387	1,145	0,996	1,069
2023-01	1,188	1,095	1,053	1,055	0,971	1,252	1,130	1,049	0,934	1,097
2023-02	1,258	1,058	1,087	1,021	1,023	1,162	1,056	1,064	1,009	0,991
2023-03	1,196	1,091	1,183	0,991	1,062	1,225	1,154	1,029	1,079	1,086
2023-04	1,153	1,203	1,070	0,941	1,079	1,183	1,093	1,018	1,013	1,069
2023-05	1,215	1,223	1,398	0,906	1,244	1,199	1,186	1,029	1,018	1,080
2023-06	1,211	1,182	1,285	0,951	1,000	1,294	1,014	1,130	1,013	0,958
2023-07	1,149	1,153	1,364	0,991	0,920	1,220	1,098	1,211	1,062	1,019
2023-08	1,129	1,153	0,833	0,841	0,903	1,337	1,121	1,084	0,868	1,008

Метою третього етапу є визначення двох інтегральних показників (рівень віктимізації споживачів фінансових послуг (IX), рівень довіри до фінансових послуг (IY)) шляхом застосування трансформації Box-Cox до нормалізованих даних і подальшої згортки за допомогою функції Berger and Casella:

– трансформація Box-Cox (формула 3.10):

$$h_1 = x - 1 \tag{3.10}$$

– середня арифметична Berger and Casella (формула 3.11):

$$F(\mu_{jg}) = \frac{1}{m}\sum_{i=1}^{m} (z_{ijg} - \mu_{jg})^2 \qquad (3.11)$$

$$\mu_{jg} = h_1^{-1}(\frac{1}{m}\sum_{i=1}^{m} h_1\ (z_{ijg})\ )$$

де $F(\mu_{jg})$ – інтегральний показник Berger and Casella в розрізі j-го періоду для g-ої країн.

Результати розрахунку інтегральних показників рівня віктимізації споживачів фінансових послуг (FX) та рівня довіри до фінансових послуг (FY) для України наведено на рисунку 3.15.

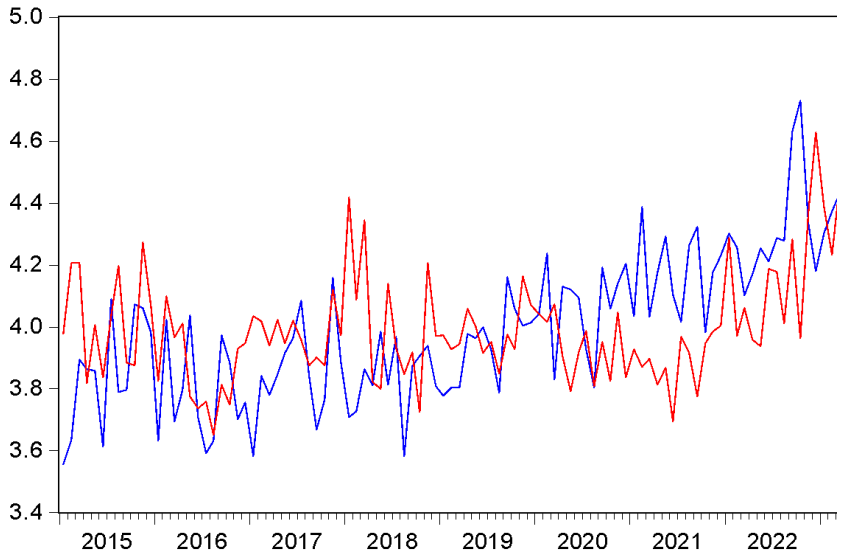


Рисунок 3.15 – Рівень віктимізації споживачів фінансових послуг (FX) та рівень довіри до фінансових послуг (FY) в Україні

Наступним кроком даного етапу виступає приведення інтегрального показника до проміжку значень від нуля до одиниці за допомогою наступної формули 3.12:

$$I_{jg} = \frac{F(\mu_{jg})}{F(\mu_{jg}) + S_j(F(\mu_{jg}))} \quad (3.12)$$

де I_{jg} – інтегральний показник Berger and Casella в розрізі j-го періоду для g-ої країн, приведений до проміжку значень від нуля до одиниці;

$F(\mu_{jg})$ – максимальне значення показника Berger and Casella для g-ої країни за весь розглянутий часовий інтервал;

$S_j(F(\mu_{jg}))$ – середнє квадратичне відхилення показника Berger and Casella для g-ої країни за весь розглянутий часовий інтервал.

Результати приведення значень інтегральних показників, які коливаються від 0 до 1 ум.од., наведено на рисунках 3.16-3.19.

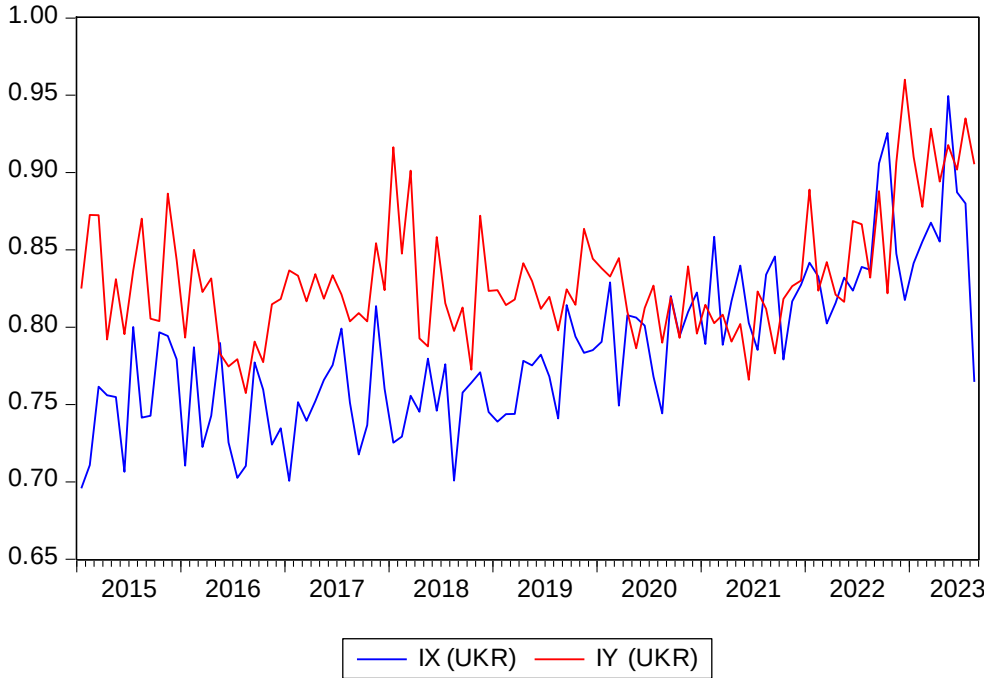


Рисунок 3.16 – Рівень віктимізації споживачів фінансових послуг (IX) та рівень довіри до фінансових послуг (IY) в Україні

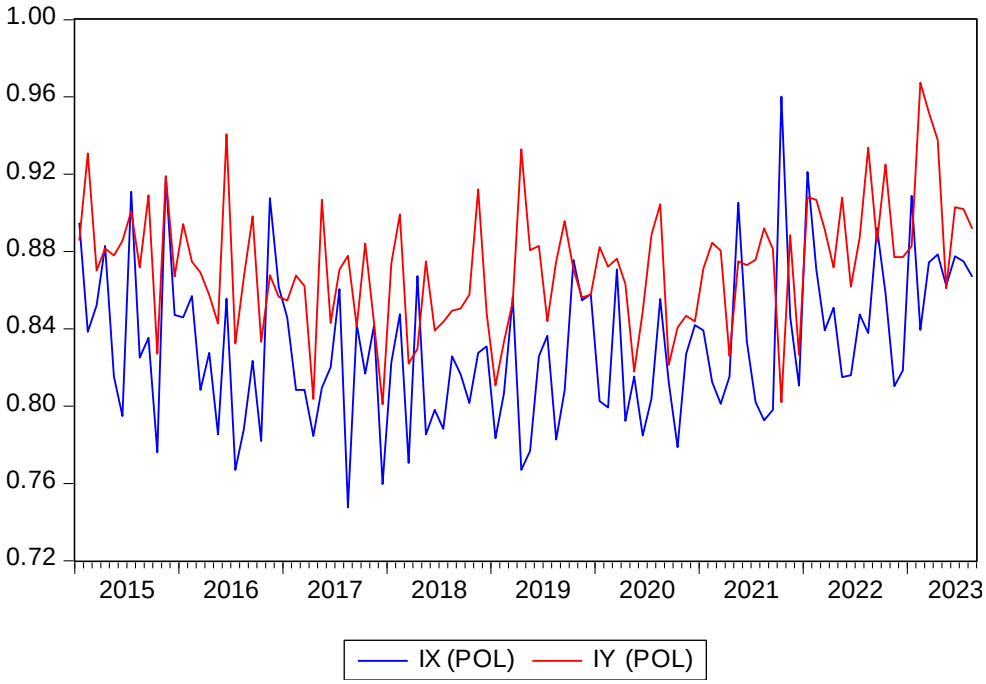


Рисунок 3.17 – Рівень віктимізації споживачів фінансових послуг (IX) та рівень довіри до фінансових послуг (IY) в Польщі

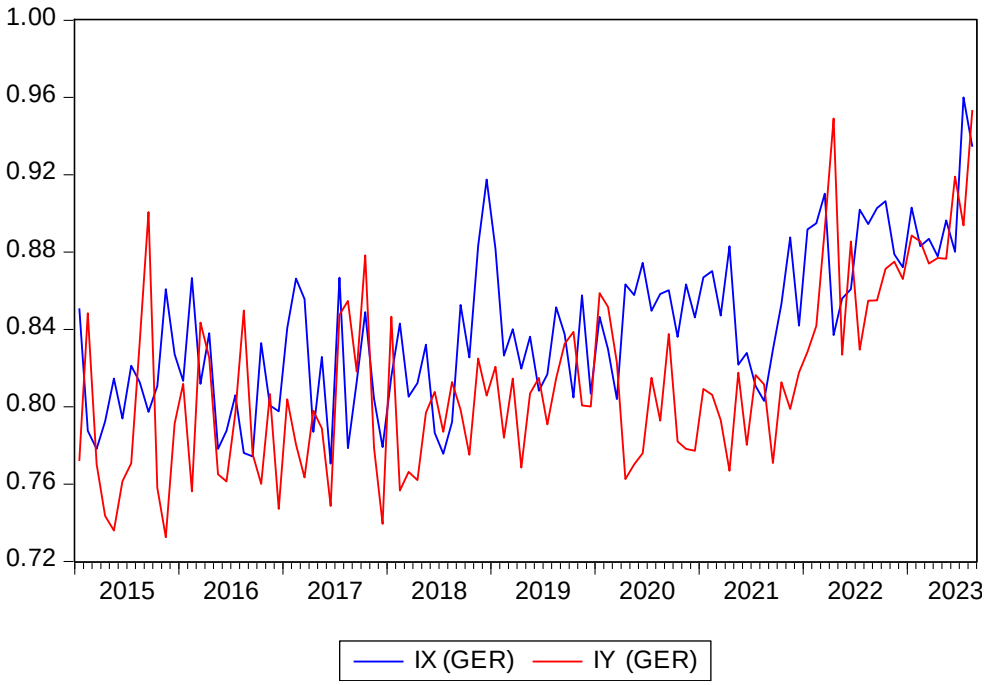


Рисунок 3.18 – Рівень віктимізації споживачів фінансових послуг (IX) та рівень довіри до фінансових послуг (IY) в Німеччині

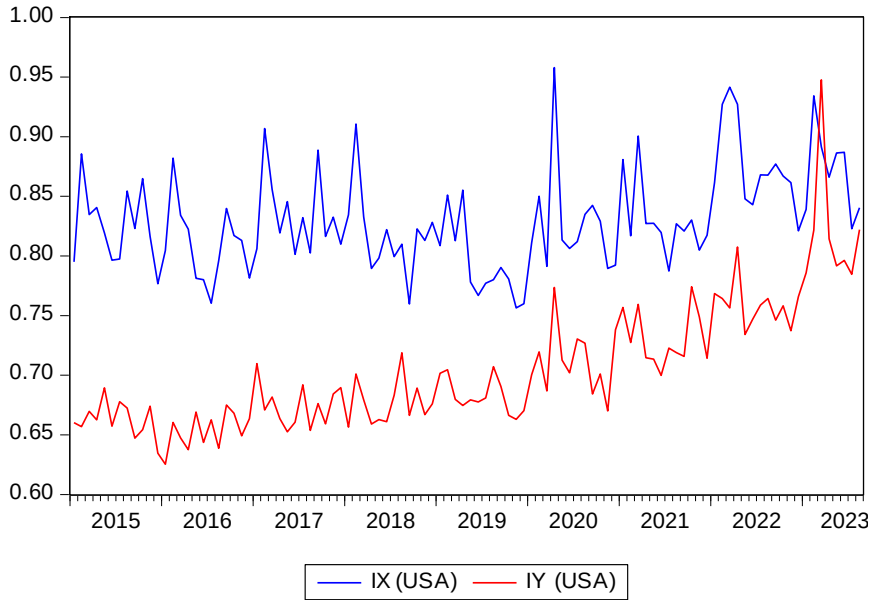


Рисунок 3.19 – Рівень віктимізації споживачів фінансових послуг (IX) та рівень довіри до фінансових послуг (IY) в США

Дані рисунків 3.16-3.19 демонструють, що середній рівень віктимізації споживачів фінансових послуг серед аналізованих країн становить 0,821 ум.од., при цьому найвище середньомісячне значення цього інтегрального показника зафіксовано для Німеччини (0,840 ум.од.), тоді як найнижче – для України (0,784 ум.од.). Стосовно другого інтегрального показника, то у середньомісячне значення показника рівня довіри населення до фінансових інститутів становить 0,805 ум.од (тоді як найвище значення з поміж чотирьох країн має Польща (0,872 ум.од), а найнижче – США (0,704 ум.од.)).

Для візуалізації сезонних коливань значень двох інтегральних показників у розрізі чотирьох країн побудовано графіки сезонності (рисунок 3.20). Аналіз сезонних коливань рівня віктимізації споживачів фінансових послуг дозволяє сформувати наступні висновки: у травні відбувається у середньому збільшення масштабів фінансових кібершахрайств в Україні, тоді як найменший обсяг кібершахрайств у середньому фіксується у серпні; найбільше середнє значення рівня віктимізації споживачів фінансових послуг у США зафіксовано у лютому, а найменше – у грудні; у Польщі та Німеччині розподіл фінансових кібершахрайств по місяцям є майже рівномірним.

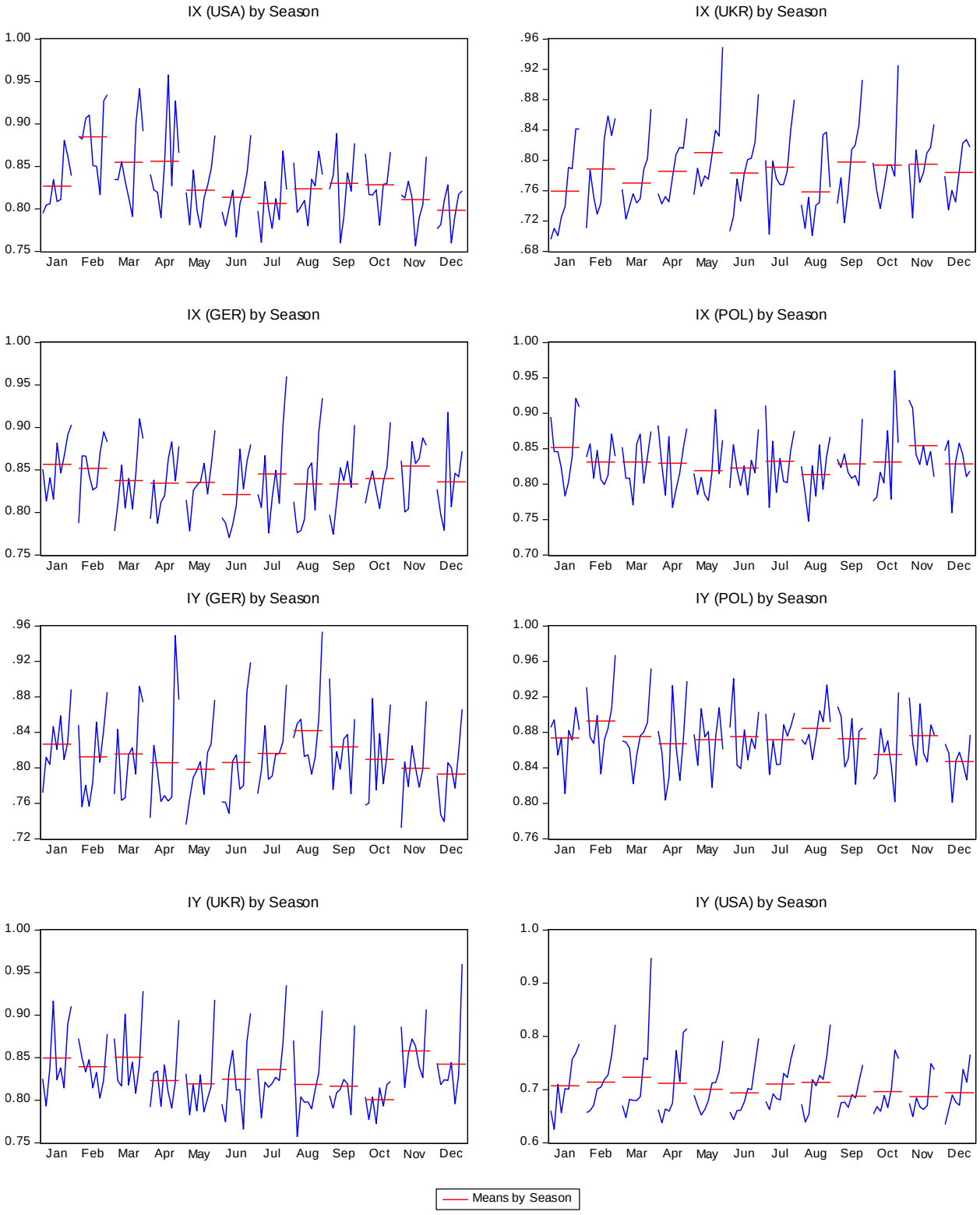


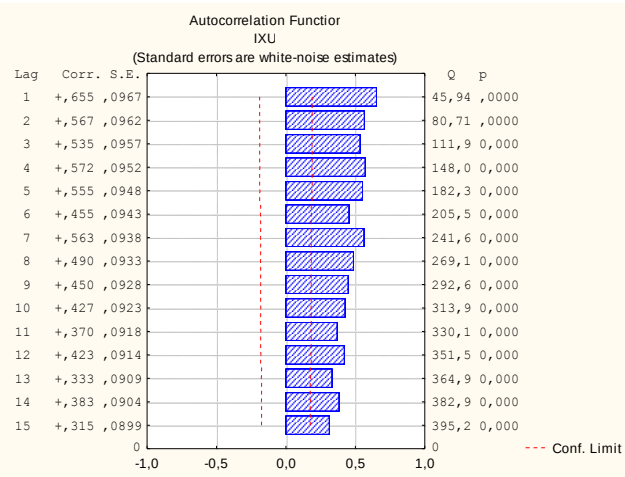
Рисунок 3.20 – Сезонність в динаміці рівня віктимізації споживачів фінансових послуг (IX) та довіри до фінансових послуг (IY)

Сезонна візуалізація інтегрального показника довіри до фінансових установ дозволяє стверджувати, що зниження цього показника в Україні щорічно в середньому відбувається в жовтні, тоді як збільшення – у січні,

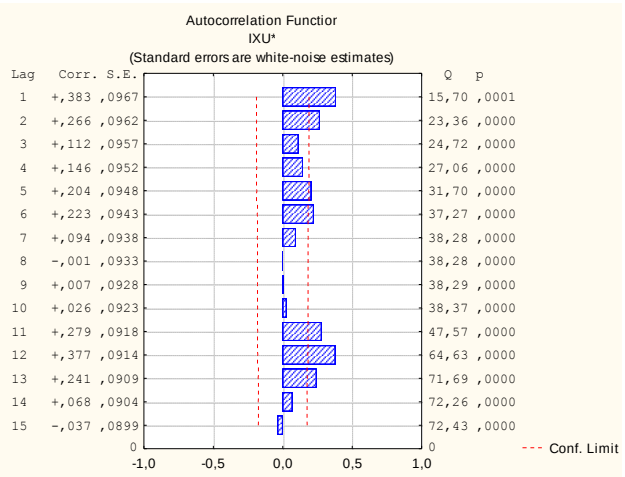
березні та листопаді. Середньомісячні значення рівня довіри до фінансових установ в США, Польщі та Німеччині є майже рівномірними.

Наступним етапом запропонованого науково-методтчного підходу є ідентифікація величини лагових затримок в розрізі розглянутих країн за допомогою автокореляційних функцій та корелограм. Проведення автокореляційного аналізу здійснено з використанням програми Statistica. Результати побудови корелограми, що відображає залежність рівня довіри до фінансового сектору від кібершахрайств з урахуванням часового лагу подано на рисунку 3.21.

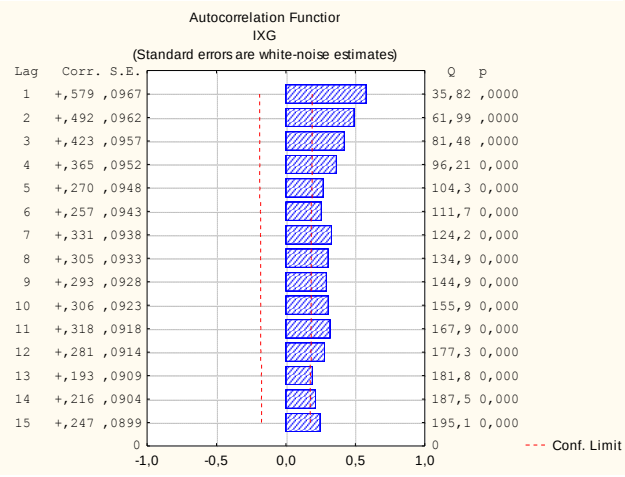
Україна



США



Німеччина



Польща

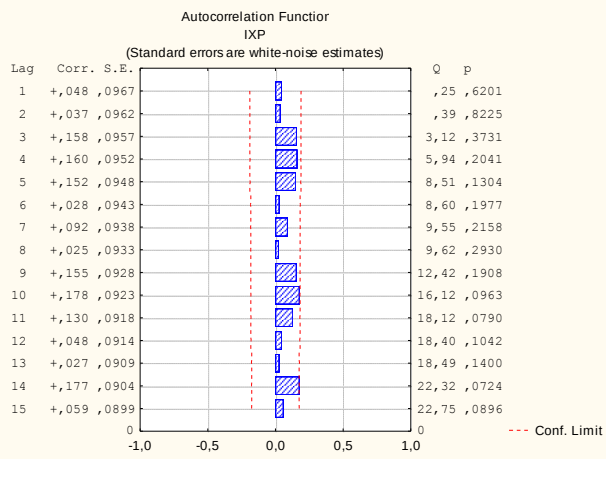


Рисунок 3.21 – Корелограма залежності рівня довіри до фінансового сектору від кібершахрайств з урахуванням часового лагу

Аналіз рисунку 3.21 дозволяє констатувати варіацію значень автокореляційної функції різних рівнів часового ряду в залежності від часового лагу та статистичну значущість для першого рівня. Так, в розрізі значень автокореляційної функції для України спостерігається тенденція зменшення з першого до третього рівня зі стрибкоподібним збільшенням значення автокореляційної функції четвертого рівня і подальшим поверненням до тенденції зменшення для 6 та 11 рівнів. Але найбільшим за абсолютним значення виступає коефіцієнт автокореляції 1 рівня. Даний факт свідчить про доцільність врахування лагових затримок впливу кібершахрайств на довіру до фінансового сектору для України на рівні 1 місяця. Аналіз автокореляційних функцій для інших країн дозволяє ідентифікувати наступні лагові затримки впливу кібершахрайств на рівень довіри до фінансових установ: США – 1 місяць, Німеччина – 1 місяць, Польща – 3 місяці.

Завершальним етапом науково-методичного підходу є оцінювання впливу фінансових кібершахрайств на рівень довіри до фінансового сектору шляхом побудови поліноміальної моделі розподіленого лагу Алмона. Даний інструментарій дозволяє побудувати регресійну модель з урахуванням лагових затримок значень одного часового ряду на основі іншого. Загальний вигляд моделі розподіленого лагу має наступний вигляд (формула 3.13):

$$y_t = b_0 \cdot x_t + b_1 \cdot x_{t-1} + b_2 \cdot x_{t-2} + \cdots + b_k \cdot x_{t-k} \qquad (3.13)$$

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 (формула 3.14):

$$b_k = a_0 + a_1 \cdot i + a_2 \cdot i^2 + \cdots + a_q \cdot i^q, q < k \quad (3.14)$$

де a_q – поліноміальні коефіцієнти регресійної моделі.

Результати розрахунку параменрів для поліноміальної моделі розподіленого лагу Алмона подано представлено у вигляді рисунку 3.22.

	Polyn. Distr. Lags; Regression Coefficients (Spreadsheet1.sta) Indep: IXU Dep: IYU Lag: 1 R= ,9984 R-square= ,9967 N: 103			
Lag	Regressn Coeff.	Standard Error	t(101)	p
0	0,5483379853	0,1156080764	4,7430768004	0,0000069319
1	0,5088948630	0,1156992535	4,3984282310	0,0000270545

Рисунок 3.22 - Фрагмент поліноміальної моделі розподіленого лагу Алмона в розрізі впливу фінансових кібершахрайств на рівень довіри до фінансових установ в розрізі України

Аналіз p-рівня дозволяє стверджувати про статистичну значущість в розрізі впливу фінансових кібершахрайств на довіру до фінансових установ лагу на рівні 0 і 1, оскільки відповідне значення ймовірності не перевищує 0,05. Відповідно, стандартна похибка без лагової затримки і з лагом 1 місяць є низькою, критерій Стьюдента статистичної значущості відповідного регресійного коефіцєнту моделі розподіленого лагу Алмона є прийнятним і перевищує критично допустимий рівень. Отже, на основі даних графи «Regressn Coeff» рисунку 3.22 закономірність впливу кібершахрайств на довіру до фінансових установ може бути формалізована у вигляді наступної моделі (формула 3.15):

$$FYUKR(t) = 0.5483 \cdot FX(t) + 0.5089 \cdot FX(t-1) \quad (3.15)$$

де $FYUKR(t)$ – інтегральний показник рівня довіри до фінансових установ в момент часу t в розрізі України;

$FX(t)$ – значення показника рівня кібершахрайств в момент часу t.

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

	Polyn. Distr. Lags; Regression Coefficients (Spreadsheet1.sta) Indep: IXU* Dep: IYU* Lag: 1 R= ,9982 R-square= ,9964 N: 103			
Lag	Regressn Coeff.	Standard Error	t(101)	p
0	0,5495293427	0,0909860100	6,0397125068	0,0000000258
1	0,2985143709	0,0910333514	3,2791758851	0,0014288457

Рисунок 3.23 - Фрагмент поліноміальної моделі розподіленого лагу Алмона в розрізі впливу фінансових кібершахрайств на рівень довіри до фінансових установ в розрізі США

Дані рисунку 3.23 наочно демонструють, що вплив віктимізації споживачів фінансових послуг на зміну довіри до фінансових установ є значимим на лагу на рівні 0 та 1, оскільки відповідне значення ймовірності не перевищує 0,05. Пропонується обрати в якості лагової затримки впливу 1 місяць. Формалізація взаємозв'язку між цими інтегральними показниками для США подана у вигляді наступної моделі (формула 3.16):

$$FYUSA(t) = 0.5495 \cdot FX(t) + 0.2985 \cdot FX(t-1) \qquad (3.16)$$

де $FYUSA(t)$ – інтегральний показник рівня довіри до фінансових установ в момент часу t в розрізі США;

$FX(t)$ – значення показника рівня кібершахрайств в момент часу t.

Зв'язок між рівнем віктимізації споживачів фінансових послуг та довірою до фінансового сектору є статистично значимим у розрізі лагів 0 та 1

(значення ймовірності не перевищує 0,05) (рисунок 3.24). Пропонується обрати в якості лагової затримки впливу 1 місяць.

	Polyn. Distr. Lags; Regression Coefficients (Spreadsheet1.sta) Indep: IXG Dep: IYG Lag: 1 R= ,9989 R-square= ,9978 N: 103			
Lag	Regressn Coeff.	Standard Error	t(101)	p
0	0,3243634763	0,1076344917	3,0135644349	0,0032641955
1	0,6439407815	0,1077450509	5,9765230595	0,0000000345

Рисунок 3.24 - Фрагмент поліноміальної моделі розподіленого лагу Алмона в розрізі впливу фінансових кібершахрайств на рівень довіри до фінансових установ в розрізі Німеччини

На основі значень параметрів поліноміальної моделі розподіленого лагу Алмона закономірність впливу кібершахрайств на рівень довіри до фінансових установ для Німеччини може бут формалізована у вигляді наступної моделі (формула 3.17):

$$FYGER(t) = 0.3244 \cdot FX(t) + 0.6439 \cdot FX(t-1) \qquad (3.17)$$

де $FYGER(t)$ – інтегральний показник рівня довіри до фінансових установ в момент часу t в розрізі Німеччини;

$FX(t)$ – значення показника рівня кібершахрайств в момент часу t.

	Polyn. Distr. Lags; Regression Coefficients (Spreadsheet1.sta) Indep: IXP Dep: IYP Lag: 3 R= ,9994 R-square= ,9987 N: 101			
Lag	Regressn Coeff.	Standard Error	t(97)	p
0	0,3259964659	0,0738698715	4,4131180856	0,0000264355
1	0,2701328844	0,0704177590	3,8361471305	0,0002224150
2	0,2071925751	0,0703101192	2,9468386243	0,0040207020
3	0,2467403543	0,0734745705	3,3581734806	0,0011222361

Рисунок 3.25 - Фрагмент поліноміальної моделі розподіленого лагу Алмона в розрізі впливу фінансових кібершахрайств на рівень довіри до фінансових установ в розрізі Польщі

Критерій Стьюдента та його p-значимість вказує на наявність статистично значимого впливу кібершахрайств на зміну довіри до фінансових установ на всіх лагах (0, 1, 2, 3). Пропонується обрати лагову затримку в обсязі 3 місяці. Модель з розподіленим лагом має наступний вигляд (формула 3.18):

$$FYPOL(t) = 0.3600 \cdot FX(t) + 0.2701 \cdot FX(t-1) + 0.2072 \cdot FX(t-2) + 0.2467 \cdot FX(t-3) \quad (3.18)$$

де $FYPOL(t)$ – інтегральний показник рівня довіри до фінансових установ в момент часу t в розрізі Польщі;

$FX(t)$ – значення показника рівня кібершахрайств в момент часу t.

Побудовані модель з розподіленим лагом (формули 3.15-3.18) мають високі показники якості, а саме коефіцієнт детермінації становить 0,99, а також порівняння залишкової дисперсії з дисперсією середнього арифметичного на основі значення критерію Фішера також вказує на адекватність побудованої моделі (p-value < 0,05).

Підсумовуючи, за результатами проведеного емпіричного дослідження встановлено, що висунуту гіпотезу доцільно прийняти, оскільки між віктимізацією споживачів фінансових послуг та довірою до фінансових установ у розрізі різних країн існує статистично значимий зв’язок з лаговою затримкою в основному в 1 місяць. Емпіричні розрахунки наочно демонструють посилення інформаційних заходів для споживачів фінансових послуг для підвищення рівня їх обізнаності у сфері особистої кібербезпекиз особливим акцентом на найбільш вразливу верству населення.

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

4.1 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 [106, 107].

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 4.1 представлено динаміку розвитку ринку криптовалют та DeFi за період з 3 кварталу 2020 року по 1 квартал 2022 року.

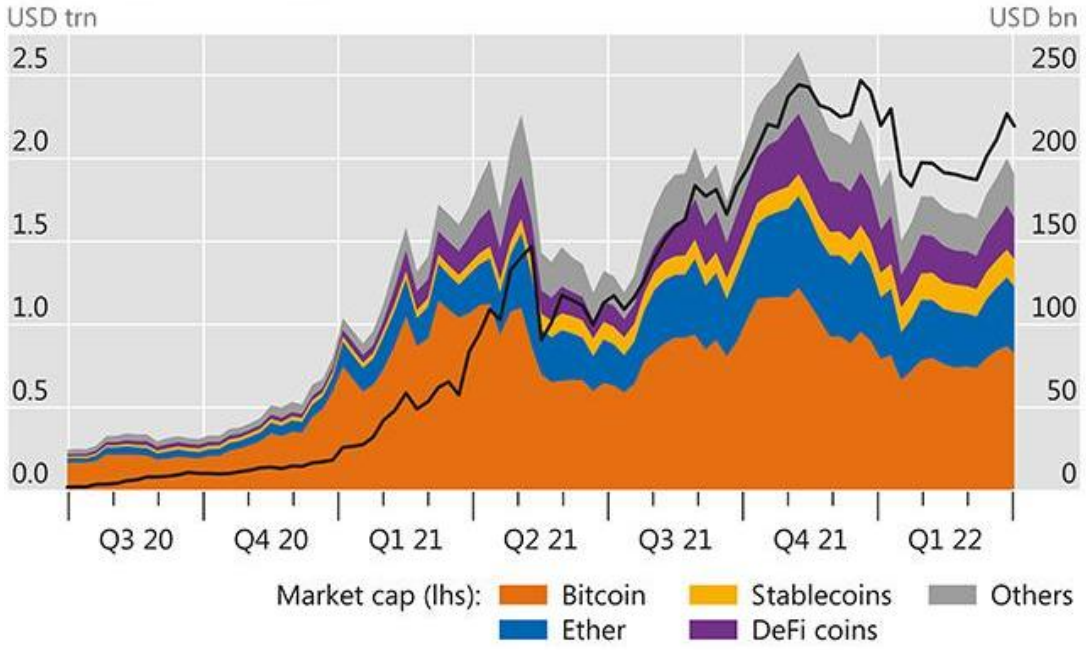


Рисунок 4.1 – Обсяг ринку криптовалют та DeFi у період 3 квартал 2020 – 1 квартал 2022

Джерело: Банк міжнародних розрахунків [108]

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 [109].

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 [110].

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. 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 [111]. Крім того, автори пропонують розширити класифікацію цифрових фінансових активів (рисунок 4.2).

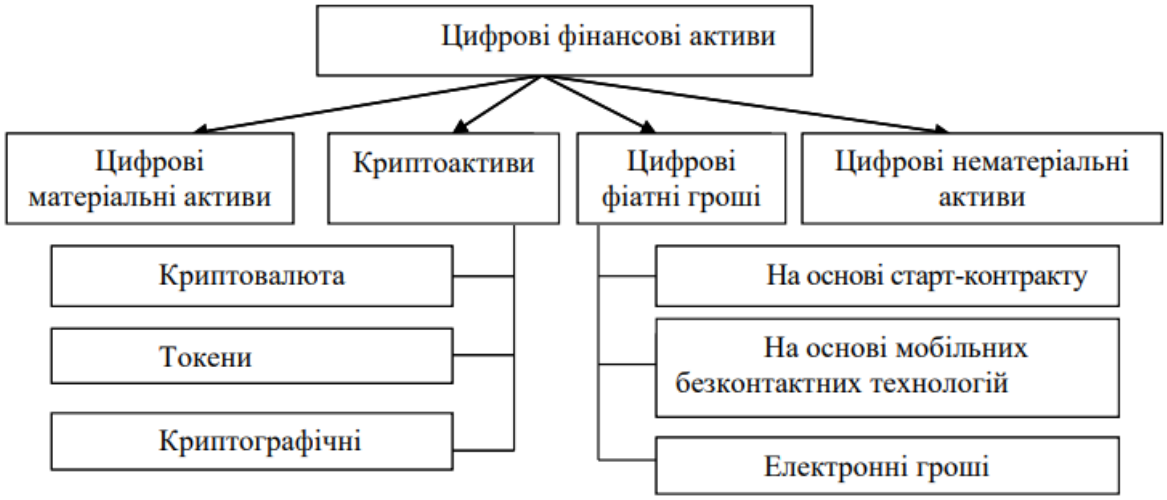


Рисунок 4.2 – Класифікація цифрових фінансових активів [111]

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», 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 [112]. 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 4.3 представлена систематизація сутності віртуальних активів у Франції, Великій Британії та на рівні Європарламенту.

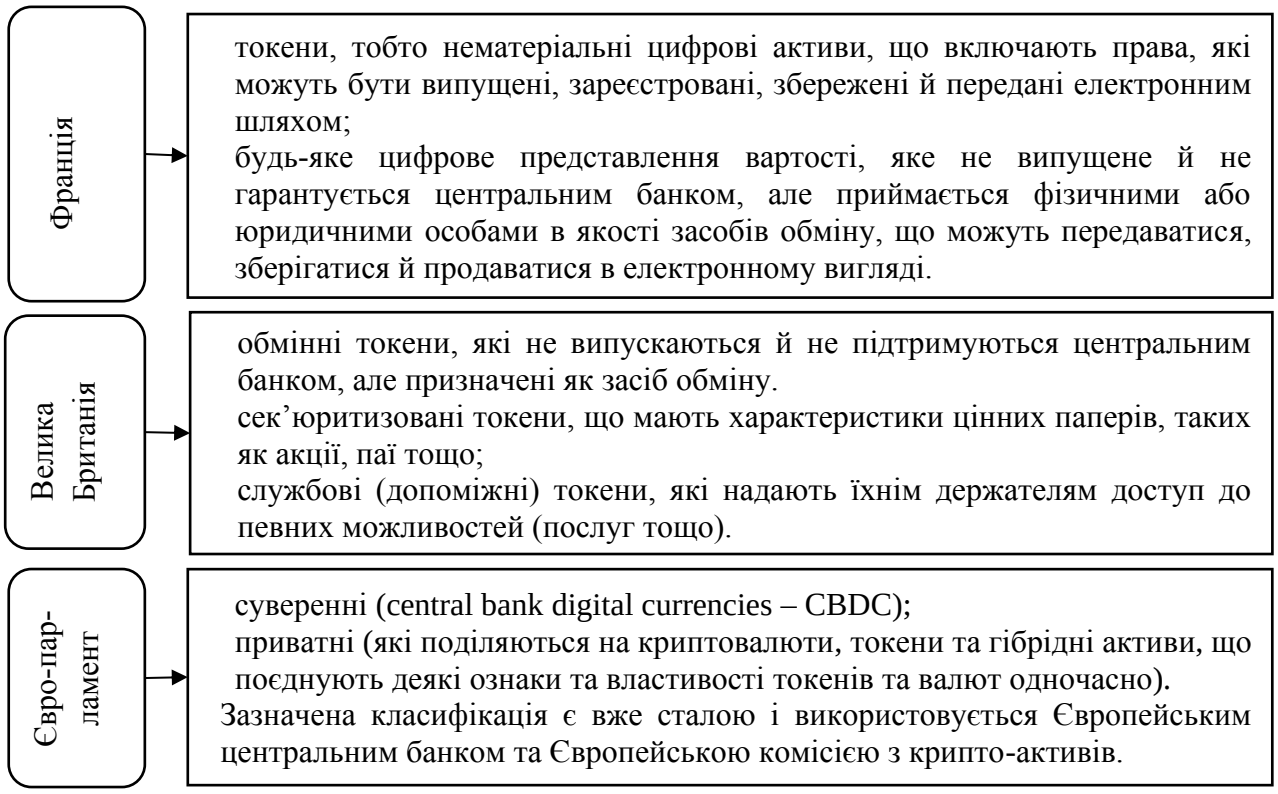


Рисунок 4.3 – Підходи до визначення цифрових активів за законодавством Франції, Великої Британії та Європарламентом [113]

За даними Міжнародного фінансового фонду, більше 100 країн активно розглядають шляхи створення цифрових валют центрального банку, а деякі вже почали їх використовувати (таблиця 4.1) [114]. 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 4.1 – Характеристика цифрових валют країн, де CBDC запущено, знаходяться в тестуванні або в розробці [114]

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 4.1

Назва валюти	Країна	Опис
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.

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 (рисунок 4.4). 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.

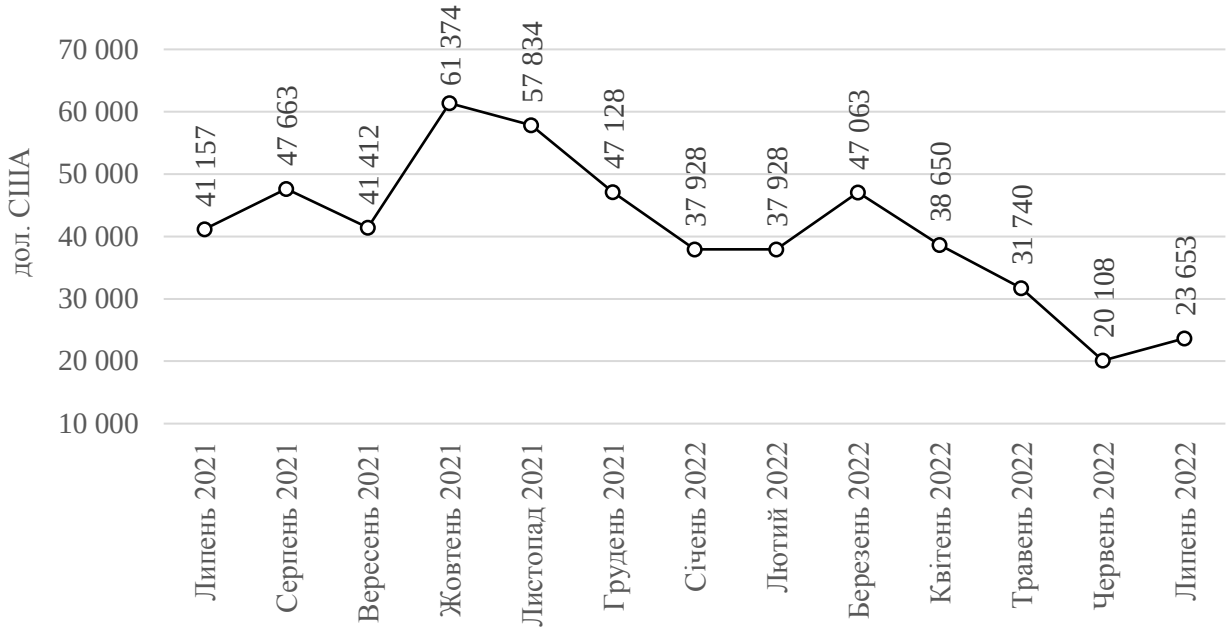


Рисунок 4.4 – Вартість Bitcoin протягом липня 2021 – липня 2022, дол. США [115]

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 [116].

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 [117].

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 (рисунок 4.5). Це становить приблизно 0,6 відсотка загального світового споживання електроенергії. Другою екологічною проблемою є електронні відходи, які стосуються електроніки, яку викидають наприкінці терміну служби.

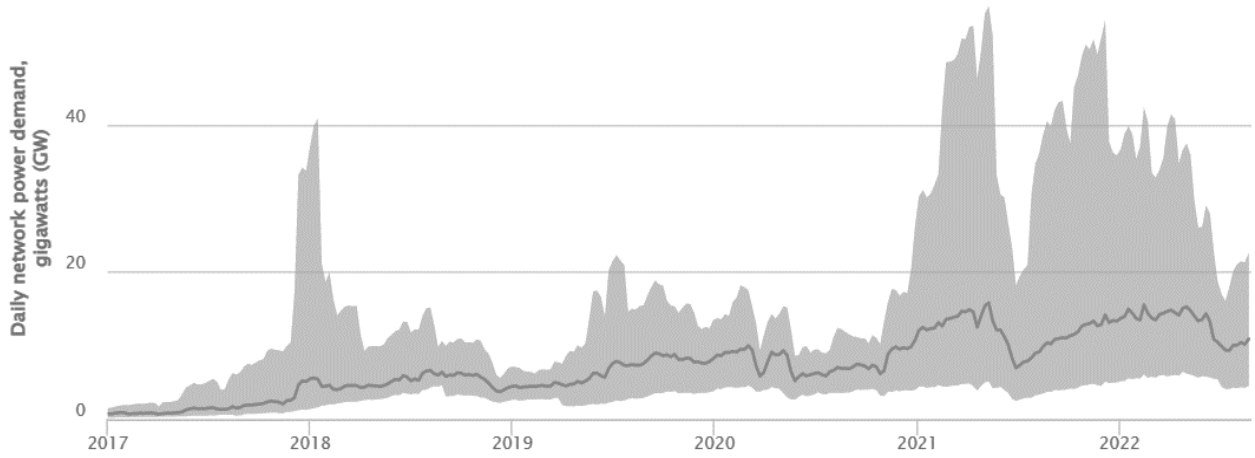


Рисунок 4.5 – Динаміка споживання електроенергії мережею Bitcoin у період 2017-2022 [118]

На думку Джага К. та Бача К. [119] 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 [120].

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.

4.2 Визначення закономірностей здійснення фінансових кібершахрайств з використанням криптовалюти

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. [121] опиує функції, вплив та проблеми криптовалюти у контексті фінансових технологій; Лю РХ.Ф., Рен Х., Лю С., Цзян Х. [122] охарактеризовують ключових агентів у криптовалютній економіці; Бейлі А. М., Реттлер Б., і Вармке К. [123] визначають філософію, політику та економік криптовалюти; Лопес-Мартін К., Беніто Муела С. і Аргедас Р [124] розкривають ефективність криптовалютних ринків; Хак І. У., Манінгам А., Чупрадіт С., Суксатан В. і Хуо К. [125] досліджують управління ризиками на ринку криптовалют; Махдаві-Дамгані Б., Фрейзер Р., Хауелл,Дж., і Халдорссон Дж.С. [126] 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. [127] 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. [128] щодо статусу криптовалюти в Марокко; Віджая Г. [129] стосовно ролі криптовалюти в Індонезійському центральному банку; Райлі Дж. [130] про сучасний стан регулювання криптовалюти в Китаї та його вплив у всьому світі; Уквуезе Ф. О. [131] щодо специфіки роботи з криптовалютою у Нігерії та Південній Африці; Дельва Бенавідес Дж. Е., і Торрес Амайя Ф. Е. [132] 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. [133] описують виявлення шахрайства криптовалютних операцій на базі використанням ринкових і соціальних сигналів; Тайхманн Ф. М. Дж., Фалькер М. [134] досліджують використання криптовалюти як засобу для фінансових злочинів; Хуанг С. [135] висвітлює зв'язок криптовалюти зі злочинністю; Колеснікова К., Мезенцева О., Мукатаєв Т. [136] аналізують транзакції з криптовалютою для виявлення незаконних операцій; Дюпюї Д. та Глісон К. [137] вивчають проблему відмивання грошей за допомогою криптовалюти; Троцце А., Кампс Дж., Акартуна Е.А., Хетцель Ф.Дж., Клейнберг Б., Девис Т., Джонсон С.Д. [138] досліджують зв'язок криптовалюти та майбутніх фінансових злочинів; Рен Б. і Люсі Б. [139] показують різницю між чистими та брудними криптовалютними ринками; Акартуна Е. А., Джонсон С. Д., і Торнтон А. [140] розкривають особливості запобігання ризикам відмивання грошей та фінансування тероризму через криптоактиви; Люсі Б. М., Вінь С. А., Яровая Л., і Ван Ю. [141] 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 криптооперації, 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 криптоваюти 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, 3D 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 4.1-4.4 [122]:

$$S_v = \frac{|(u,v)|(u,v)\in C_v^{size} and\ (v,u)\in C_v^{size}|}{|(u,v)|(u,v)\in C_v^{size} or\ (v,u)\in C_v^{size}|}, \quad (4.1)$$

Коефіцієнт кластеризації виражається формулою 4.2:

$$K_v = \frac{1}{\sum N_{inout}(v)(\sum N_{inout}(v)-1)-2\sum N^*_{inout}(v)}\text{T(v)}, \quad (4.2)$$

Щільність мережі транзакцій зображується формулою 4.3:

$$D_v^{size} = \frac{m}{n(n-1)}, \quad (4.3)$$

$$S_v^{size} = \frac{|(u,w)|(u,w)\in C_v^{size} and\ (w,u)\in C_v^{size}|}{m}, \quad (4.4)$$

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

V – вузли адрес блокчейна,

$C = \{(V_s, V_t, t), V_s, V_t \in V\}$ – 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.

– 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 4.5) та невизначеності криптовалютної політики (cryptocurrency policy uncertainty index – CrPolUI, формула 4.6) [141]:

$$CrPrUI = \frac{(Vpr_t - \mu pr)}{\delta pr} + 100 \quad (4.5)$$

де 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.

$$CrPolUI = \frac{(Vpol_t - \mu pol)}{\delta pol} + 100 \quad (4.6)$$

де $Vpol_t$ – 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 4.7:

$$\Delta y_t = \varepsilon \epsilon_{y_{t-1}} + \omega_1 \Delta y_{t-1} + \ldots + \omega_{p-1} \Delta y_{t-p+1} + \psi^+ d_t + \varphi_t \qquad (4.7)$$

де 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.

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 [56, 141]:

- 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 (формула 4.8) [143]:

$$supp(X \to Y) = P\ (X \cap Y) = \frac{n(\{X;Y\} \in d_i}{N} \tag{4.8}$$

- 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 (формула 4.9):

$$conf(X \to Y) = P\ (X|Y) = \frac{n1(\{X;Y\} \in d_i}{n1(\{X\} \in d_i} \tag{4.9}$$

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 використанням 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. 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 [144], тоді як фрагмент сформованої статистичної бази подано в таблиці 4.2 .

Таблиця 4.2 – 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 4.3.

Таблиця 4.3 – 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	75,9678	77,7212
-73745,232761<TES<=94068,968712, -73645,038405<TER<=96923,921976	==>	-0,070274<FRAUD<=0,124189	77,1872	77,7164
-39,576163<URFA<=100,277515, -73645,038405<TER<=96923,921976	==>	-0,070274<FRAUD<=0,124189	75,8764	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, -73745,2327<TES<=94068,968	77,1872	77,6608
-39,576163<URFA<=100,277515, -73645,038405<TER<=96923,921976	==>	-0,070274<FRAUD<=0,124189, -73745,2327<TES<=94068,9687	75,8053	77,6275
-73745,232761<TES<=94068,968712	==>	-0,070274<FRAUD<=0,124189, -73645,038<TER<=96923,9219	77,1872	77,5815
-39,576163<URFA<=100,277515, -73745,232761<TES<=94068,968712	==>	-0,070274<FRAUD<=0,124189, -73645,038<TER<=96923,921	75,8053	77,5548
-73645,038405<TER<=96923,921976	==>	-0,070274<FRAUD<=0,124189, -73745,2327<TES<=94068,9687	77,1872	77,6608
-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	74,5351	77,4142
-39,576163<URFA<=100,277515, -73645,038405<TER<=96923,921976, -35,997920<USTA<=87,555079	==>	-0,070274<FRAUD<=0,124189	74,4436	77,3928
-73745,232761<TES<=94068,968712, -35,997920<USTA<=87,555079	==>	-0,070274<FRAUD<=0,124189	75,3480	77,3524
-73645,038405<TER<=96923,921976, -35,997920<USTA<=87,555079	==>	-0,070274<FRAUD<=0,124189	75,2565	77,3311
-73745,232761<TES<=94068,968712, -73645,038405<TER<=96923,921976, -35,997920<USTA<=87,555079	==>	-0,070274<FRAUD<=0,124189	75,1854	77,3145
-574,848976<AVR<=776,291550, -73645,038405<TER<=96923,921976	==>	-0,070274<FRAUD<=0,124189	73,5697	76,9558

Продовження таблиці 4.3

Body	==>	Head	Support (%)	Confidence(%)
-39,576163<URFA<=100,277515, -574,848976<AVR<=776,291550, -73745,232761<TES<=94068,968712	==>	-0,070274<FRAUD<=0,124189	72,3402	76,9455
-574,848976<AVR<=776,291550, -73745,232761<TES<=94068,968712, -73645,038405<TER<=96923,921976	==>	-0,070274<FRAUD<=0,124189	73,5189	76,9435
-39,576163<URFA<=100,277515, -574,848976<AVR<=776,291550, -73645,038405<TER<=96923,921976	==>	-0,070274<FRAUD<=0,124189	72,2487	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	72,1979	76,9106
-11,224277<AVS<=100,744593, -73645,038405<TER<=96923,921976	==>	-0,070274<FRAUD<=0,124189	72,3300	76,7191
-39,576163<URFA<=100,277515, -574,848976<AVR<=776,291550, -35,997920<USTA<=87,555079	==>	-0,070274<FRAUD<=0,124189	71,3138	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 4.3, 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 4.6).

	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	9, -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<US	6,00000	6919,00	70,3079

Рисунок 4.6 – Частота виявлених випадків здійснення фінансових кібершахрайств з використанням Ефіріум

Аналіз рисунку 4.6 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%.

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 4.7).

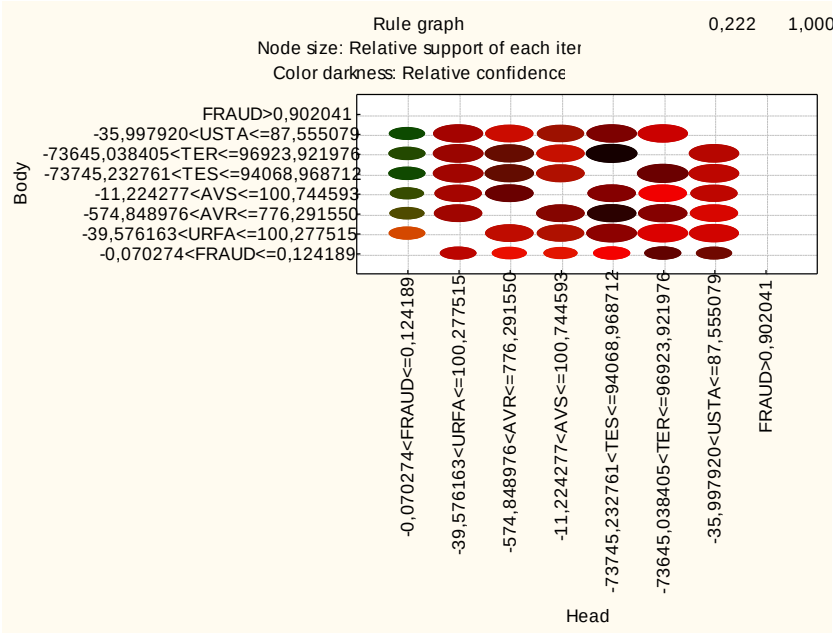


Рисунок 4.7 – Граф асоціативних правил

В рамках даного етапу побудовано граф виявлених на другому етапі асоціативних правил, представлений на рисунку 4.7, 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 4.8 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.

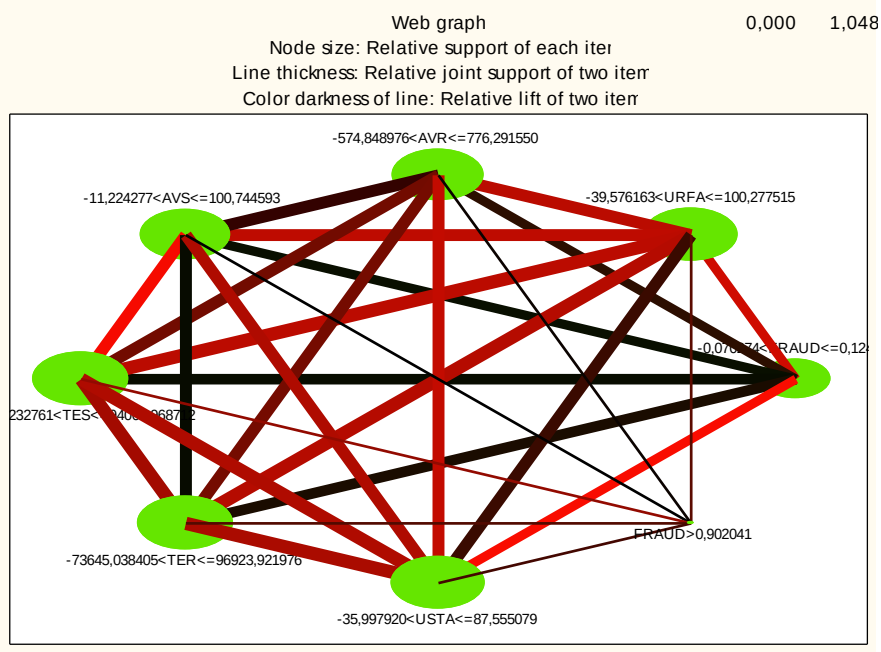


Рисунок 4.8 – Веб-граф підтримки виявлених асоціативних правил в розрізі здійснення фінансових кібершахрайств з використанням Ефіріум

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.

4.3 Оцінювання впливу використання криптовалют на кібербезпеку країни

Через збільшення кількості кібератак, підвищення хакерської активності та цифровізації суспільства, уряди більшості країн у співпраці з організаціями приватного сектору, академічними колами та фахівцями з кібербезпеки змушені вдаватися до зважених заходів підвищення кібербезпеки для захисту національної безпеки й розвитку інформаційного сектору. Варто зауважити, що впровадження урядових політик і стратегій спрямованих на підвищення кібербезпеки країни вимагає проведення ґрунтованого дослідження та

розуміння факторів, які впливають на поширення та активність цифрових загроз.

Одним з факторів, який може впливати на кібербезпеку є цифровізація суспільства. Поширення нових технологій, таких як штучний інтелект, інтернет речей, хмарні обчислення або криптовалюти, може створювати нові вектори атак кіберзлочинців, потенційні ризики для інформаційної безпеки, потребу розробки нових стандартизованих практик перевірки та протидії виявленим методам злочинності тощо. Наприклад, криптовалюти, через децентралізацію, слабке регулювання й конфіденційність блокчейн технології, можуть використовуватися кіберзлочинцями для відмивання грошей, платежів програм-вимагачів і фінансування злочинних дій. Крім того конфіденційність платежів може створити перепони для відстеження та розслідування кіберзлочинів правоохоронними органами. Більш повне розуміння впливу криптовалют на кібербезпеку може допомогти урядам у розробці ефективних програм для підвищення кібербезпеки та боротьби з цифровими атаками.

Проведений нами аналіз наукової літератури, дозволяє зробити висновок, що тема взаємозв’язку поширеності й використання криптовалют на кібербезпеку є актуально і користується увагою наукової спільноти. Проте розглянуті нами роботи зосереджувалися переважно на технічному та правовому аспектах поширеності та використання криптовалют в цифровій злочинності, в той час, як тема впливу окремих аспектів використання криптовалют на кібербезпеку країни лишається недостатньо дослідженою та потребує більшої уваги науковців.

Для проведення моделювання нами було зібрано набір даних, з 10 факторними змінними, які характеризують аспекти використання криптовалюти, і однією результатною змінною, яка демонструє рівень кібербезпеки країни. Набір даних зібраний щодо 24 країн Європейського Союзу у 2020 році.

Залежною ознакою нами було обрано загальну оцінку кібербезпеки країни відповідно до Глобального звіту про кіберзлочинність компанії SEON [145], оскільки вона оцінює за 100 бальною шкалою загальний рівень

кібербезпеки країни базуючись на таких аспектах, як Національний індекс кібербезпеки [146] (індекс, оцінюваний NCSI Project Team, який зосереджений на оцінці готовності країн запобігати кіберзагрозам за рівнем впровадження відповідних нормативно правових актів), Глобальний індекс кібербезпеки [147] (показник, створений ITU-D, відділом Міжнародного союзу електрозв'язку, він крім правових оцінює технічні, організаційні, кооперацийні заходи а також розвиток потенціалу країни у сфері кібербезпеки) і Індекс ризику кібербезпеки [148] (індекс оцінюваний компанією PasswordsManagers.co, який базується на рейтингах країн за кількістю виявлених випадків цифрових загроз різних видів). Таким чином, загальна оцінка кібербезпеки країни враховує найбільшу кількість аспектів кіберебезпеки країни починаючи від оцінки правового поля й закінчуючи кількістю виявлених кіберзлочинів, тому вона є репрезентативним показником загального рівня захищеності країни від цифрових загроз. Найвищі оцінки кібербезпеки за цим показником станом на 2020 рік мають такі країни Європейського Союзу, як Бельгія, Фінляндія й Іспанія (рис. 4.9).

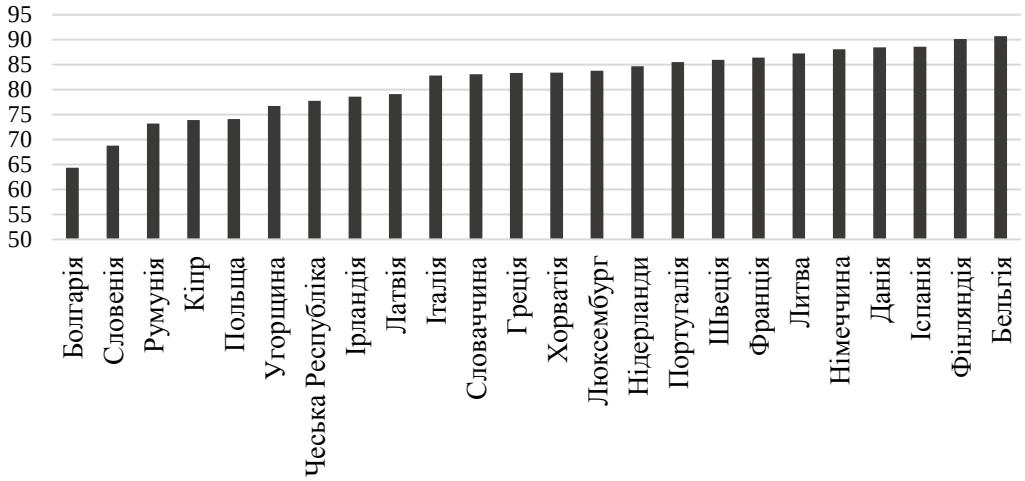


Рисунок 4.9 - Оцінка кібербезпеки (y_2) країн Європейського Союзу станом на 2020 рік

Список факторних змінних (наведений у таблиці 4.4), характеризує 5 аспектів використання криптовалют населенням країни, зокрема:

— поширеність володіння та використання криптовалют серед населення країни (змінні x_1, x_3, x_4, x_8): популярність криптовалютного ринку може привернути додаткову увагу кіберзлочинців до можливостей шахрайства й викрадення коштів користувачів, криптоджекінгу, використання криптовалют для відмівання коштів або спонсорування злочинної діяльності тощо;

— державне правове регулювання використання криптовалют (змінна x_6): ефективне регулювання криптовалютної діяльності урядами та регуляторними органами може сприяти ідентифікації користувачів на криптовалютних біржах, забезпеченню заходів безпеки, запобіганню відмиванню грошей і фінансуванню тероризму; усе це має позитивно вплинути на кібербезпеку країни;

— цифрова грамотність населення (змінні x_2 і x_7): цифрова грамотність населення може знизити ризики кіберзлочинності з використанням криптовалют, адже допомагає користувачам бути обізнаними про поширені методи кіберзлочинності (зокрема фішинг, шахрайство, джекінг та ін.), створювати більш надійні ключі захисту до криптовалютних гаманців, виявляти підозрілі дії інших користувачів, користуватися більш захищеними біржами та іншими платформами з криптовалютними транзакціями тощо;

— інвестиційна грамотність населення (змінні x_8 і x_9): інвестиційна грамотність населення може мати позитивний вплив на рівень кібербезпеки країни, оскільки вона свідчить про обізнаність населення щодо інвестиційного шахрайства, розуміння нестабільності ринку і необхідності захисту інвестиційних платформ, можливості оцінки інвестиційних ризиків та ін;

— поширеність в країні сфер злочинного використання криптовалют (x_5 і x_{10}): змінні цієї категорії характеризують обсяг ринку даркнету країни й обсяг її тіньової економіки, високий рівень обох змінних може негативно впливати на рівень кібербезпеки країни, оскільки оплата злочинних товарів і послуг за допомогою криптовалюти в даркнеті або поза державним обліком і контролем

(тіньова економіка) може вказувати на нерегульованість криптовалютного ринку й свідчити про наявність злочинних криптовалютних транзакцій.

Таблиця 4.4 – Факторні змінні, які характеризують аспекти використання криптовалют в країні

Показник		Джерело даних
x_1	відсоток населення, який має право власності на криптовалюти	Дані про право власності на криптовалюту. Криптовалюта в усьому світі. Triple-A.
x_2	відсоток осіб з базовими або вище загальними цифровими навичками	ESS: опитування ЄС щодо використання ІКТ у домогосподарствах та окремими особами. Євростат.
x_3	відсоток опитаних, який має або мав криптовалюти (інше джерело)	Flash Eurobarometer FL509: Роздрібні фінансові послуги та продукти
x_4	відсоток опитаних, який користується мобільним додатком для інвестування в криптоактиви раз на тиждень і частіше	
x_5	загальний дохід ринку даркнету (в євро на душу населення)	Криптовалюти та наркотики: аналіз використання криптовалюти на ринках даркнету в ЄС та сусідніх країнах. Довідковий документ на замовлення EMCDDA
x_6	оцінка правових заходів у сфері регулювання цифрових активів (за 20-бальною шкалою)	Глобальний індекс кібербезпеки 2020. Вимірювання відданості кібербезпеці. Сектор розвитку Міжнародного союзу електрозв'язку
x_7	відсоток осіб, який користувалися Інтернетом протягом останніх 3 місяців	Використання ІКТ у домогосподарствах та окремими особами. Євростат
x_8	відсоток населення, який інвестує в криптовалюту	Flash Eurobarometer FL509: Роздрібні фінансові послуги та продукти
x_9	відсоток населення, який інвестує в традиційні активи	
x_{10}	розмір тіньової економіки за 2020 році (у % офіційного ВВП)	Оподаткування неформальної економіки в ЄС. Дослідження на запит комітету FISC

Джерело: авторська розробка на основі [147, 149, 150, 151, 152, 153, 153]

Таким чином нами було створено набір даних для подальшої побудови регресійної моделі з метою оцінки впливу аспектів використання криптовалют на оцінку кібербезпеки країн Європейського Союзу (таблиця 4.5).

Під час дослідження нами були використані такі загальнонаукові методи, як аналіз, синтез, абстракція, аналогія та узагальнення. Основним методом моделювання є використання багатофакторної регресії. Цей метод був обраний, оскільки він є простим та гнучким у вивченні впливу множини факторів на результатну змінну, а також дозволяє оцінити відносну важливість

різних незалежних змінних у поясненні варіації залежної змінної і провести економічну інтерпретацію виявлених зв’язків.

Таблиця 4.5 - Набір даних для побудови регресійної моделі

Країна	y	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	x_9	x_{10}
Бельгія	90,7	1,4	54,2	6,5	4,3	260,9	20,0	81,1	6,0	32,0	16,2
Болгарія	64,4	2,2	31,2	13,1	10,8	328,9	17,3	19,8	13,0	13,0	32,9
Греція	83,4	1,5	52,5	10,0	8,0	110,8	19,4	54,0	10,0	11,0	20,9
Данія	88,4	1,2	68,7	7,6	6,4	244,0	19,3	95,7	8,0	36,0	9,8
Ірландія	78,6	1,1	70,5	10,9	6,7	310,4	20,0	77,7	11,0	21,0	9,9
Іспанія	88,6	3,0	64,2	7,8	7,7	154,6	20,0	69,4	8,0	27,0	17,4
Італія	82,8	2,4	45,6	5,7	7,7	79,1	19,7	55,3	6,0	31,0	20,4
Кіпр	73,9	1,2	50,2	13,1	9,9	386,0	20,0	71,3	13,0	10,0	24,3
Латвія	79,1	1,3	50,8	8,1	5,8	830,3	20,0	87,9	8,0	11,0	20,9
Литва	87,3	1,2	48,8	11,1	5,9	441,5	20,0	83,3	11,0	14,0	23,1
Люксембург	83,8	1,0	63,8	13,9	8,0	778,0	20,0	72,7	14,0	36,0	8,6
Нідерланди	84,7	2,7	78,9	11,6	8,5	454,7	20,0	96,0	12,0	19,0	8,1
Німеччина	88,1	4,2	48,9	6,4	9,4	174,4	20,0	55,1	6,0	33,0	10,4
Польща	74,1	2,8	42,9	8,1	9,2	171,6	19,4	61,2	8,0	14,0	22,5
Португалія	85,5	2,6	55,3	12,1	9,7	201,3	20,0	64,2	12,0	23,0	17
Румунія	73,2	1,6	27,8	8,2	9,4	127,0	18,6	18,5	8,0	12,0	29,3
Словаччина	83,1	1,4	55,2	12,2	8,3	347,4	20,0	65,1	12,0	25,0	14
Словенія	68,8	1,1	49,7	17,5	12,3	633,5	20,0	64,2	18,0	22,0	23,1
Угорщина	76,7	1,3	49,1	8,3	3,7	137,5	18,2	63,2	8,0	19,0	26
Фінляндія	90,2	1,4	79,2	9,1	7,5	494,3	20,0	96,4	9,0	42,0	11,4
Франція	86,4	5,9	62,0	4,7	5,7	156,1	20,0	78,2	5,0	22,0	13,6
Хорватія	83,4	1,2	63,4	16,1	10,7	206,5	20,0	68,4	16,0	17,0	29,6
Чеська Республіка	77,7	1,9	59,7	12,0	8,6	367,3	18,9	81,9	12,0	24,0	14,2
Швеція	86,0	1,6	66,5	9,9	5,0	516,0	20,0	86,3	10,0	60,0	11,7

Джерело: авторська розробка

Не зважаючи не переваги та можливості, які відкривають криптовалюти перед інвесторами та іншими користувачами, їх поширення також викликає занепокоєння, зокрема з приводу потенційного впливу криптовалют на кіберзлочинність. По-перше, через децентралізацію, низький рівень державного регулювання, труднощі ідентифікації учасників транзакцій, доступність, безвідкличність та низьку вартість переказів, криптовалюти є привабливим інструментом для кіберзлочинців. По-друге, короткий історичний досвід цих систем і відносна новизна механізмів, які забезпечують їх роботу, також можуть викликати питання щодо ризиків і надійності цих

фінансових активів. Через це, не дивно, що обсяги криптовалюти задіяної в злочинній діяльності продовжують зростати. Наприклад, за даними дослідження Chainalysis Inc [154], у 2022 році вартість криптовалюти, отримання якої було пов’язано з злочинністю, досягла рекордного значення 20,6 мільярдів доларів США (рисунок 4.10). Криптовалюти часто стають інструментом у таких цифрових злочинах, як незаконна цифрова комерція (переважно у Даркнеті), відмивання грошей, хакерство, криптоджекінг і шахрайство тощо, при цьому впровадження криптовалют продовжує зростати, тому розуміння складного зв’язку між їх використанням і кіберзагрозами стає першочерговим для забезпечення надійних заходів цифрової безпеки.

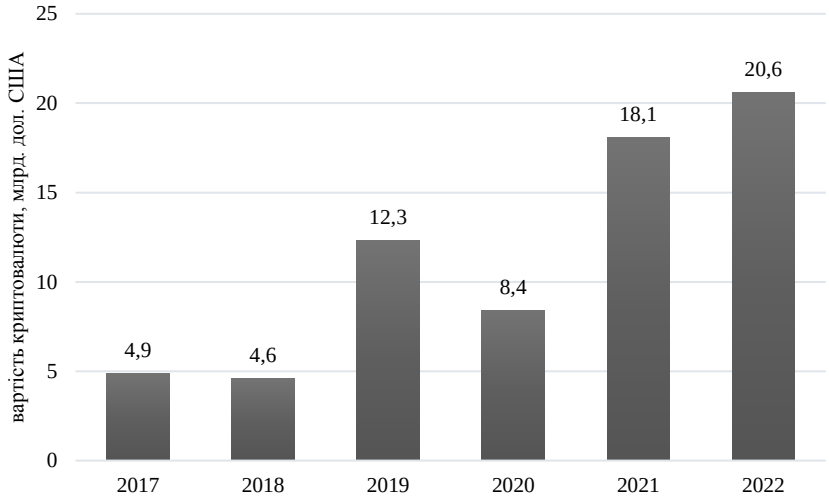


Рисунок 4.10 – Вартість криптовалюти, отриманої незаконними акаунтами 2017-2022 років

Країни Європейського Союзу відомі своїми прихильністю до інновацій, цифрової трансформації та захисту даних, тому ми обрали їх у якості середовища для вивчення впливу окремих аспектів використання криптовалют на кібербезпеку держави. З цією метою нами була побудована множинна лінійна регресійна модель з покроковим виключенням змінних. Результати покрокового виключення змінних показано на рисунку 4.11.

variable	Results of stepwise regression						
	step	R	R-square	R-square. corrected	F - incl/excl	p-value	number of
X10	-1	0,88	0,78	-0,00	0,01	0,94	7
X1	-2	0,88	0,78	-0,00	0,05	0,83	6
X3	-3	0,88	0,77	-0,01	0,64	0,43	5
X2	-4	0,86	0,75	-0,03	2,10	0,16	4
X9	-5	0,82	0,68	-0,07	5,28	0,03	3
X5	-6	0,77	0,60	-0,08	4,70	0,04	2

Рисунок 4.11 - Результати створення регресійної моделі з покроковим виключенням змінних

З рисунку 4.11 очевидно, що модель стає статистично значущою після четвертого кроку й виключення змінних x_{10}, x_1, x_3 і x_2. У результаті отримуємо модель з чотирма факторними змінними x_4 (відсоток населення, який користується мобільним додатком для інвестування в криптоактиви раз на тиждень і частіше), x_5 (загальний дохід ринку даркнету), x_6 (оцінка правових заходів у сфері регулювання цифрових активів) і x_9 (інвестування населення в традиційні активи). Така модель включає у себе змінні, які описують 4 різні аспекти використання криптовалют населенням країни й є статистично значущою за F-критерієм Фішера, тому є цікавою для подальшого розгляду. Детальніше результати отриманої моделі з чотирма факторними ознаками показані на рисунку 4.12.

N=24	Regression Outcomes R= ,86380253 R2= ,74615481 Correct. R2= ,69271372 F(4,19)=13,962 p<,00002 Standard estimation error: 3,8483					
	BETA	St. r. BETA	B	St. r. B	t(19)	p-value
intercept			-24,08	23,75	-1,01	0,32
X4	-0,37	0,12	-1,18	0,40	-2,98	0,01
X5	-0,32	0,12	-0,01	0,00	-2,61	0,02
X6	0,59	0,13	5,83	1,23	4,73	0,00
X9	0,30	0,13	0,17	0,08	2,30	0,03

Рисунок 4.12 - Отримана регресійна модель з 4 факторними змінними

Множинний коефіцієнт кореляції (R) регресійної моделі рівний 0,86, що перевищує критичне значення 0,7, тобто вказує на сильний зв'язок між результатною та факторними ознаками. Множинний коефіцієнт детермінації

доводить, що розподіл оцінки кібербезпеки серед країн Європейського Союзу у 2020 році на 74,62% пояснюється варіацією факторних змінних.

Для створеної моделі F-критерій Фішера рівний 13,96, що з рівнем значущості $p < 0,05$ підтверджує статистичну значущість рівняння регресії, це означає, що з імовірністю 95% отриманий результат може бути поширений на генеральну сукупність. Аналогічний висновок можемо зробити щодо статистичної значущості незалежних змінних, оскільки їх фактичні значення t-критерію Стьюдента також мають рівень значущості $p < 0,05$, тобто усі змінні включені в модель є статистично значущими за t-критерієм Стьюдента.

Необхідно також провести перевірку масиву пояснюючих змінних на мультиколінеарність, оскільки її наявність може спричинити зниження точності та інтерпретованості результатів подальшого моделювання. У якості критерію наявності колінеарності між факторними змінними було використано фактор інфляції дисперсії (variance inflation factor або VIF), оскільки він дозволяє кількісно оцінити завищення дисперсії оцінок параметрів регресії через наявність мультиколінеарності. За результатами перевірки (таблиця 4.6), очевидно, що значення VIF для жодної зі змінних не перевищує 5 (загальноприйнятого критичного значення), тому можна зробити висновок, що серед набору факторних змінних відсутня мультиколінеарність.

Таблиця 4.6 - Перевірка на мультиколінеарність за допомогою фактору інфляції дисперсії (VIF)

Змінна	VIF
x_4	1,13
x_5	1,10
x_6	1,17
x_9	1,24

На рисунку 4.13 також можемо побачити оцінки параметрів рівняння отриманої моделі.

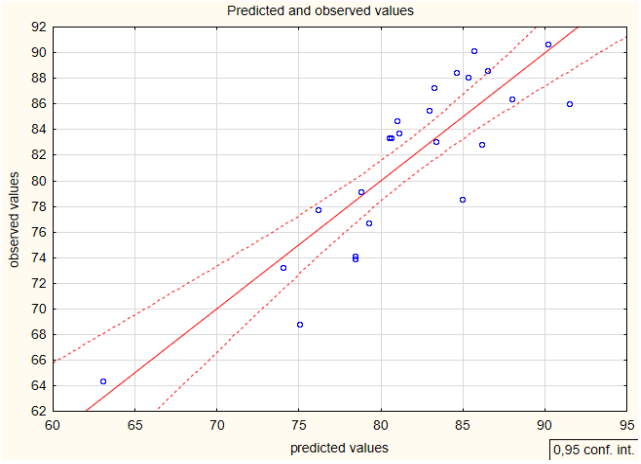


Рисунок 4.13 - Графік залежності між фактичними та прогнозами регресійної моделі

Виходячи з їхнього значення, можемо записати вигляд рівняння регресії (формула 4.10):

$$Y_2 = -24{,}08 - 1{,}18x_4 - 0{,}01x_5 + 5{,}83x_6 + 0{,}17x_9 \qquad (4.10)$$

де y_2– загальна оцінку кібербезпеки країни, шкала від 0 до 100 балів (де 0 – мінімальна оцінка, а 100 – максимальна);

x_4– відсоток населення, який користується мобільним додатком для інвестування в криптоактиви раз на тиждень і частіше;

x_5– загальний дохід ринку даркнету, євро на душу населення;

x_6– оцінка правових заходів у сфері регулювання цифрових активів, за 20-бальною шкалою (де 0 – мінімальна оцінка, а 20 – максимальна);

x_9– відсоток населення, який інвестує в традиційні активи.

За цим рівнянням (4.10) можемо визначити прогнозовані за регресійною моделюю значення результатної ознаки та порівняти їх з фактично визначеним значенням загальних оцінок кібербезпеки країн. За рис. 7 очевидно, що між цими значеннями існує позитивна кореляція, адже точки на графіку згруповані навколо діагональної лінії від нижнього лівого кута до верхнього правого кута. Це вказує на те, що регресійна модель працює добре та фіксує зв’язок між

предикторами та результатною ознакою. Близькість точок до діагональної лінії також свідчить про те, що прогнози моделі є близькими до фактичних значень оцінок кібербезпеки країн.

За оцінками параметрів регресії можемо висунути гіпотезу, що підвищення відсотка населення, який активно користується криптовалютами (x_4 – відсоток людей, які користуються мобільним додатком для інвестування в криптоактиви раз на тиждень і частіше) на 1% у середньому може призвести до зниження оцінки кібербезпеки на 1,18. Це можна пояснити тим, що децентралізований характер і анонімність криптовалют роблять їх привабливими інструментами для кіберзлочинців. Правоохоронним органам важко відстежувати транзакції з криптовалютою, що також полегшує злочинцям здійснення незаконних транзакцій. При цьому впровадження надійних заходів безпеки та зростання обізнаності населення щодо безпечного використання цифрових активів можуть не встигати за швидким зростанням кількості користувачів криптовалюти. Такі процеси здатні привернути увагу хакерів, спонукати їх до використання криптовалют у кількох напрямках, зокрема, як інструмент для:

— атак програм-вимагачів (злочинці шифрують дані жертв і вимагають викуп у криптовалюті за надання ключа дешифрування тощо);

— криптоджекінгу (кіберзлочинці використовують комп’ютерні ресурси жертв для майнінгу криптовалют без їх відома чи згоди, при цьому генеруючи нові цифрові активи за рахунок продуктивності системи жертви та споживання електроенергії);

— шахрайства, зокрема фішингу (кіберзлочинці видають себе за законні криптовалютні біржі, гаманці або початкові пропозиції монет (ICO), щоб обманом змусити користувачів розкрити їхні закриті ключі, паролі або надіслати кошти на шахрайські адреси);

— незаконної торгівлі у даркнеті (криптовалюти є поширеним способом оплати в торгівлі викраденими даними, хакерськими інструментами та іншими незаконними товарами у даркнет);

— відмивання грошей (злочинці можуть конвертувати свої незаконно отримані прибутки в криптовалюти, а потім назад у традиційні валюти різними способами, що ускладнює відстеження походження коштів).

З іншого боку варто зазначити, що, хоча в короткостроковій перспективі криптовалюти надали нові можливості для кіберзлочинців, вони за своєю суттю не пов’язані з кіберзлочинністю. Багато законних компаній і осіб використовують криптовалюти в законних цілях, а сама технологія має потенціал для підвищення безпеки та конфіденційності в різних сферах. Таким чином, вплив поширеності криптовалют на оцінку кібербезпеки в довгостроковому періоді є менш однозначним.

Меншою мірою на рівень оцінки кібербезпеки негативно впливає підвищення популярності використання даркнету (x_5 – загальний дохід ринку даркнету). За оцінкою параметра регресії, можемо припускати, що підвищення доходу ринку даркнету на 1 євро на душу населення у середньому може спричинити зниження оцінки кібербезпеки на 0,01. Такий вплив може бути спричинений тим, що ринок даркнету є одним з джерел фінансування для кіберзлочинців і використовуватися для продажу викрадених даних, адже використання криптовалют дозволяє покупцям і продавцям здійснювати транзакції, не розкриваючи свою особистість або місцезнаходження. Через це криптовалюти є основним способом оплати електронних транзакцій у Dark Web. Таким чином, хоча криптовалюти можуть приносити користь у різних галузях, однак їх анонімність та децентралізація роблять крипртовалюти привабливими для кіберзлочинців, які прагнуть здійснювати незаконну діяльність, зберігаючи певний ступінь анонімності.

Заходами, які пом’якшують негативний вплив поширення криптовалют на кібербезпеку можуть бути розвиток цифрової та інвестиційної грамотності користувачів, підвищення обізнаності про ризики, пов’язані з криптовалютами та кіберзлочинністю, розробка профільного законодавства й контроль за надійністю протоколів безпеки криптовалютних бірж, запровадження правил і стандартів для забезпечення захисту коштів і особистої інформації

користувачів, міжнародна співпраця, розробка та вдосконалення інструментів аналізу блокчейну тощо.

Значний позитивний ефект на оцінку кібербезпеки країни має підвищення оцінки правових заходів у сфері регулювання цифрових активів (x_6). За оцінкою відповідного параметра регресії, зростання оцінки правових заходів у сфері регулювання цифрових активів на 1 у середньому може призвести до підвищення оцінки кібербезпеки на 5,83. Це легко пояснити, адже правове регулювання криптовалют може сприяти прозорості, дотриманню стандартів ідентифікації користувачів і боротьби з відмиванням грошей, міжнародній співпраці та обміну інформацією тощо.

Однак варто зауважити, що, хоча правове регулювання криптовалют може позитивно впливати на кібербезпеку у ньому варто дотримуватися балансу між регуляцією та інноваціями, адже надмірні та обтяжливі правила можуть стримувати технологічний прогрес і перешкоджати законному використанню криптовалют. Частково визначити цей баланс можна опираючись на урядові практики на прикладі країн Європейського Союзу з високими оцінками правових заходів у сфері регулювання цифрових активів (x_6). Наразі провідна політика регулювання цифрових активів у Європейському Союзі здійснюється відповідно до Повідомлення Комісії до Європейського Парламенту, Ради, Європейського Економічного та Соціального Комітету та Комітету Регіонів щодо стратегії цифрових фінансів для ЄС [153]. Згідно з цим документом основними цілями регулювання цифрових активів є:

— забезпечення правової визначеності;

— підтримка інновацій та усунення регуляторних перешкод, які можуть стримувати розвиток фінансових технологій, одночасно зі зменшенням ризиків, що виникають у зв’язку з цим;

— захист європейських користувачів, інвесторів і бізнесу, шляхом створення довіри та впевненості в цілісності ринку;

— підтримка фінансової стабільності на європейському рівні.

Таким чином, можемо ствердити, що впровадження ефективного правового регулювання цифрових активів спрямованого на перераховані цілі може сприяти значному підвищенню оцінки кібербезпеки країни.

Деякий позитивний вплив на оцінку кібербезпеки має також підвищення інвестиційної грамотності населення, яке представлене змінною x_9 (відсоток населення, що інвестує в традиційні активи). Підвищення цього показника на 1% у середньому може призвести до підвищення оцінки кібербезпеки на 0,17. Причиною цього може бути те, що підвищення інвестиційної грамотності надає людям знання та навички для прийняття обґрунтованих фінансових рішень, розпізнавання потенційних кіберзагроз і вживання профілактичних заходів для захисту своїх інвестицій та особистої інформації.

Зрозуміло, що запровадження та реалізація згаданих заходів запобігання та протидії злочинному використанню криптовалют вимагають активних дій від багатьох зацікавлених сторін, зокрема криптовалютних бірж, урядів, регуляторних органів і окремих осіб для спільного вирішення проблем і пом’якшення негативного впливу криптовалют на кібербезпеку. Розробка і реалізація заходів безпеки пов’язаних з використанням криптовалюти можуть потребувати значних зусиль, проте вони здатні значно зменшити негативний вплив криптовалют на кібербезпеку.

Отже, за результатами моделювання, збільшення кількості користувачів, які користуються мобільним додатком для інвестування в криптоактиви раз на тиждень і частіше, є значним фактором підвищення ризиків кібербезпеки. З огляду на зростання популярності та вживаності криптовалют, цей факт вимагає уваги державних органів і організацій задля розробити ефективних стратегій і правил регулювання цифрових активів. Ще одним виявленим фактором зниження рівня кібербезпеки є підвищення доходу ринку даркнету, який є популярною платформою для продажу викрадених даних та інших незаконних товарів і послуг, часто використовуючи криптовалюту у якості засобу оплати.

Іншим висновком з моделі є виявлення значного позитивного впливу підвищення якості правових заходів у сфері регулювання цифрових активів на оцінку кібербезпеки країни. Існування чітких та ефективних нормативних актів значно сприяє запобіганню кіберзагроз, пов'язаних з використанням криптовалют, та їх швидкому виявленню. Це створює перспективи для майбутнього вивчення нормативно-правового поля країн Європейського Союзу з найвищими оцінками правових заходів у сфері регулювання цифрових активів і перспектив адаптації аналогічних правових практик в Україні. Іншим фактором, який позитивно впливає на рівень кібербезпеки держави є інвестиційна грамотність населення. Імовірним поясненням цьому є те, що громадяни, які займаються інвестуванням в традиційні активи, підвищують свій рівень інвестиційної грамотності, яка допомагає їм розпізнавати ризики інвестування також і цифрових активів.

Дослідження дає підстави для підвищення громадської уваги до впровадження ефективного державного регулювання криптовалютної діяльності та сприяння інвестиційній грамотності населення, створення заходів, які покликані підвищити рівень кібербезпеки та забезпечити стабільний та безпечний розвиток цифрового середовища в країні. Такі дії потребують подальшого дослідження конкретних практик регулювання цифрових активів у країнах Європейського Союзу, аналізу їх придатності до українського контексту та розробки системи політичних практик мінімізації негативного впливу використання криптовалют на кібербезпеку.

4.4 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 4.14-4.15) 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.

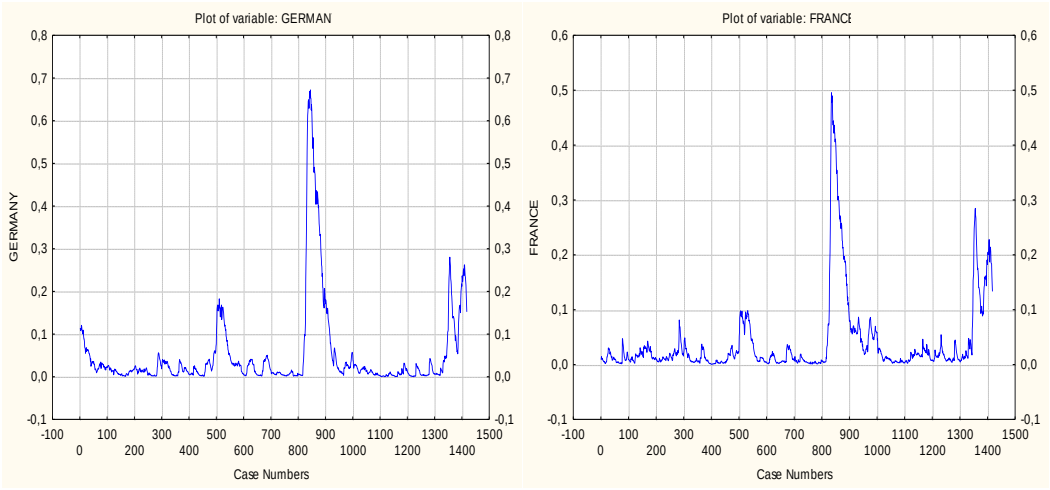


Рисунок 4.14 – Динаміка часового ряду індексу фінансової стабільності для Німеччини (лівий графік) та Франції (правий графік)

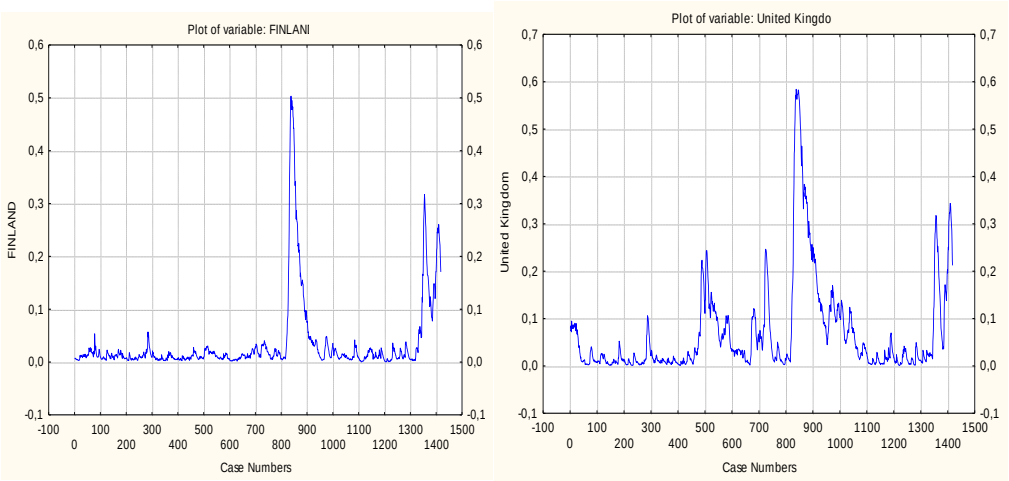


Рисунок 4.15 – Динаміка часового ряду індексу фінансової стабільності для Фінляндії (лівий графік) та Великобританії (правий графік)

Переходячи до аналізу результативних показників характеристики фінансової стабільності України, зазначимо, що динаміка варіації індексів фінансового стресу, субіндексів банківського сектору, поведінки домогосподарств, валютного ринку (рисунки 4.16–4.17) носить хвилеподібний характер. Жодний з досліджуваних показників не розвивався поступово.

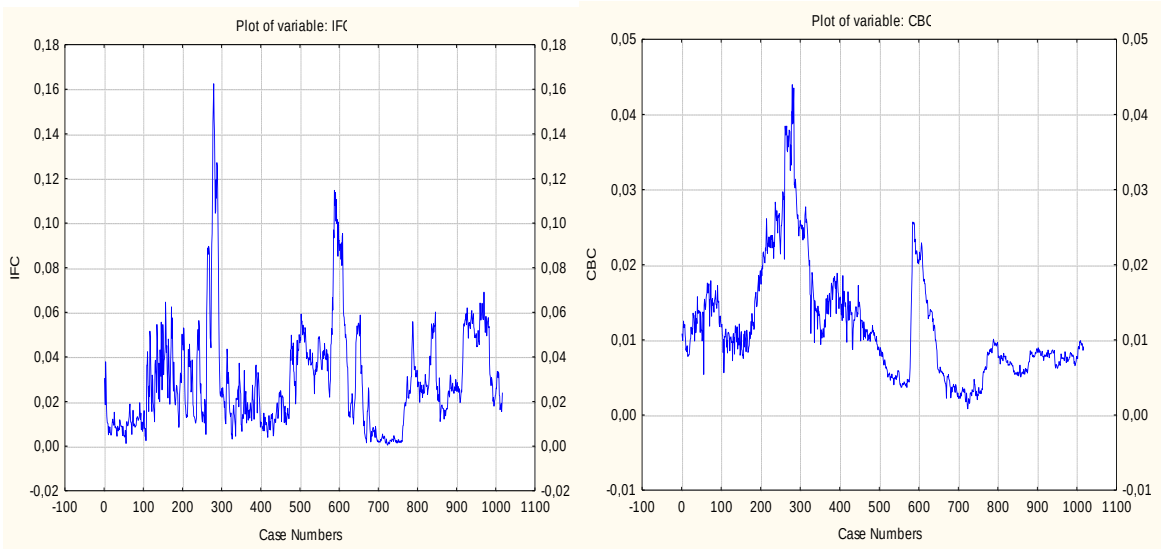


Рисунок 4.16 – Динаміка часового ряду індексу фінансового стресу (лівий графік) та субіндексу банківського сектору (правий графік) для України

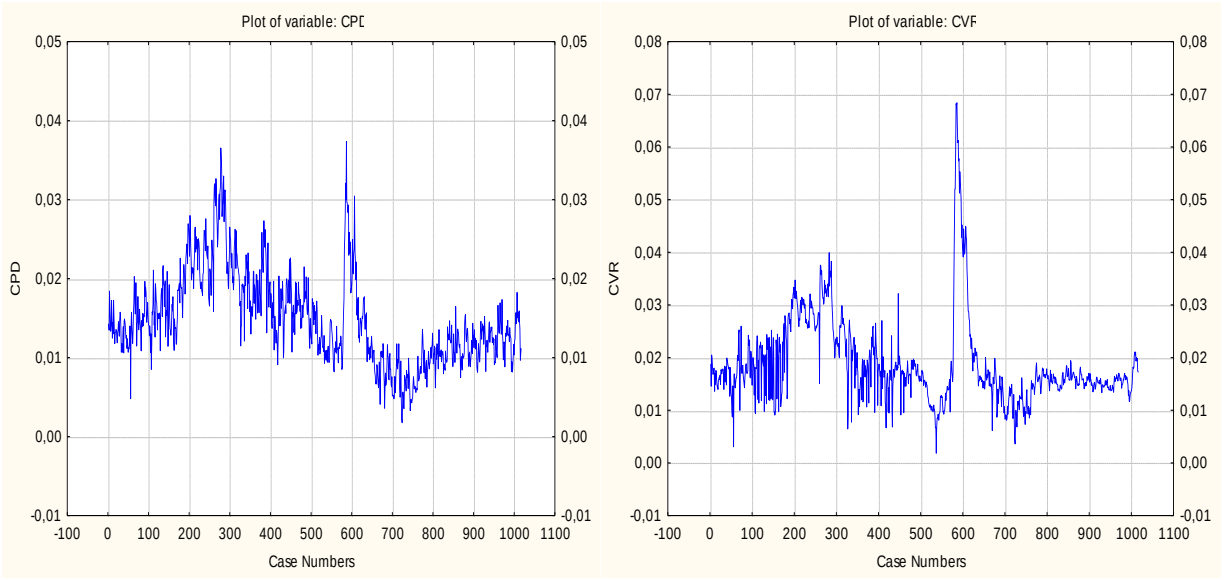


Рисунок 4.17 – Динаміка часового ряду субіндексу поведінки домогосподарств (лівий графік) та субіндексу валютного ринку (правий графік) для України

Переходячи до факторних ознак визначення впливу криптовалют на фінансову стабільність держави, представимо графічно динаміку варіації вартості та обсягів криптовалют BTC та ETH (рисунки 4.18-4.19).

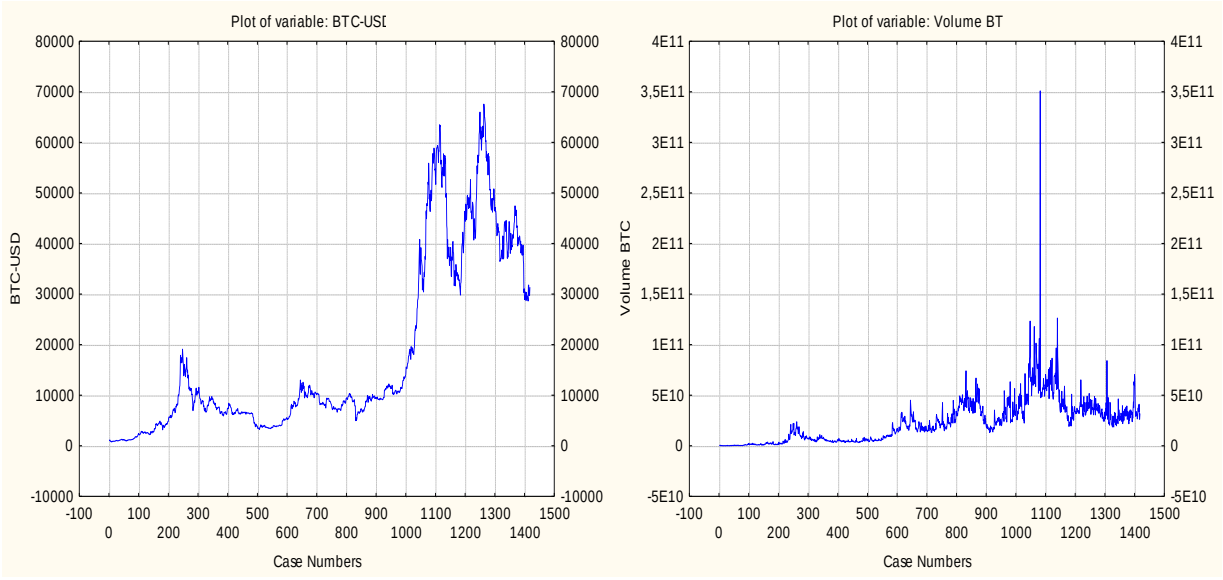


Рисунок 4.18 – Динаміка часового ряду вартості (лівий фрагмент) та обсягів криптовалют BTC (правий фрагмент)

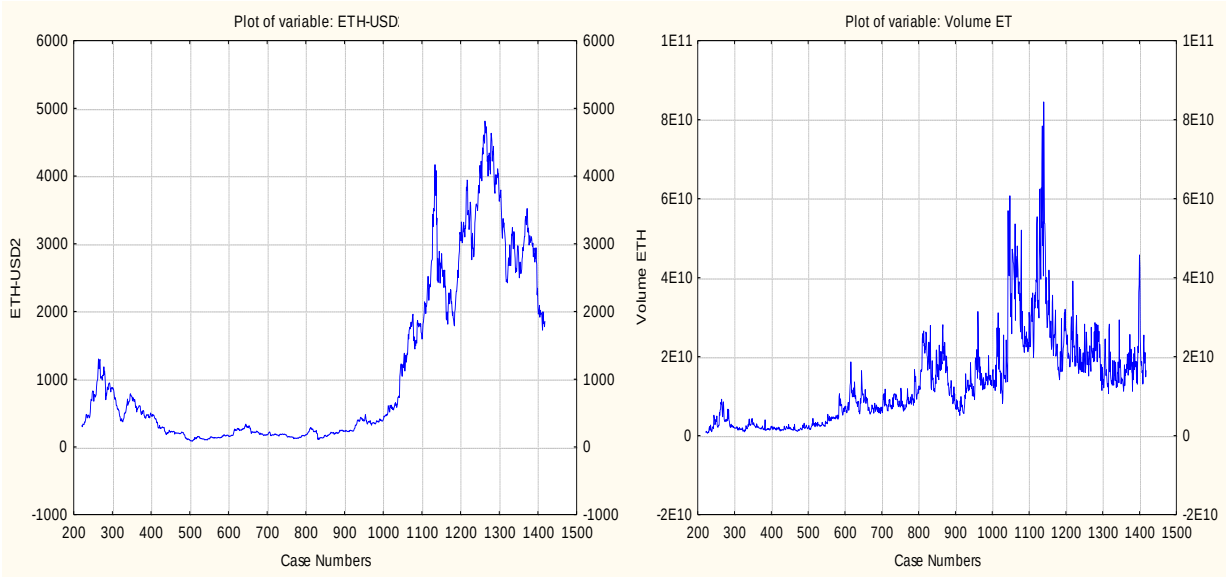


Рисунок 4.19 – Динаміка часового ряду вартості (лівий фрагмент) та обсягів криптовалют ETH (правий фрагмент)

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 4.7.

Таблиця 4.7 – 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 4.8.

Таблиця 4.8 – 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 4.8 (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 (рисунок 4.20).

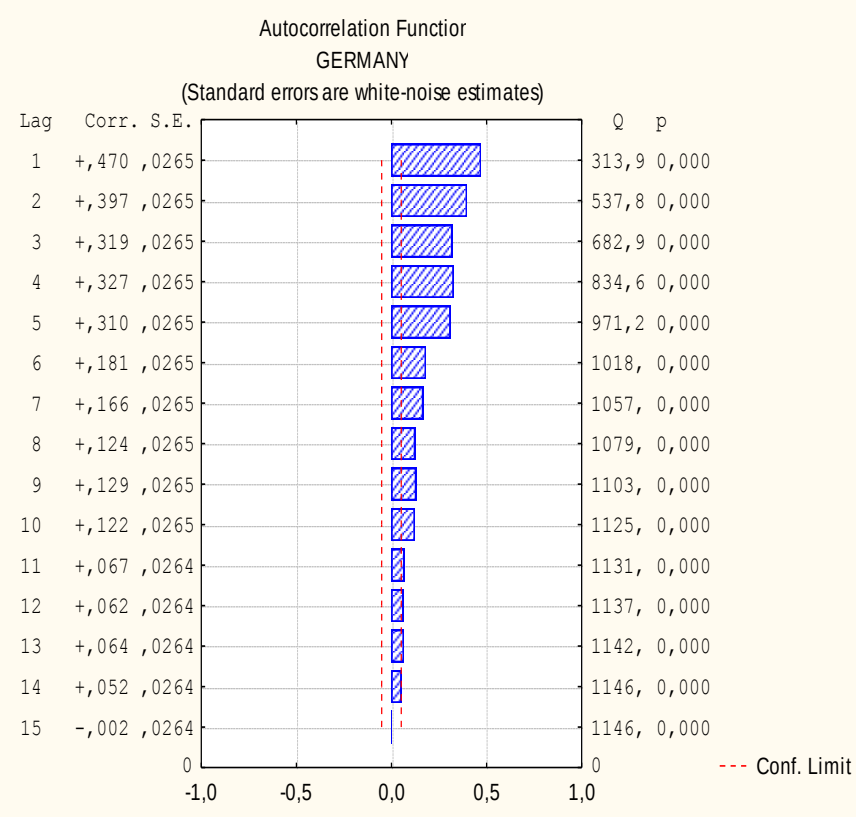


Рисунок 4.20 – Корелограми залежності значень автокореляційних функцій від часових лагів для Німеччини (лівий фрагмент) та Фінляндії (правий фрагмент)

Аналіз рисунку 4.20 (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 Франції та Великобританії, представлених на рисунку 4.21.

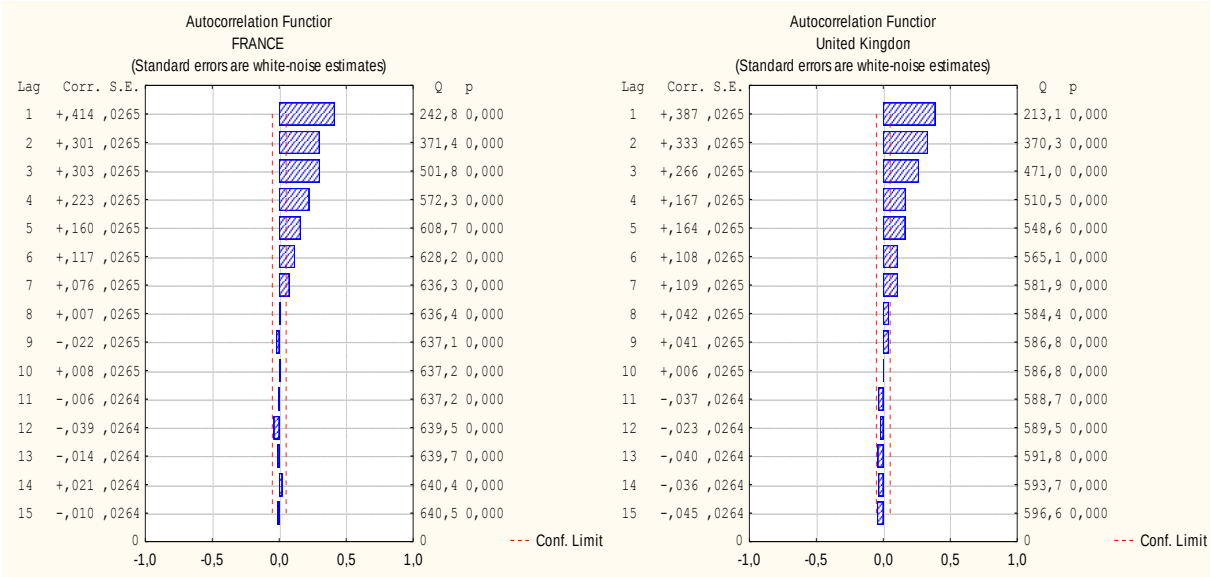


Рисунок 4.21 – Корелограми залежності значень автокореляційних функцій від часових лагів для Франції (лівий фрагмент) та Великобританії (правий фрагмент)

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 4.22 і 4.23.

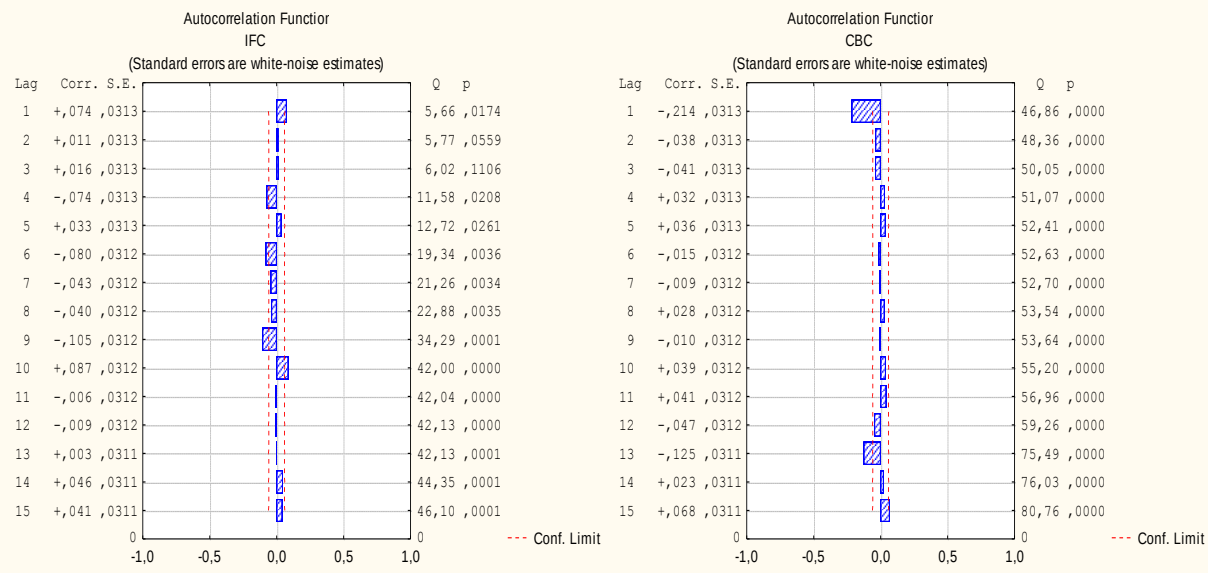


Рисунок 4.22 – Корелограми залежності значень автокореляційних функцій від часових лагів для України в розрізі індексу фінансового стресу (лівий фрагмент) та субіндексу банківського сектору (правий фрагмент)

Аналіз рисунку 4.22 (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 4.22 і рисунку 4.23.

Таким чином, на основі ґрунтового аналізу рисунків 4.22 і 4.23, 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.

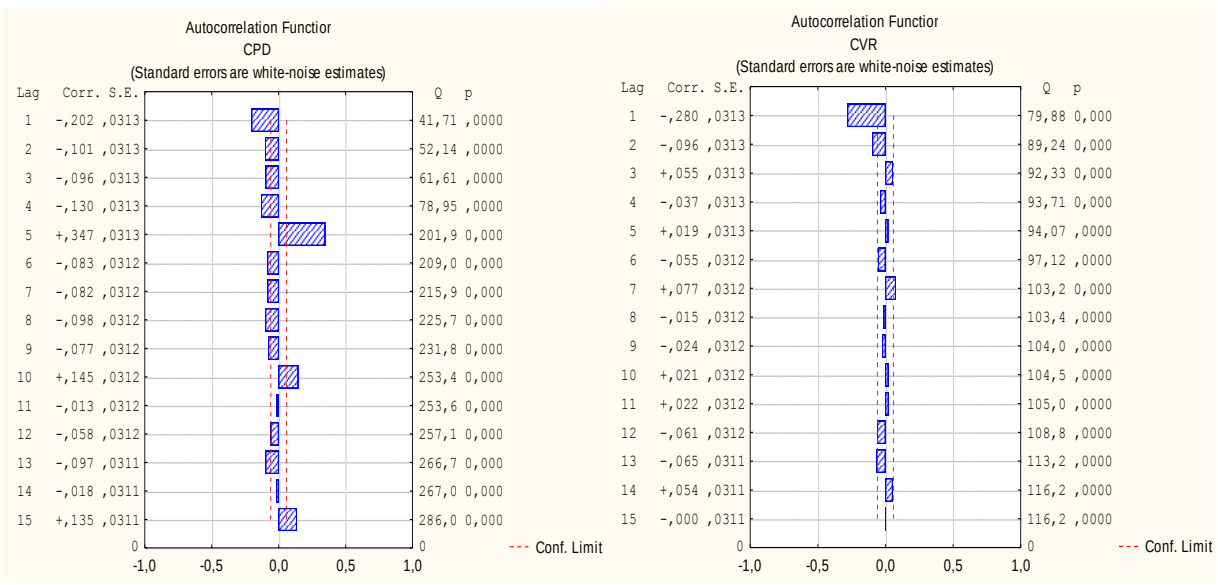


Рисунок 4.23 – Корелограми залежності значень автокореляційних функцій від часових лагів для України в розрізі субіндексу поведінки домогосподарств (лівий фрагмент) та субіндексу валютного ринку (правий фрагмент)

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 (формула 4.11):

$$y_t = b_0 \cdot x_t + b_1 \cdot x_{t-1} + b_2 \cdot x_{t-2} + \cdots + b_k \cdot x_{t-k} \qquad (4.11)$$

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 (формула 4.12):

$$b_k = a_0 + a_1 \cdot i + a_2 \cdot i^2 + \cdots + a_q \cdot i^q, q < k \qquad (4.12)$$

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 4.9-4.24.

Таблиця 4.9 – 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 4.9) 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 (формула 4.13):

$$G\text{ermany(t)} = 0.2318 \cdot 10^{-6} \cdot \text{BTC\_USD(t} - 2) \qquad (4.13)$$

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 (формула 4.13) 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.

На основі застосування статистично значущих лагів та регресійних коефіцієнтів (таблиця 4.10) поліноміальна моделі розподіленого лагу Алмона в розрізі впливу обсягів криптовалюти BTC на фінансову стабільність Німеччини набуває вигляду (формула 4.14):

$$Germany(t) = 0.333 \cdot 10^{-12} \cdot VBTC(t-2) + 0.384 \cdot 10^{-12} \cdot VBTC(t-3) + 0.283 \cdot 10^{-12} \cdot VBTC(t-1) + 0.434 \cdot 10^{-12} \cdot VBTC(t-4) \quad (4.14)$$

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

Таблиця 4.10 – 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

Таблиця 4.11 – 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 4.11) поліноміальна моделі розподіленого лагу Алмона в розрізі впливу вартості криптовалюти ETH на фінансову стабільність Німеччини набуває вигляду (формула 4.15):

$$Germany(t) = 0.3114 \cdot 10^{-5} \cdot ETH\_USD(t-2) \quad (4.15)$$

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

На основі застосування статистично значущих лагів та регресійних коефіцієнтів (таблиця 4.12) поліноміальна моделі розподіленого лагу Алмона в розрізі впливу обсягів криптовалюти ETH на фінансову стабільність Німеччини набуває вигляду (формула 4.16):

$$Germany(t) = 0.534 \cdot 10^{-12} \cdot VETH(t-2) + 0.707 \cdot 10^{-12} \cdot VETH(t-3) \quad (4.16)$$

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

Таблиця 4.12 – 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 4.13 – 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 4.13) поліноміальна моделі розподіленого лагу Алмона в розрізі впливу вартості криптовалюти BTC на фінансову стабільність Франції набуває вигляду (формула 4.17):

$$France(t) = 0.2244 \cdot 10^{-6} \cdot BTC\_USD(t-2) \quad (4.17)$$

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 4.14 – 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 4.14) поліноміальна моделі розподіленого лагу Алмона в розрізі впливу обсягів криптовалюти BTC на фінансову стабільність Франції набуває вигляду (формула 4.18):

$$France(t) = 0.270 \cdot 10^{-12} \cdot VBTC(t-2) + 0.309 \cdot 10^{-12} \cdot VBTC(t-3) + 0.230 \cdot 10^{-12} \cdot VBTC(t-1) + 0.349 \cdot 10^{-12} \cdot VBTC(t-4) \quad (4.18)$$

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

Таблиця 4.15 – 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 4.15) поліноміальна моделі розподіленого лагу Алмона в розрізі впливу вартості криптовалюти ETH на фінансову стабільність Франції набуває вигляду (формула 4.19):

$$France(t) = 0.3281 \cdot 10^{-5} \cdot ETH\_USD(t-2) \qquad (4.19)$$

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

Таблиця 4.16 – 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 4.16) поліноміальна моделі розподіленого лагу Алмона

в розрізі впливу обсягів криптовалюти ETH на фінансову стабільність Франції набуває вигляду (формула 4.20):

$$France(t) = 0.451 \cdot 10^{-12} \cdot VETH(t-2) + 0.626 \cdot 10^{-12} \cdot VETH(t-3) + 0.800 \cdot 10^{-12} \cdot VETH(t-4) \quad (4.20)$$

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

Таблиця 4.17 – 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 4.17) поліноміальна моделі розподіленого лагу Алмона в розрізі впливу вартості криптовалюти BTC на фінансову стабільність Фінляндії набуває вигляду (формула 4.21):

$$Finland(t) = 0.2144 \cdot 10^{-6} \cdot BTC\_USD(t-2) \quad (4.21)$$

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 4.18 – 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 (формула 4.22):

$$Finland(t) = 0.251 \cdot 10^{-12} \cdot VBTC(t-2) + 0.315 \cdot 10^{-12} \cdot VBTC(t-3) + 0.379 \cdot 10^{-12} \cdot VBTC(t-4) + 0.187 \cdot 10^{-12} \cdot VBTC(t-1) \quad (4.22)$$

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

Таблиця 4.19 – 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 4.19) поліноміальна моделі розподіленого лагу Алмона в розрізі впливу вартості криптовалюти ETH на фінансову стабільність Фінляндії набуває вигляду (формула 4.23):

$$Finland(t) = 0.3179 \cdot 10^{-5} \cdot ETH(t-2) \quad (4.23)$$

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

Таблиця 4.20 – 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 4.20) поліноміальна моделі розподіленого лагу Алмона в розрізі впливу обсягів криптовалюти ETH на фінансову стабільність Фінляндії набуває вигляду (формула 4.24):

$$Finland(t) = 0.418 \cdot 10^{-12} \cdot VETH(t-2) + 0.614 \cdot 10^{-12} \cdot VETH(t-3) + 0.809 \cdot 10^{-12} \cdot VETH(t-4) \quad (4.24)$$

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

Таблиця 4.21 – 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 4.21) поліноміальна моделі розподіленого лагу Алмона в розрізі впливу вартості криптовалюти BTC на фінансову стабільність Великобританії набуває вигляду (формула 4.25):

$$United\_Kingdom(t) = 0.3930 \cdot 10^{-6} \cdot BTC\_USD(t-2) \qquad (4.25)$$

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

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

На основі застосування статистично значущих лагів та регресійних коефіцієнтів (таблиця 4.22) поліноміальна моделі розподіленого лагу Алмона в розрізі впливу обсягів криптовалюти BTC на фінансову стабільність Великобританії набуває вигляду (формула 4.26):

$$\begin{aligned} &United\_Kingdom(t) \\ &= 0.362 \cdot 10^{-12} \cdot VBTC(t-2) + 0.387 \cdot 10^{-12} \cdot VBTC(t-3) \\ &+ 0.411 \cdot 10^{-12} \cdot VBTC(t-4) + 0.338 \cdot 10^{-12} \cdot VBTC(t-1) \\ &+ 0.436 \cdot 10^{-12} \cdot VBTC(t-5) + 0.313 \cdot 10^{-12} \cdot VBTC(t) \end{aligned} \qquad (4.26)$$

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

Таблиця 4.22 – 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

Таблиця 4.23 – 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 4.23) поліноміальна моделі розподіленого лагу Алмона в розрізі впливу вартості криптовалюти ETH на фінансову стабільність Великобританії набуває вигляду (формула 4.27):

$$\text{United\_Kingdom(t)} = 0.4820 \cdot 10^{-5} \cdot \text{ETH\_USD(t} - 2) \qquad (4.27)$$

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

Таблиця 4.24 – 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 4.24) поліноміальна моделі розподіленого лагу Алмона в розрізі впливу обсягів криптовалюти ETH на фінансову стабільність Великобританії набуває вигляду (формула 4.28):

$$\begin{aligned} UK(\mathrm{t}) = {} & 0.549 \cdot 10^{-12} \cdot \mathrm{VETH}(\mathrm{t}-2) + 0.668 \cdot 10^{-12} \cdot \mathrm{VETH}(\mathrm{t}-3) \\ & + 0.787 \cdot 10^{-12} \cdot \mathrm{VETH}(\mathrm{t}-4) + 0.906 \cdot 10^{-12} \\ & \cdot \mathrm{VETH}(\mathrm{t}-5) \end{aligned} \quad (4.28)$$

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

Аналіз наведених вище моделей розподіленого лагу (4.13) – (4.28) дозволяє систематизувати величини лагових затримок та напрямки впливу криптовалют на фінансову стабільність Німеччини, Фінляндії, Франції, Великобританії у вигляді таблиці 4.25.

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.

Таблиця 4.25 – 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

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 4.26).

На основі представлених в таблиці 4.26 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.

Таблиця 4.26 – 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

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 4.29:

$$EK = \frac{dy}{dx} \cdot \frac{\underline{x}}{\underline{y}} \tag{4.29}$$

де EK - коефіцієнт еластичності;

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

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

Оскільки для даного випадку $\frac{dy}{dx}$ буде дорівнювати регресійним коефіцієнтам (b_k), представленим в таблиці 4.27, формула 4.30 буде набувати наступного вигляду:

$$EK(b_k) = b_k \cdot \frac{\underline{x}}{\underline{y}} \tag{4.30}$$

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 (таблиці 4.27-4.28).

Таблиця 4.27 – 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 4.28 – 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 4.26) та середніх значень факторних та результативної ознак для Німеччини, Фінляндії, Франції, Великобританії (таблиці 4.27-4.28) у формулу 4.30 обчислимо коефіцієнти еластичності впливу 1%-вої зміни фінансових активів на відсоткову зміну індексу фінансової стабільності держав (таблиця 4.29).

Таким чином, на основі даних таблиці 4.29 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.

Таблиця 4.29 – 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

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 4.30).

На основі застосування статистично значущих лагів та регресійних коефіцієнтів (таблиця 4.30) поліноміальна моделі розподіленого лагу Алмона в розрізі впливу вартості криптовалюти BTC на індекс фінансового стресу для України набуває вигляду (формула 4.31):

$$\mathrm{IFC(t)} = 0.1272 \cdot 10^{-6} \cdot \mathrm{BTC\_USD(t-3)} + 0.2847 \cdot 10^{-6} \cdot \mathrm{BTC\_USD(t-2)} + 0.4423 \cdot 10^{-6} \cdot \mathrm{BTC\_USD(t-1)} + 0.5998 \cdot 10^{-6} \cdot \mathrm{BTC\_USD(t)} \quad (4.31)$$

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

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

Таблиця 4.30 – 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

Таблиця 4.31 – 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

На основі застосування статистично значущих лагів та регресійних коефіцієнтів (таблиця 4.31) поліноміальна моделі розподіленого лагу Алмона

в розрізі впливу обсягів криптовалюти BTC на індекс фінансового стресу для України набуває вигляду (формула 4.32):

$$IFC(t) = 0.110 \cdot 10^{-12} \cdot VBTC(t-2) + 0.106 \cdot 10^{-12} \cdot VBTC(t-3) + 0.102 \cdot 10^{-12} \cdot VBTC(t-4) + 0.114 \cdot 10^{-12} \cdot VBTC(t-1) + 0.098 \cdot 10^{-12} \cdot VBTC(t-5) + 0.118 \cdot 10^{-12} \cdot VBTC(t) + 0.095 \cdot 10^{-12} \cdot VBTC(t-6) \quad (4.32)$$

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

Таблиця 4.32 – 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 4.32) поліноміальна моделі розподіленого лагу Алмона в розрізі впливу вартості криптовалюти ETH на індекс фінансового стресу для України набуває вигляду (формула 4.33):

$$\mathrm{IFC(t)} = 0.1937 \cdot 10^{-5} \cdot \mathrm{ETH\_USD(t-3)} + 0.2710 \cdot 10^{-5} \cdot \mathrm{ETH\_USD(t-2)} + 0.3484 \cdot 10^{-5} \cdot \mathrm{ETH\_USD(t-1)} + 0.4258 \cdot 10^{-5} \cdot \mathrm{ETH\_USD(t)} \quad (4.33)$$

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

Таблиця 4.33 – 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 4.33) поліноміальна моделі розподіленого лагу Алмона в розрізі впливу обсягів криптовалюти ETH на індекс фінансового стресу для України набуває вигляду (формула 4.34):

$$IFC(t) = 0.192 \cdot 10^{-12} \cdot VETH(t-3) + 0.201 \cdot 10^{-12} \cdot VETH(t-2) + 0.183 \cdot 10^{-12} \cdot VETH(t-4) + 0.211 \cdot 10^{-12} \cdot VETH(t-1) + 0.173 \cdot 10^{-12} \cdot VETH(t-5) + 0.220 \cdot 10^{-12} \cdot VETH(t) \quad (4.34)$$

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

Таблиця 4.34 – 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 4.34) поліноміальна моделі розподіленого лагу Алмона

в розрізі впливу вартості криптовалюти BTC на субіндекс банківського сектору для України набуває вигляду (формула 4.35):

$$CBC(t) = 0.8602 \cdot 10^{-7} \cdot BTC\_USD(t-1) \quad (4.35)$$

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 4.35 – 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 4.35) поліноміальна моделі розподіленого лагу Алмона в розрізі впливу обсягів криптовалюти BTC на субіндекс банківського сектору для України набуває вигляду (формула 4.36):

$$CBC(t) = 0.073 \cdot 10^{-12} \cdot VBTC(t-1) + 0.073 \cdot 10^{-12} \cdot VBTC(t-2) + 0.072 \cdot 10^{-12} \cdot VBTC(t) \quad (4.36)$$

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 4.36 – 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 4.36) поліноміальна моделі розподіленого лагу Алмона в розрізі впливу вартості криптовалюти ETH на субіндекс банківського сектору для України набуває вигляду (формула 4.37):

$$CBC(t) = 0.1237 \cdot 10^{-5} \cdot ETH\_USD(t-1) \qquad (4.37)$$

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 4.37 – 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 4.37) поліноміальна моделі розподіленого лагу Алмона

в розрізі впливу обсягів криптовалюти ETH на субіндекс банківського сектору для України набуває вигляду (формула 4.38):

$$CBC(t) = 0.127 \cdot 10^{-12} \cdot VETH(t-1) \quad (4.38)$$

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 4.38 – 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 4.38) поліноміальна моделі розподіленого лагу Алмона в розрізі впливу вартості криптовалюти BTC на субіндекс поведінки домогосподарств для України набуває вигляду (формула 4.39):

$$CPD(t) = 0.5947 \cdot 10^{-7} \cdot BTC\_USD(t-2) + 0.6324 \cdot 10^{-7} \cdot BTC\_USD(t-3) \quad (4.39)$$

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 4.39 – 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.	StandardError	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 4.39) поліноміальна моделі розподіленого лагу Алмона в розрізі впливу обсягів криптовалюти BTC на субіндекс поведінки домогосподарств для України набуває вигляду (формула 4.40):

$$CPD(t) = 0.051 \cdot 10^{-12} \cdot VBTC(t-2) + 0.053 \cdot 10^{-12} \cdot VBTC(t-3) + 0.054 \cdot 10^{-12} \cdot VBTC(t-4) + 0.049 \cdot 10^{-12} \cdot VBTC(t-1) + 0.056 \cdot 10^{-12} \cdot VBTC(t-5) + 0.048 \cdot 10^{-12} \cdot VBTC(t) \quad (4.40)$$

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

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

На основі застосування статистично значущих лагів та регресійних коефіцієнтів (таблиця 4.40) поліноміальна моделі розподіленого лагу Алмона в розрізі впливу вартості криптовалюти ETH на субіндекс поведінки домогосподарств для України набуває вигляду (формула 4.41):

$$CPD(t) = 0.9758 \cdot 10^{-6} \cdot ETH\_USD(t-3) + 0.8352 \cdot 10^{-6} \cdot ETH\_USD(t-2) + 0.1116 \cdot 10^{-6} \cdot ETH\_USD(t-4) \quad (4.41)$$

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 4.40 – 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

Таблиця 4.41 – 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 4.41) поліноміальна моделі розподіленого лагу Алмона в розрізі впливу обсягів криптовалюти ETH на субіндекс поведінки домогосподарств для України набуває вигляду (формула 4.42):

$$CPD(t) = 0.088 \cdot 10^{-12} \cdot VETH(t-2) + 0.095 \cdot 10^{-12} \cdot VETH(t-3) + 0.102 \cdot 10^{-12} \cdot VETH(t-4) + 0.081 \cdot 10^{-12} \cdot VETH(t-1) + 0.109 \cdot 10^{-12} \cdot VETH(t-5) \quad (4.42)$$

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 4.42 – 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 4.42) поліноміальна моделі розподіленого лагу Алмона в розрізі впливу вартості криптовалюти BTC на субіндекс валютного ринку для України набуває вигляду (формула 4.43):

$$CVR(t) = 0.1608 \cdot 10^{-6} \cdot BTC\_USD(t-1) \quad (4.43)$$

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 4.43 – 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 4.43) поліноміальна моделі розподіленого лагу Алмона в розрізі впливу обсягів криптовалюти BTC на субіндекс валютного ринку для України набуває вигляду (формула 4.44):

$$CVR(t) = 0.139 \cdot 10^{-12} \cdot VBTC(t-1) + 0.140 \cdot 10^{-12} \cdot VBTC(t-2) + 0.139 \cdot 10^{-12} \cdot VBTC(t) \quad (4.44)$$

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 4.44 – 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 4.44) поліноміальна моделі розподіленого лагу Алмона

в розрізі впливу вартості криптовалюти ETH на субіндекс валютного ринку для України набуває вигляду (формула 4.45):

$$CVR(t) = 0.2329 \cdot 10^{-5} \cdot ETH\_USD(t-1) \quad (4.45)$$

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 4.45 – 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 4.45) поліноміальна моделі розподіленого лагу Алмона в розрізі впливу обсягів криптовалюти ETH на субіндекс валютного ринку для України набуває вигляду (формула 4.46):

$$CVR(t) = 0.248 \cdot 10^{-12} \cdot VETH(t-1) + 0.253 \cdot 10^{-12} \cdot VETH(t-2) + 0.243 \cdot 10^{-12} \cdot VETH(t) \quad (4.46)$$

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 4.46).

Таблиця 4.46 – 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+

На основі аналізу таблиці 4.46 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.

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 4.47).

На основі представлених в таблиці 4.47 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.

Таблиця 4.47 – 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	$0.1608 \cdot 10^{-6}$	$0.139 \cdot 10^{-12}$	$0.2329 \cdot 10^{-5}$	$0.248 \cdot 10^{-12}$

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 4.48-4.49).

Таблиця 4.48 – 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 4.49 – 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 4.47) та середніх значень факторних та результативної ознак для України (таблиці 4.48-4.49) у формулу (4.30) обчислимо коефіцієнти еластичності вливу 1%-вої зміни фінансових активів на відсоткову зміну індексу фінансової стабільності держав (таблиця 4.50).

Таблиця 4.50 – 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 4.50 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 на 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%.

5 МЕТОДИЧНІ ЗАСАДИ ОЦІНЮВАННЯ РОЛІ ДІДЖИТАЛІЗАЦІЇ В СИСТЕМІ ПРОТИДІЇ ЛЕГАЛІЗАЦІЇ ДОХОДІВ, ОТРИМАНИХ НЕЗАКОННИМ ШЛЯХОМ

5.1 Дослідження місця та значення діджиталізації в системі протидії легалізації доходів, отриманих незаконним шляхом

Стрімкий розвиток інформаційних технологій в банківській сфері вплинув на збільшення швидкості проведення транзакцій, підвищення рівня доступності клієнтів до банківських послуг, розширення спектру банківських послуг та інше. В цілому, інформаційні технології значно покращують ефективність функціонування економічних систем.

Проте поряд з позитивними зрушеннями в фінансовій сфері інформаційні технології 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, доцільно оцінити рівень ефективності системи протидії легалізації кримінальних доходів в частині виявлення фінансових операцій, які можуть бути спрямовані на легалізацію незаконних доходів, та результативних факторів, які на неї 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 [155].

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 [156].

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 шахрайств. Динаміка результативної ознаки відображена на рисунку 5.1. На основі даних рисунку 5.1 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 [157].

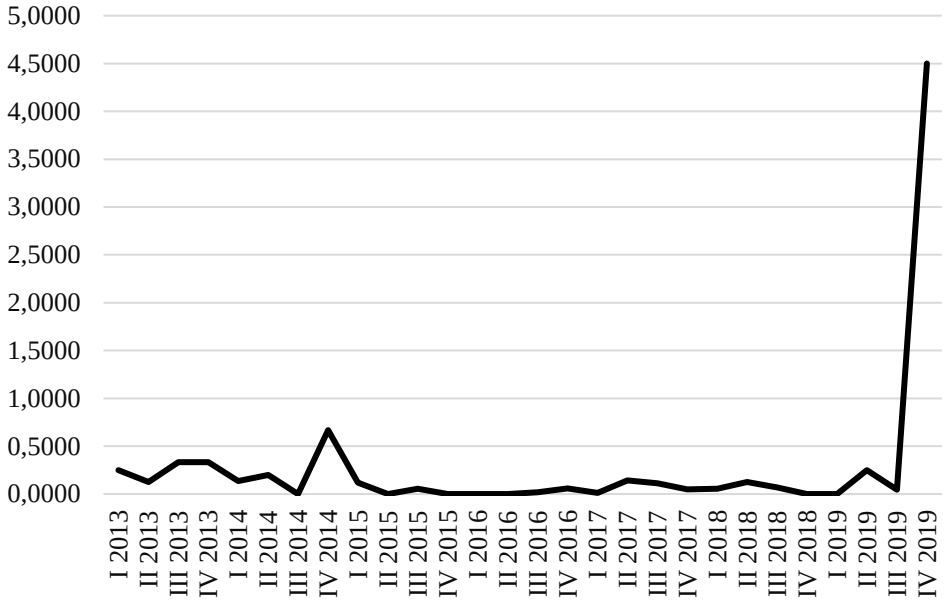


Рисунок 5.1 – Частка направлених до суду обвинувальних актів у загальній кількості кримінальних правопорушень, за якими проводилось досудове розслідування у відповідний період

Джерело: розроблено автором на основі [158]

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 5.2). 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

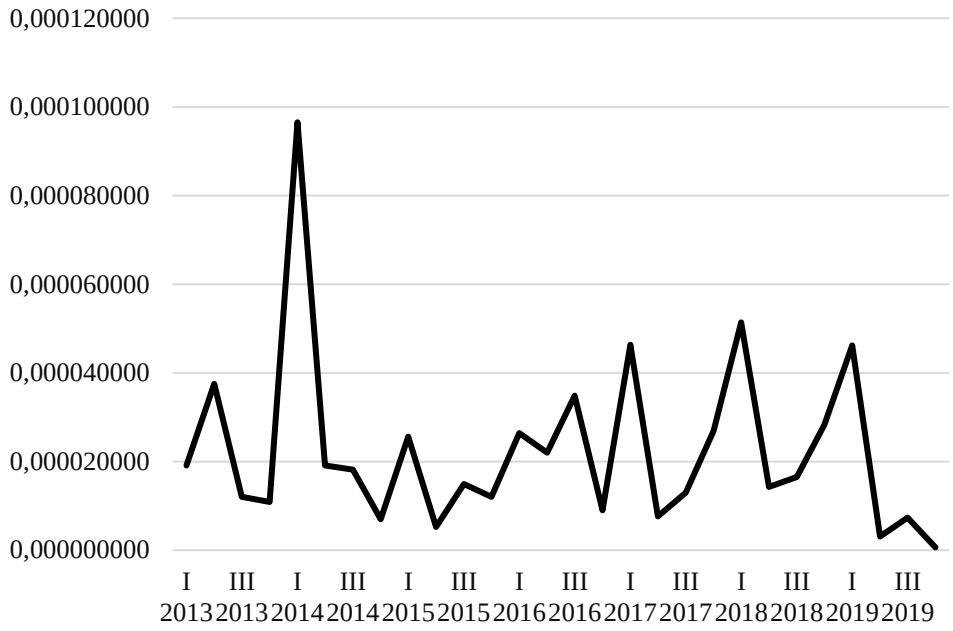


Рисунок 5.2 – Частка кримінальних правопорушень по яких проводилось досудове розслідування, яка припадає на одне повідомлення про операцію, що було передане до Державної служби фінансового моніторингу

Джерело: розроблено автором на основі [158]

Характеристикою другої альтернативи є показник діджиталізації економіки, який є відношенням кількості абонентів мережі інтернет до чисельності населення (рисунок 5.3). 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.

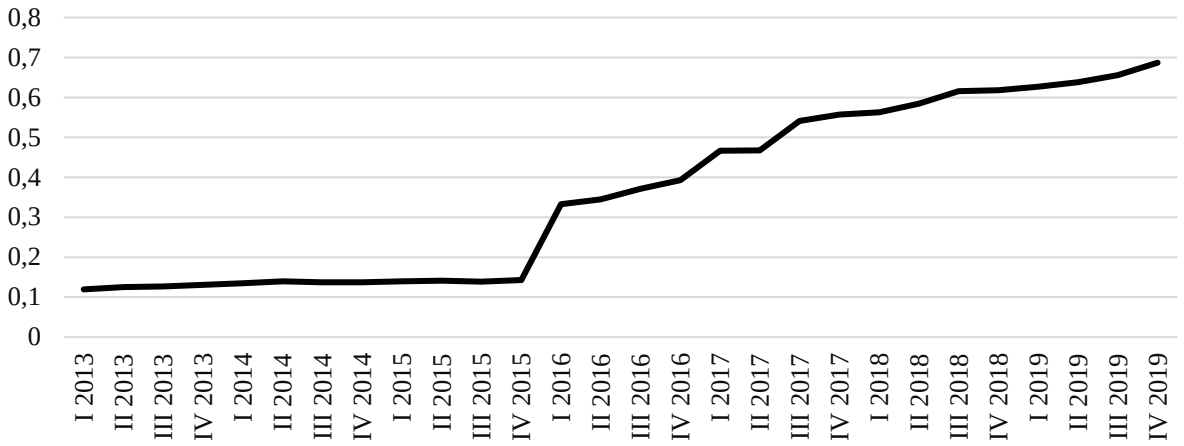


Рисунок 5.3 – Динаміка діджиталізації економіки України

Джерело: розроблено автором на основі [158]

Для специфікації функції залежності результативної ознаки від факторних, побудуємо корелограму нульових різниць (рисунок 5.4) та таблицю автокореляційної функції (рисунок 5.5).

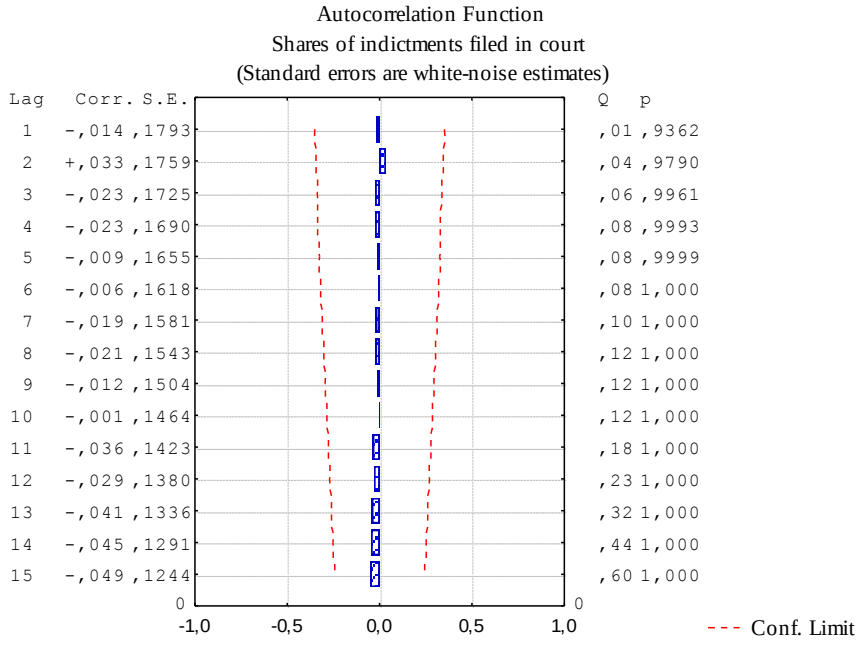


Рисунок 5.4 – Корелограма нульових різниць Частки направлених до суду обвинувальних актів

Джерело: розроблено автором

Lag	Autocorrelation Function Shares of indictments filed in court (Standard errors are white-noise estimates) Auto-Corr.	Std.Err.	Box & Ljung Q	p
1	-0,0143	0,1793	0,0064	0,93624
2	0,0334	0,1759	0,0425	0,97896
3	-0,0231	0,1725	0,0604	0,99612
4	-0,0226	0,1690	0,0783	0,99925
5	-0,0086	0,1655	0,0810	0,99990
6	-0,0060	0,1618	0,0824	0,99998
7	-0,0191	0,1581	0,0969	0,99999
8	-0,0208	0,1543	0,1151	1,00000
9	-0,0122	0,1504	0,1216	1,00000
10	-0,0015	0,1464	0,1217	1,00000
11	-0,0356	0,1423	0,1843	1,00000
12	-0,0290	0,1380	0,2283	1,00000
13	-0,0408	0,1336	0,3215	1,00000
14	-0,0453	0,1291	0,4448	1,00000

Рисунок 5.5 – Значення автокореляційної функції та статистична значущість коефіцієнтів автокореляції нульових різниць Частки направлених до суду обвинувальних актів

Джерело: розроблено автором

Як видно з рисунків 5.4 та 5.5, 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 (формула 5.1):

$$u(x_1, x_2, x_3, \dots, x_n) = \prod_{j=1}^{n} \left(x_j - \varphi_j\right)^{\beta_j} \quad (5.1)$$

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 (5.1) набуває вигляду функції Кобба-Дугласа (формула 5.2).

$$u(x_1, x_2) = \prod_{j=1}^{2} \left(x_j\right)^{\beta_j}, \sum_{j=1}^{2} \beta_j = 1 \quad (5.2)$$

Враховуючи обмеження $\sum_{j=1}^{2} \quad \beta_j = 1$ формули (5.2), 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 (формула 5.3):

$$\sum_{t=1}^{T} \quad \left(u_t - \prod_{j=1}^{2} \quad (x_{jt})^{\beta_j} \right)^2 \rightarrow min \tag{5.3}$$

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

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 (формула 5.3) оцінювання ефективності системи протидії легалізації кримінальних доходів за допомогою функції корисності дозволяє отримати наступні результати (формула 5.4) при мінімальному значенні суми квадратів відхилень фактичних значень частка направлених до суду обвинувальних актів від їх теоретичних рівнів на рівні 18,28 од.

$$u(x_1, x_2) = {x_1}^{0,0019} \cdot {x_2}^{0,9981} \quad (5.4)$$

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.

Як результат, 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.

5.2 Оцінювання ефективності інституційних змін системи протидії легалізації доходів одержаних незаконним шляхом

Окремо потрібно зупинитись на дослідження інституційної складової системи протидії легалізації доходів, одержаних незаконним шляхом. На даний час, державні органи контролю, на основі підозрілих операцій виявлених Державною службою фінансового моніторингу у 2021 році на загальну суму 103190,92 млн грн, передали до суду 15 обвинувальних актів. У свою чергу, судами було винесено 32 обвинувальні вироки і повернуто державі 510,8 млн грн [160]. Порівняльний аналіз свідчить про те, що левова частка доходів, отриманих незаконним шляхом знаходиться поза увагою Державної служби фінансового моніторингу, а походження ще меншої частини грошей вдається обґрунтувати доказами та відстояти позицію держави у суді.

Актуалізація питання ефективності діяльності інституційної складової системи протидії легалізації незаконних доходів в Україні підвищується також тією ситуацією, що протягом останніх років ця система зазнала певних змін: частина органів припинила своє існування, а деякі навпаки – тільки почали свою діяльність.

Переходячи безпосередньо до основної мети дослідження, в першу чергу зауважимо, що процес легалізації коштів, отриманих незаконним

шляхом складається з трьох етапів: розміщення, розшарування та інтеграція. Відповідно до цих стадій відбувається трансформація злочинних доходів у фінансові інструменти, які відрізняються за параметрами місця, часу, типу та структури. Зловмисники намагаються не стільки диверсифікувати джерела походження кримінальних доходів, скільки збільшити різноманітність шляхів їх легалізації. Протягом стадії розшарування приховується слід злочинних доходів, ускладнюються фінансові операції та заплутуються транзакції. Завершується процес легалізації поверненням відмитих коштів у національну економіку, але уже під видом офіційних доходів.

В свою чергу, держава може використовувати два шляхи протидії легалізації кримінальних доходів: створення сприятливих соціально-економічних умов для детінізації економіки, що призведе до мінімізації потенційно отриманого ефекту від незаконних дій; посилення регуляторного впливу у вигляді збільшення інструментів контролі та підвищення рівня покарання за легалізацію кримінальних доходів.

В медах цього дослідження сконцентруємо увагу на другому напрямку боротьби з процесом легалізації кримінальних доходів, а саме напрямку виявлення та покарання за легалізацію кримінальних доходів. Це обумовлено тим, що в межах його реалізації можна спиратись на чітко сформований механізм взаємодії державних інститутів, тоді як забезпечення першого напрямку потребує реалізації численних методів удосконалення кожної галузі економіки.

Регулятивний механізм протидії легалізації незаконних доходів складається з двох елементів: виявлення та покарання. На етапі виявлення задіяні такі інституції системи протидії легалізації незаконних доходів, як Державна служба фінансового моніторингу, Національний банк України, Національна комісія з цінних паперів та фондового ринку. Основна їх роль по відношенню до протидії легалізації – виявити ймовірні спроби легалізації кримінальних доходів.

У свою чергу, етап покарання складається з декількох кроків, які реалізують різні групи державних інституцій. Так, встановлення всіх обставин ймовірного злочину, підтримання публічного обвинувачення та здійснення правосуддя забезпечується системою правоохоронних органів. Відповідно до Кримінального процесуального кодексу України, досудове слідство і дізнання (власне встановлення всіх обставин ймовірного злочину) здійснюють слідчі підрозділи Національної поліції, Служби безпеки України, органів Державного бюро розслідувань, підрозділ детективів та підрозділ внутрішнього контролю Національного антикорупційного бюро України, підрозділи детективів органів Бюро економічної безпеки України. Зазначені підрозділи збирають, досліджують, оцінюють та використовують докази для встановлення обставин злочину. Зазначені органи формують доказову базу і встановлюють факт легалізації кримінальних доходів.

На прокуратуру покладені функції державного обвинувачення в суді, тобто відстоювання доказів і фактів, які були зібрані органами досудового слідства.

На завершальному етапі процесу покарання, суд встановлює достатність наданих доказів та здійснює правосуддя: підтверджує або спростовує факт легалізації доходів, отриманих незаконним шляхом та визначає міру покарання в разі винесення обвинувального вироку.

Без ефективної роботи органів слідства, прокуратури та суду неможливе високоефективне функціонування системи протидії легалізації незаконних доходів. Неважливо, наскільки якісно фінансовий моніторинг виявив ймовірні випадки легалізації незаконних доходів, якщо доказова база буде неправильно сформована та міститиме недостатньо доказів в суді позиція обвинувачення буде не обґрунтованою й призведе до позитивного для буде дуже складно виправдати звинувачуваного.

Зважаючи на необхідність постійного підвищення ефективності роботи правоохоронних органів в Україні відбувається постійна трансформація даної системи: виникають нові органи слідства, переформатується діяльність

прокуратури та організація діяльності судів. Останнім часом були створені Національна поліція (2015 рік), Національне антикорупційне бюро України (2015), Державне бюро розслідувань (2016 рік), Бюро економічної безпеки України (2021 рік). У 2016 році розпочалась судова реформа. Уповноваженими державними органами постійно приймаються рішення про удосконалення діяльності правоохоронних органів: зміни до законів, постанови Кабінету міністрів, внутрішні нормативно-правові акти правоохоронних органів.

Провівши експрес огляд трансформації елементу «покарання» системи протидії легалізації кримінальних доходів, актуальності набуває визначення впливу прийнятих змін на його ефективність. З цією метою використаємо методологію аналізу виживаності. Саме цей підхід дозволить визначити ймовірність уникнення покарання на кожному з часових етапів трансформації інституційної складової системи протидії легалізації кримінальних доходів. Отримані результати дозволять сформувати інформаційну базу для прийняття ефективних управлінських рішень з приводу подальшого удосконалення реформування державних органів покарання та виявити рівень успішності загального тренду інституційної складової системи протидії легалізації кримінальних доходів.

Переходячи безпосередньо до аналізу науково-методичного підходу до оцінювання ефективності інституційних змін системи протидії легалізації кримінальних доходів зазначимо, що він складається з 5-ти етапів кожен з яких буде детально розглянутий нижче.

На першому етапі відбувається формування статистичної бази дослідження. Так, з єдиного державного реєстру судових рішень було відібрано 42 спостереження, які являють собою судові провадження, що закінчились обвинувальним чи виправдувальним вироком у період з 2019 по 2022 рік. Встановлений початок вчинення злочинного діяння, направленого на отримання незаконного доходу з метою подальшої його легалізації по вибірці був у проміжку від 2009 до 2022 року.

Відповідно до таблиці Д.1, додатку Д, розглядаємо дві дати – Дата почату вчинення злочину та Дата вироку суду. Для розрахунку моделі в програмі STATISTICA ці дати було розділено на 6 змінних: Day_1, Month_1, Year_1, Day_2, Month_2, Year_2, де змінні з позначкою 1 відповідають дню, місяцю і року Дати початку вчинення злочину, а змінні з позначкою 2 – дню, місяцю і року Дати вироку суду відповідно. Характеристиками спостережень виступають NRA – Кількість суміжних статтей Кримінального кодексу України, які описують злочини, за допомогою яких було реалізоване накопичення незаконного доходу. Стовпець Суміжні статті є інформативним і не буде брати участь у моделі виживаності.

All – Сума доходу, отриманого незаконним шляхом, грн. FSR – Сума компенсованих державі коштів у вигляді конфіскацій чи відшкодування судових витрат, грн. ND – Кількість підсудних осіб, відповідно до яких здійснювалось провадження. NIILE – Кількість потерпілих фізичних та юридичних осіб. Censored – бінарна змінна, яка набуває значення 1 в разі винесення обвинувального вироку суду. NYCV – Кількість років позбавлення волі відповідно до вироку суду.

Переходячи до аналізу другого етапу, зупинимось на дослідженні ефективності інституційних змін у системі протидії легалізації кримінальних доходів на основі побудови таблиць виживаності.

Метод аналізу таблиць виживання будується на підході аналізу вибірок даних, для яких важливий інтервал часу між подіями що відбулись. Сутність таблиці виживаності полягає в тому, що період спостереження вибірки ділиться на менші інтервали часу. Для кожного інтервалу часу для вирахування ймовірності настання термінальної події протягом цього інтервалу часу використовуються всі спостереження, які відбулись щонайменше протягом цього часу. Потім розраховані для кожного інтервалу оцінки ймовірності використовуються для оцінки ймовірності настання події в різні моменти часу.

Для нашого дослідження термінальною подією є винесення вироку судом. За допомогою методу побудови таблиць виживання планується

розрахувати ймовірності винесення не настання для зловмисників такої події як винесення вироку судом, а отже низької ефективності системи протидії легалізації кримінальних доходів протягом певного періоду часу.

Для побудови таблиць виживання було використано спеціалізоване програмне забезпечення для статистичного аналізу STATISTICA (таблиця 5.1). В даному програмному забезпеченні реалізований блок нелінійного оцінювання аналізу виживання на основі життєвих міток та аналізу розподілу.

На основі даних таблиці 5.1, протягом перших 500 днів після вчинення злочину з метою отримання незаконного доходу з подальшою легалізацією цих доходів (стовпчики Interval Start та Interval Width) серед 42 спостережень (Number Entering) тільки у 8 випадках був винесений обвинувальний вирок (Number Dying). Відповідно, частка «вижившихх» спостережень за перші 500 днів, тобто тих, для яких не настала дата ухвалення обвинувального вироку, склала 0,807 (Proportn Surviving). Натомість частка «померлих», тобто тих спостережень, для яких було ухвалено обвинувальний вирок – 0,193. Відповідно, ймовірність ухвали обвинувального вироку протягом відповідного інтервалу (0 – 500 днів) у спостережень склала 0,0004 (Hazard rate). Причому, очікувана медіанна тривалість «життя» (Median Life Exp), тобто медіанний час між вчиненням злочину та вироком суду склав 1329 дні.

Аналізуючи наступний часовий інтервал (від 500 до 1000 днів) зауважимо, що число спостережень, по яким було ухвалено обвинувальний вирок суду склало 6 одиниць, проте відносне вираження та ймовірність ухвали обвинувального вироку майже не змінилась. Проте, медіана очікуваної тривалості слідства зменшилась до 1040 днів. Відповідно, за перші 1000 днів від вчинення злочину до вироку суду 80,72 % злочинців не отримають покарання (Cum. Prop. Surviving). Виходячи з цього, система протидії легалізації кримінальних доходів за приблизно 2 роки 9 місяців була ефективною на 19,28%.

Таблиця 5.1 – Значення таблиці «життя» в межах реалізації оцінювання ефективності інституційних змін у системі протидії легалізації кримінальних доходів на основі побудови таблиць виживаності

Interval	Interval Start	Mid Point	Interval Width	Number Entering	Number Withdrwn	Number Exposed	Number Dying	Proportn Dead	Proportn Survivng
A	1	2	3	4	5	6	7	8	9
Int.1	0,00	250,18	500,36	42,0	1	41,5	8	0,193	0,807
Int.2	500,36	750,55	500,36	33,0	0	33,0	6	0,182	0,818
Int.3	1000,73	1250,91	500,36	27,0	0	27,0	10	0,370	0,630
Int.4	1501,09	1751,27	500,36	17,0	2	16,0	6	0,375	0,625
Int.5	2001,46	2251,64	500,36	9,0	2	8,0	5	0,625	0,375
Int.6	2501,82	2752,00	500,36	2,0	0	2,0	0	0,250	0,750
Int.7	3002,18	3252,36	500,36	2,0	0	2,0	0	0,250	0,750
Int.8	3502,55	3752,73	500,36	2,0	0	2,0	0	0,250	0,750
Int.9	4002,91	4253,09	500,36	2,0	0	2,0	0	0,250	0,750
Int.10	4503,27	4753,46	500,36	2,0	1	1,5	0	0,333	0,667
Int.11	5003,64	5253,82	500,36	1,0	0	1,0	0	0,500	0,500
Int.12	5504,00			1,0	1	0,5	0	1,000	0,000

Продовження таблиці 5.1

Interval	Cum.Prop Survivng	Problty Density	Hazard Rate	Std.Err. Cum. Surv	Std.Err. Prob.Den	Std.Err.Haz. Rate	Median Life Exp	Std.Err. Life Exp.
A	10	11	12	13	14	15	16	17
Int.1	1,0000	0,0004	0,0004	0,0000	0,0001	0,0001	1329	158,7629
Int.2	0,8072	0,0003	0,0004	0,0612	0,0001	0,0002	1040	225,4408
Int.3	0,6605	0,0005	0,0009	0,0738	0,0001	0,0003	775	203,9189
Int.4	0,4158	0,0003	0,0009	0,0770	0,0001	0,0004	660	160,1164
Int.5	0,2599	0,0003	0,0018	0,0696	0,0001	0,0007	400	141,5242
Int.6	0,0975	0,0000	0,0006	0,0516	0,0001	0,0008	1223	1257,993
Int.7	0,0731	0,0000	0,0006	0,0489	0,0001	0,0008	1223	1257,9930
Int.8	0,0548	0,0000	0,0006	0,0429	0,0000	0,0008	1168	943,4948
Int.9	0,0411	0,0000	0,0006	0,0363	0,0000	0,0008	1001	707,6210
Int.10	0,0308	0,0000	0,0008	0,0300	0,0000	0,0011	751	612,8178
Int.11	0,0206	0,0000	0,0013	0,0233	0,0000	0,0018	250	500,3636
Int.12	0,0103			0,0155				

Джерело: розроблено автором

Тенденція ухвалення обвинувальних вироків починає змінюватись на 3-5 інтервалах (від 1000 до 2500 днів). Протягом цих періодів частка винесених обвинувальних вироків (для спостережень, по яким раніше не було вироків) склала 0,37, 0,38 та 0,63 для інтервалів 3, 4 та 5 відповідно. Ймовірність ухвали

обвинувального вироку склала 0,0009, 0,0009 та 0,0018 одиниць, а медіанний час між початком вчинення злочину та вироком складе 775, 660 та 400 днів відповідно. Можна очікувати, що протягом 6 років 10 місяців 74% злочинців отримають обвинувальні вироки.

Відповідно до кінця досліджуваного періоду часу залишилось 2 спостереження, обвинувальні вироки по яким не були винесені, тобто розцінюємо ці випадки як виключення. На кожному з інтервалів вони мали схожу ймовірність винесення обвинувального вироку, проте він так і не був винесений.

Третій етап моделювання присвячений дослідженню ефективності інституційних змін у системі протидії легалізації кримінальних доходів на основі методу Каплана-Мейєра.

Результати етапу дослідження ефективності інституційних змін системи у системі протидії легалізації доходів, отриманих незаконним шляхом на основі підходу Каплана-Мейєра (формула 5.5), відображено у таблиці 5.2.

$$S(t) = \prod_{j=1}^{t} \left(\frac{n-j}{n-j-1}\right)^{\delta_j} \qquad (5.5)$$

де S(t) – оцінка функції виживаємості;

n – загальна кількість подій;

$\prod_{j=1}^{t}$ – геометрична сума по всім спостереженням, які завершились до моменту t;

δ_j – дорівнює 1, якщо спостереження містить повну інформацію і дорівнює 0 – якщо не повну;

j – номер спостережень, у ранжованому по порядку зростання кількості днів списку.

В таблиці 5.2 стовпчик Case Number відповідає номерам спостережень, відсортованих у порядку зростання кількості днів, які минули від початку

вчинення злочину до винесення обвинувального вироку судом. Кількість днів зазначена в стовпчику Time. Спостереження з позначкою «+» свідчать про неповноту вхідних даних. Відповідно, спостереження 24 відповідає злочину, від початку вчинення якого до винесення обвинувального вироку пройшло 58 днів, тоді як для спостереження 13 це значення відповідає 2331 день.

Таблиця 5.2 – Результат розрахунків за методом Каплана-Мейєра

Case Number	Time	Cumulatv	Standard	Case Number	Time	Cumulatv	Standard
24	58	0,976	0,024	12	1304	0,491	0,078
1	163	0,952	0,033	33	1372	0,466	0,078
10	210	0,929	0,040	11	1388	0,442	0,078
18	261	0,905	0,045	20	1441	0,417	0,077
6	303	0,881	0,050	9	1540	0,392	0,076
27	351	0,857	0,054	31	1616	0,368	0,075
21	376	0,833	0,058	35+	1658		
22	481	0,810	0,061	4+	1709		
5+	500			19	1805	0,340	0,075
17	516	0,785	0,064	29	1814	0,311	0,074
32	703	0,760	0,066	7	1827	0,283	0,072
14	749	0,736	0,068	38	1978	0,255	0,070
36	816	0,711	0,070	25	2078	0,226	0,068
8	857	0,687	0,072	16	2162	0,198	0,065
40	861	0,662	0,074	15	2241	0,170	0,062
34	1030	0,638	0,075	30	2309	0,142	0,057
26	1042	0,613	0,076	13	2331	0,113	0,053
23	1076	0,589	0,077	41+	2388		
28	1079	0,564	0,077	37+	2400		
2	1079	0,540	0,078	42+	4846		
3	1142	0,515	0,078	39+	5504		

Джерело: розроблено автором

Значення Cumulative Survival відображає ймовірність того, що для будь-якого випадковим чином обраного злочину час між початком вчинення злочину і винесенням обвинувального вироку буде більшим за значення зі стовпця Time.

Для спостереження 24, час якого дорівнює 58, а отже ймовірність того, що винесення обвинувального вироку суду за злочином легалізації незаконних доходів буде більшою за 58 днів дорівнює 97,6%. Ймовірність того, що обвинувальний вирок суду буде винесено за 481 день – 81% (спостереження

22). З ймовірністю 73,6% покарання за злочин настане через 749 днів, тобто понад 2 роки (спостереження 14). Значення стовпчику Standard Error свідчать про незначний розмір похибки, а отже розрахованим значенням можна довіряти.

Зі збільшенням часу між моментом вчинення злочину та моментом винесення обвинувального вироку суду зменшується ймовірність того, що не буде винесено обвинувальний вирок суду, проте процес займає роки.

Четвертий етап науково-методичного підходу оцінювання ефективності інституційних змін у системі протидії легалізації доходів, отриманих незаконним шляхом базується на основі графічного аналізу функції виживання (рисунок 5.6).

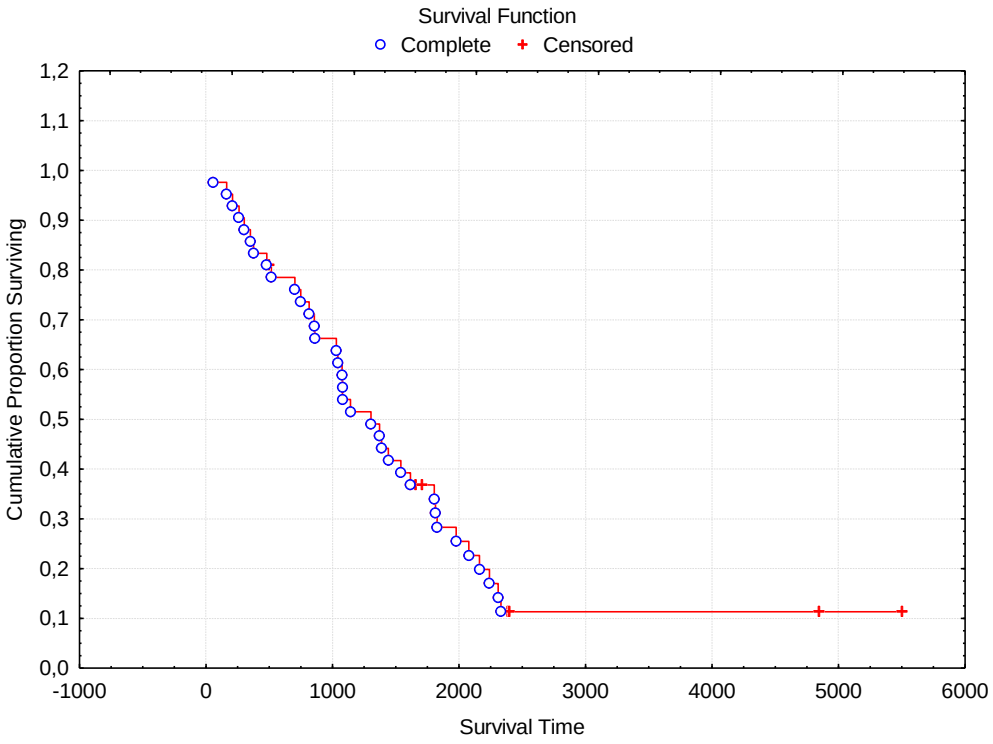


Рисунок 5.6 – Візуалізація залежності ефективності інституційних змін в системі протидії легалізації кримінальних доходів

Джерело: розроблено автором

На рисунку 5.6 графічно відображено отриману залежність. Зі зростанням часу виживання (вісь x) зменшується число не «вижившихх», а отже

збільшується число тих спостережень, за якими було винесено обвинувальний вирок у суді за статтею 209 ККУ «Легалізація (відмивання) доходів, одержаних злочинним шляхом».

В межах п’ятого етапу запропонованого науково-методичного підходу здійснюється аналіз рівномірності розподілу функції виживаності.

Для відображення сутності розподілу ефективності інституційних змін системи протидії легалізації кримінальних доходів відобразимо квартильний розподіл спостережень. Відповідно до рисунку 5.7 25% спостережень охоплюють час «виживання» рівний 723 дні, тобто для 25% злочинів пройде щонайменше 2 роки, поки не буде винесений обвинувальний вирок суду. Другий квартіль, що відповідає медіанній кількості злочинів, пройде приблизно 1242 дні (3 роки і 5 місяців). Для 3 квартилю (75% спостережень) між вчиненням злочину і винесенням обвинувального вироку суду пройде близько 1995 днів (5 років і 6 місяців).

	Percentiles of the Survival Function
Percentiles	Survival Time
25'th percentile (lower quartile)	722,618
50'th percentile (median)	1242,059
75'th percentile (upper quartile)	1994,765

Рисунок 5.7 – Процентілі функції виживання

Джерело: розроблено автором

Відповідно до проведеного дослідження, інституційна складова системи протидії легалізації доходів, отриманих незаконним шляхом потребує вдосконалення. Її трансформація протягом 2015-2021 рр., а саме поява нових державних органів протедії економічним злочинам не призвела до кардинальних змін системи, а головне не відбулось зростання кількості покарань й обсягів повернутих грошей до державного бюджету України. Час, який проходить від початку вчинення злочину з метою легалізації незаконних доходів до винесення судом обвинувального вироку найчастіше триває роками. Розмір інтервалу у таблиці виживання складає 500 днів (1 рік і 4

місяці), при тому що за цей період лише 19,3% кримінальних проваджень завершаться обвинувальним вироком суду. В межах другого інтервалу частка кримінальних проваджень з обвинувальним вироком склала 81,8% від тих проваджень, які залишаться після першого часового інтервалу. Відповідно тільки після того, як мине 2 роки 9 місяців частка закритих проваджень буде складати 37%, а на п'ятому інтервалі досягне 62%. Виходячи з цього, можна стверджувати, що результат діяльності інституційної складової системи протидії легалізації доходів, отриманих незаконним шляхом прослідковується тівльки через 2 роки 9 місяців після того, як злочин буде вчинено.

Згідно з аналізом результатів за методом Каплана-Майєра, зі збільшенням часу між моментом вчинення злочину та моментом винесення обвинувального вироку суду зменшується ймовірність того, що не буде винесено обвинувальний вирок суду, проте процес займає роки. Для спостереження 24, вирок по якому був винесений за 58 днів, ймовірність того, що буде вирок по схожому провадженню складає 2,4%. А для спостереження 22, обвинувальний вирок суду за яким був винесений на 481 день – 19%, для спостереження 14 – 749 днів з ймовірністю 26,4%. Ймовірність винесення обвинувального вироку більше 50% настає тільки для 12 спостереження (50,9%), після того як пройде 1304 дні. Тобто, якщо після вчинення злочину пройде 3 роки 7 місяців, ймовірність винесення обвинувального вироку буде 50,9%.

На основі практичних результатів запропонованного науково-методичного підходу до оцінювання ефективності інституційних змін системи протидії легалізації доходів одержаних незаконним шляхом на основі аналізу виживаності справедливо зауважити наступне. Подальші дослідження повинні бути направлені на детальний аналіз структурих елементів інституційної частини системи протидії легалізації незаконних доходів, щоб виокремити слабкі сторони кожного етапу: фінансового моніторингу, слідства та судової системи. Оскільки неефективна робота будь-якого елементу інституційної складової веде до загальної її неефективності.

5.3 Прогнозування ефективності каналів протидії легалізації кримінальних доходів

Розглядаючи процес протидії легалізації доходів, отриманих незаконним шляхом у вигляді системи, як сукупності взаємопов'язаних елементів доцільно провести його декомпозицію. Це дозволить більш детально розглянути як сам процес легалізації незаконних доходів, так і його складові частини, а також визначити вплив кожної з них на результативний показник. В розрізі процесу прогнозування зазначений підхід дозволяє отримати більш достовірні результати, оскільки кожна зі складових веде себе індивідуально та здійснює особливий вплив на легалізацію кримінальних доходів.

Отже, переходячи безпосередньо до ідентифікації складових частин системи протидії легалізації незаконних доходів, зауважимо, що на наш погляд доцільно виокремити наступні елементи: інституційний, податковий, освітній та інвестиційний канали протидії легалізації доходів, отриманих незаконним шляхом. Саме ці чотири канали охоплюють весь спектр наявного на даний час в Україні впливу на систему протидії легалізації доходів, отриманих незаконним шляхом.

Розглядаючи кожну зі складових більш детально зауважимо, що інституційний канал протидії легалізації є каналом прямого впливу, оскільки охоплює сукупність органів, діяльність яких направлена на виявлення фактів легалізації, їх доведення та притягнення злочинців до відповідальності. Діяльність цього каналу прослідковується після вчинення самого злочину і направлена на відшкодування нанесених злочинцями збитків та демонстрації невідворотності покарання, зменшуючи кількість потенційних злочинців.

Освітній канал протидії легалізації доходів, отриманих незаконним шляхом має опосередкований вплив на процес легалізації, проте нехтувати ним не можна. Освіта має декілька напрямків впливу на процес легалізації кримінальних доходів. По-перше, система освіти формує

висококваліфікованих спеціалістів, які забезпечують функціонування інституційного каналу протидії легалізації. Фахівці з економіки та фінансів необхідні для виявлення фактів легалізації доходів, отриманих незаконним шляхом. Фахівці з права – формують основу органів слідства та судової системи. Окрім цього, фахівці-правники є генеруючим фактором нормативно-правових актів, в тому числі в сфері протидії легалізації кримінальних доходів. По-друге, якісна освіта надає можливість людям реалізувати життєві цілі в легальному секторі суспільного життя, не вдаючись до скоєння злочинів. По-третє, високий рівень освіченості, фінансової грамотності, дозволить законослухняним громадянам стати більш захищеними від злочинців та знизить ризик втягнення їх до злочинів. По-четверте, високий рівень освіченості, знання своїх прав та обов'язків, скоротить рівень корупції, як одного з джерел накопичення доходів, отриманих незаконним шляхом.

Податковий канал протидії легалізації доходів, отриманих незаконним шляхом характеризується декількома факторами. З одного боку – махінації з податками це джерело отримання незаконних доходів як бази для легалізації. І виходячи з цього, потрібно будувати таку систему оподаткування, щоб максимально унеможливити можливості до здійснення податкових афер. З іншого боку – надмірність податкового навантаження, складність у адмініструванні податків штовхає суб'єктів господарювання до тіньових схем своєї діяльності. Як наслідок зростає частина тіньової економіки, в якій накопичуються кошти для легалізації. Сутність податкового каналу протидії легалізації зводиться до розбудови справедливої, зручної системи оподаткування, яка буде спонукати суб'єкти господарювання до чистого та відкритого ведення своєї діяльності. Відтак, зменшуються ризики для суб'єктів господарювання, скорочується обсяг тіньової економіки, і зрештою знижуються обсяги легалізації незаконних доходів.

Інвестиції є основним інструментом транскордонного руху фінансових ресурсів. Частина доходів, отриманих незаконним шляхом маскуються під виглядом інвестицій. Через заплутування джерел походження коштів,

отримання в інвестиційного доходу здійснюється їх легалізація. Інвестиційний канал протидії легалізації доходів, отриманих незаконним шляхом направлений на створення сприятливого інвестиційного клімату, одночасно із забезпеченням прозорості інвестиційного процесу. Виходячи з цього, інвестиції мають контролюватись, проте надмірна бюрократизація процесу інвестування ускладнюватиме їх адміністрування. Інвестиційний канал протидії легалізації має підтримувати баланс між свободою конкурентного інвестиційного ринку та контролем над ризиком легалізації доходів, отриманих незаконним шляхом.

Ефективне управління системою протидії легалізації незаконних доходів передбачає покращення кожного з каналів. Проте, в умовах економічної нестабільності, спричиненої військовими діями чи іншими факторами гостро постає питання раціонального розподілення фінансових та людських ресурсів на забезпечення функціонування держави.

Відповідно до цього, постає питання пріоритизації розподілу наявних ресурсів. Для цього потрібно визначити поточний стан каналів протидії легалізації доходів, отриманих незаконним шляхом та передбачити його розвиток в найближчому майбутньому. Цю задачу дозволяє вирішити інструментарій прогнозування соціально-економічних процесів.

Побудова адекватних прогнозів ефективності каналів протидії легалізації доходів, отриманих незаконним шляхом дозволить визначити слабкі місця в поточний момент часу та в майбутньому, а отже і розподілити ресурси з максимізацією їх ефективності.

Для реалізації поставленої задачі пропонуємо науково-методичний підхід до прогнозування ефективності каналів протидії легалізації доходів, отриманих незаконним шляхом, який складається з п’яти етапів.

Першим етапом науково-методичного підходу виступає збір статистичної бази показників. Основною метою етапу є підбір даних, які релевантно характеризують ефективність кожного з каналів протидії

легалізації доходів, отриманих незаконним шляхом: інвестиційного, податкового, освітнього та інституційного.

Другий етап науково-методичного підходу – попередня обробка даних, тобто їх підготовка до використання в майбутніх етапах. Оскільки зібраний набір містить пропущені значення, їх потрібно обробити шляхом заміщення середнім арифметичним значенням, якщо пропущене значення знаходиться всередині варіаційного ряду (формула 5.6) та за допомогою середнього темпу приросту, якщо пропущене значення знаходиться на початку (формула 5.7) чи на кінці варіаційного рядку (формула 5.8).

$$x_i = \frac{x_{i-1}+x_{i+1}}{2} \tag{5.6}$$

де x_i – пропущене значення варіаційного ряду;

x_{i-1} – попереднє до пропущеного значення варіаційного ряду;

x_{i+1} – наступне за пропущеним значення варіційного ряду.

$$x_1 = \frac{x_2}{\sqrt[n]{\frac{x_n}{x_2}}} \tag{5.7}$$

де x_1– пропущене перше значення варіаційного ряду;

x_n – останнє значення варіаційного ряду;

x_2 – друге значення варіційного ряду4

n – кількість одиниць у варіаційному ряді.

$$x_n = x_{n-1}\sqrt[n]{\frac{x_{n-1}}{x_1}} \tag{5.8}$$

де x_n – пропущене останнє значення варіаційного ряду;

x_{n-1} – попереднє до пропущеного значення варіаційного ряду;

x_1 – перше значення варіаційного ряду;

n – кількість одиниць у варіаційному ряді.

Переходячи до третього етапу науково-методичного підходу прогнозування ефективності каналів протидії легалізації зауважимо, що доцільно його розділити на 3 частини.

5/3.1 Нормалізація вхідних показників

Вхідні показники необхідно стандартизувати, привівши їх до співставного вигляду, натомість відмовившись від одиниць виміру. Для досягнення цієї мети застосуємо природну нормалізацію. Для показників-стимуляторів формула нормалізації набирає вигляду (формула 5.9):

$$x_{i_{norm}} = \frac{x_i - \min\limits_i x}{\max\limits_i x - \min\limits_i x} \tag{5.9}$$

де $x_{i_{norm}}$ – нормалізоване значення ознаки;

x_i –початкове значення ознаки;

$\min\limits_i x$ – мінімальне значення ознаки;

$\max\limits_i x$ – максимальне значення ознаки.

Для показників-дестимуляторів формула природної нормалізації набуває вигляду (формула 5.10):

$$x_{i_{norm}} = \frac{\max\limits_i x - x_i}{\max\limits_i x - \min\limits_i x} \tag{5.10}$$

де $x_{i_{norm}}$ – нормалізоване значення ознаки;

x_i – початкове значення ознаки;

$\min\limits_i x$ – мінімальне значення ознаки;

$\max_i x$ – максимальне значення ознаки.

5/3.2 Визначення вагових коефіцієнтів для інтегральних показників

Для визначення вагових коефіцієнтів для інтегральних показників пропонується скористатись методом аналізу ієрархій Сааті, який передбачає на основі пріоритетності кожного показника над іншим побудову матриці парних порівнянь з подальшою згорткою у ваговий коефіцієнт. Для визначення пріоритетності кожного показника пропонується використання методу головних компонент (формула 5.11).

$$piority_i = \frac{\sum_{j=1}^{n} (v_j * c_{ij})}{\sum_{j=1}^{n} v_j} \quad (5.11)$$

де $piority_i$ – оцінка пріоритетності змінної i;

c_i – внесок змінної i у фактор j;

v_j – % дисперсії, яка пояснюється фактором j;

n – кількість факторів.

Для матриці парних порівнянь ваги k будуть знаходитись в межах від 1..n (де n – кількість змінних), відповідно до проранжованих в порядку зростання $piority_i$.

Матриця парних порівнянь має вигляд (формула 5.12):

$$\frac{k_1}{k_1}\ \frac{k_1}{k_2} \dots \frac{k_1}{k_n}\ \frac{k_2}{k_1}\ \frac{k_2}{k_2} \dots \frac{k_2}{k_n} \dots \dots \dots \dots \frac{k_n}{k_1}\ \frac{k_n}{k_2} \dots \frac{k_n}{k_n} \quad (5.12)$$

Кожен елемент $v_{ij} > 0$, матриці відносних ваг (3.8) є відношенням ваги i-го об’єкту a_i до ваги j-го об’єкту a_j, тобто $v_{ij} = \frac{k_i}{k_j}$ для будь-яких i, j = 1 .. n.

Елементи матриці, що розташовані симетрично до головної діагоналі обернені відповідно один до одного: $v_{ij} = \frac{1}{v_{ji}}$.

Відповідно, матриця 5.12 трансформується у таку матрицю (формула 5.13):

$$v_{11}\, v_{12} \cdots v_{1j}\, v_{21}\, v_{22} \cdots v_{2j} \cdots \cdots \cdots \cdots v_{i1}\, v_{i2} \cdots v_{ij} \qquad (5.13)$$

Вагові коефіцієнти для інтегрального показника ефективності кожного каналу протидії легалізації розраховуються за формулою 5.14:

$$w_i^* = \sqrt[n]{\prod_{j=1}^{n} \quad v_{ij}} \qquad (5.14)$$

$$w_i = \frac{w_i^*}{\sum_{j=1}^{n} \quad w_j^*}$$

де w_i – значення вагового коефіцієнта;

v_{ij} – елементи матриці 5.12;

n – кількість змінних.

5/3.3 Побудова інтегральних оцінок каналів протидії легалізації.

Для реалізації цього етапу пропонується використовувати модифіковану модель Раша (формула 5.15):

$$I_i = \frac{\sum_{i=1}^{n} \quad e^{x_{i_{norm}} * w_i}}{\sum_{i=1}^{n} \quad (e^{x_{i_{norm}}} + 1)} \qquad (5.15)$$

де I_i – інтегральна оцінка і-го значення інтегрального показника відповідного каналу протидії легалізації;

$x_{i_{norm}}$ – нормалізоване значення змінної;

w_i – ваговий коефіцієнт відповідної змінної;

n – кількість спостережень змінної.

Четвертим етапом науково-методичного підходу прогнозування ефективності каналів протидії легалізації доходів, отриманих незаконним шляхом є прогнозування інтегральних оцінок кожного каналу.

Для прогнозування на п’ять років вперед необхідно обрати таку специфікацію моделі, яка буде давати найменшу похибку та забезпечувати статистичну значущість результату.

Для побудови прогнозу ефективності інституційного та інвестиційного каналів пропонується обрати гіперболічний тип залежності, оскільки динаміка даних показників найкраще описується саме цією кривою. Загальний вигляд приведений у формулі 5.16.

$$\hat{y} = \alpha + \frac{\beta}{x} \tag{5.16}$$

де y – значення залежної змінної – інтегрального показника каналу протидії легалізації незаконних доходів;

x – порядковий номер року моделювання;

α, β – коефіцієнти регресії.

Для освітнього каналу притаманна параболічна залежність, тому пропонуємо обрати загальну модель параболічної регресії (формула 5.17):

$$y = \alpha + \beta * x^2 \tag{5.17}$$

де y – значення залежної змінної – інтегрального показника каналу протидії легалізації незаконних доходів;

x – порядковий номер року моделювання;

α, β – коефіцієнти регресії.

Для податкового каналу протидії легалізації незаконних доходів пропонуємо обрати регресію, яка відповідає кореню квадратному (формула 5.18):

$$y = \alpha + \beta * \sqrt{x} \quad (5.18)$$

де y – значення залежної змінної – інтегрального показника каналу протидії легалізації незаконних доходів;

x – порядковий номер року моделювання;

α, β – коефіцієнти регресії.

На п’ятому етапі науково-методичного підходу пропонується узагальнити чотири канали протидії легалізації доходів, отриманих незаконним шляхом, у один інтегральний показник ефективності каналів протидії легалізації доходів, отриманих незаконним шляхом. Для досягнення цієї мети повторимо етап 3, але за вхідні змінні візьмемо інтегральні оцінки каналів протидії легалізації з прогнозними значеннями.

Для реалізації запропонованого науково-методичного підходу оцінки ефективності каналів протидії легалізації доходів, отриманих незаконним шляхом, на першому етапі необхідно зібрати статистичну базу показників, які характеризують ефективність каналів протидії легалізації доходів, отриманих незаконним шляхом.

Інформаційною базою для дослідження виступають показники ефективності каналів протидії легалізації доходів, отриманих незаконним шляхом. Для податкового каналу: Податок на прибуток (% від прибутку) – T1, Час, затрачений на сплату податків (годин на рік) – T2, Податкове навантаження (% від прибутку) – T3, Витрати на реєстрацію власності (% від вартості власності) – T4 та Час, затрачений на реєстрацію власності (днів) – T5. Для інвестиційного каналу: Валове нагромадження капіталу (% від ВВП) – Invest1, Прямі іноземні інвестиції, чистий відтік (% від ВВП) – Invest2, Прямі

іноземні інвестиції, чистий притік (% від ВВП) – Invest3, Чисті портфельні інвестиції (платіжний баланс, поточний дол США) – Invest4, Індекс глобальної конкурентоспроможності (одиниць) – Invest5. Для освітнього каналу: Державні витрати на освіту (% від державних витрат) – E1, Залученість до вищої освіти (од) – E2, Відсоток випускників закладів вищі освіти з програм Бізнес, Адміністрування та Право (%) – E3. Для інституційного каналу: Кількість взятих на облік Державною службою фінансового моніторингу повідомлень (од) – Inst1, Сума грошей, по узагальненим матеріалам, пов'язаних з легалізацією та іншим кримінальним злочином (млн. грн) – Inst2, Сума майна, арештованого та переданого в дохід держави (млн. грн) – Inst3, Кількість кримінальних проваджень, що були відкриті чи набули розвитку з використанням нових матеріалів (од) – Inst4, Кількість обвинувальних актів скерованих до суду (од) – Inst5, Кількість справ з обвинувальним вироком (од) – Inst6. Обраний набір показників характеризує ефективність кожного з каналів протидії легалізації незаконних доходів.

Дані зібрані по Україні за період 2006-2020 рр. з офіційних веб-сайтів: Державної служби фінансового моніторингу, Світового банку, ініціативи Doing Business. Дані наведені в таблицях К.1 та К.2 Додатку К.

Для реалізації другого етапу, застосовуємо формулу 5.6 – для показників Inst2, Inst3, E1, E3, формулу 5.7 – для показників Inst3, Invest5, формулу 5.8 – для показників E2, E3, Invest5. Результат розрахованих пропущених значень наведено у таблицях К.1 та К.2 Додатку К.

Відповідно до третього етапу науково-методичного підходу, проводимо нормалізацію вхідних даних. Для нормалізації показників Inst1, Inst2, Inst3, Inst4, Inst5, Inst6, E1, E2, E3, Invest1, Invest3, Invest4 застосуємо формулу 5.9, оскільки дані показники є стимуляторами, і їх підвищення веде до зростання ефективності каналів протидії легалізації. Для нормалізації показників Invest2, T1, T2, T3, T4 та T5 застосовуємо формулу 5.10, оскільки дані показники є дестимуляторами. Результати розрахунків наведені у таблицях К.3 та К.4 Додатку К.

Наступним кроком, за допомогою методу головних компонент в програмі STATISTICA визначаємо пріоритетні переваги показників.

Для інституційного каналу, задовільний відсоток поясненої дисперсії (>75%) відповідає трьом факторам (рисунок 5.8). Графік кам'янистого осипу (рисунок 5.9) підтверджує необхідність виділення трьох факторів, оскільки після третього фактору кут нахилу лінії помітно змінюється.

	Eigenvalues of correlation matrix, and related statistics Active variables only			
Value number	Eigenvalue	% Total variance	Cumulative Eigenvalue	Cumulative %
1	2,468058	41,13429	2,468058	41,1343
2	1,590457	26,50762	4,058515	67,6419
3	0,919292	15,32153	4,977807	82,9634
4	0,468319	7,80532	5,446126	90,7688
5	0,296866	4,94777	5,742992	95,7165
6	0,257008	4,28347	6,000000	100,0000

Рисунок 5.8 – Власні значення і відсоток поясненої дисперсії за методом головних компонент для інституційного каналу

Джерело: розроблено автором

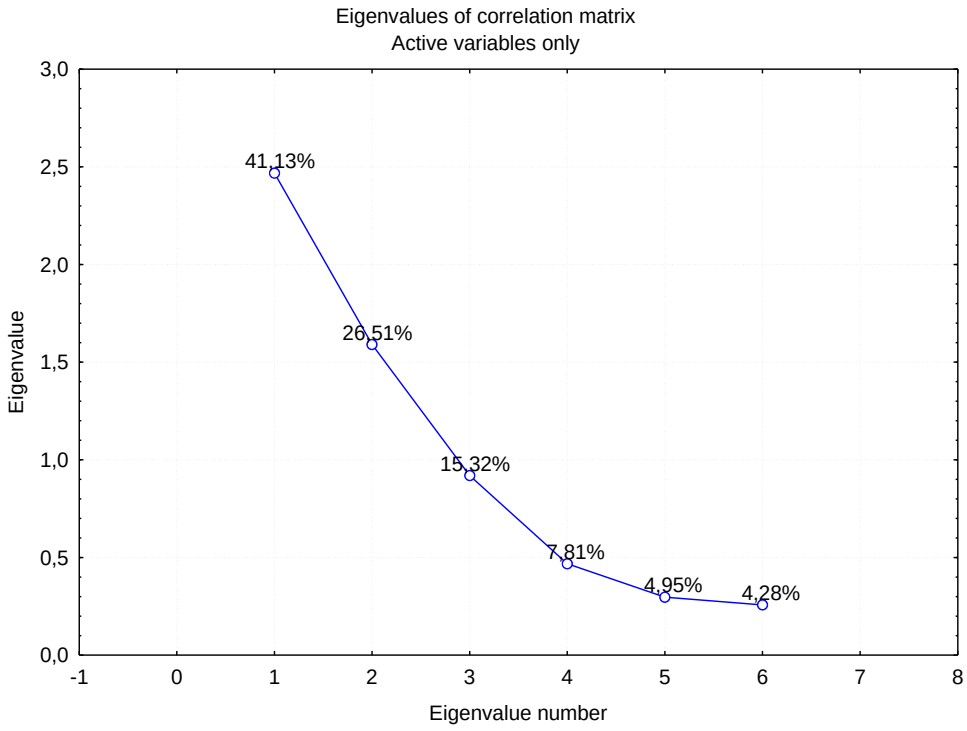


Рисунок 5.9 – Графік кам'янистого осипу для інституційного каналу

Джерело: розроблено автором

Відповідно необхідні для розрахунку пріоритетів внески змінних відображені на рисунку 5.10 та відповідають графам Factor 1, Factor 2 та Factor 3. Розраховані за формулою 5.11 оцінки пріоритетів наведені у таблиці 5.3 графі 1.

	Variable contributions, based on correlations					
Variable	Factor 1	Factor 2	Factor 3	Factor 4	Factor 5	Factor 6
Inst1	0,080267	0,341159	0,000542	0,511681	0,053113	0,013238
Inst2	0,072481	0,271374	0,318533	0,046882	0,000080	0,290650
Inst3	0,062151	0,187256	0,466303	0,220730	0,010264	0,053297
Inst4	0,268222	0,098456	0,000058	0,069028	0,101066	0,463170
Inst5	0,254744	0,064514	0,096655	0,078884	0,326964	0,178240
Inst6	0,262134	0,037241	0,117909	0,072795	0,508514	0,001405

Рисунок 5.10 – Внески змінних у кожен фактор для інституційного каналу

Джерело: розроблено автором

Таблиця 5.3 – Оцінки пріоритетів, матриця парних порівнянь та вагові коефіцієнти для інституційного каналу

priority	Показник	Inst1	Inst2	Inst3	Inst4	Inst5	Inst6	w
1	2	3	4	5	6	7	8	9
0,1489	Inst1	1,00	0,14	0,17	0,20	0,25	0,33	0,0311
0,1815	Inst2	7,00	1,00	3,00	4,00	5,00	6,00	0,4238
0,1768	Inst3	6,00	0,33	1,00	3,00	4,00	5,00	0,2552
0,1645	Inst4	5,00	0,25	0,33	1,00	3,00	4,00	0,1502
0,1648	Inst5	4,00	0,20	0,25	0,33	1,00	3,00	0,0879
0,1636	Inst6	3,00	0,17	0,20	0,25	0,33	1,00	0,0517

Джерело: розроблено автором

Застосовуючи формули 5.12 та 5.13 будуємо матрицю парних порівнянь Сатті (графи 2-8 таблиці 5.3).

Для розрахунку вагових коефіцієнтів інтегрального показника ефективності інституційного каналу протидії легалізації незаконних доходів, скористаємось формулою 5.14. Результати розрахунку наведені у графі 9 таблиці 5.3.

Розрахунки для освітнього, податкового та інвестиційного каналів протидії легалізації доходів, отриманих незаконним шляхом наведені на рисунках В.1-В.9 та в таблицях К.5-К.7 Додатку К.

Для розрахунку інтегральних показників оцінювання ефективності каналів протидії легалізації незаконних доходів скористаємось формулою 5.15. Результати розрахунків наведені у таблиці 5.4 та на рисунку 5.11

Таблиця 5.4 – Інтегральні показники

Рік	Інституційний канал (IC)	Освітні канал (EC)	Інвестиційний канал (INV)	Податковий канал (TC)
2006	0,49930	0,40149	0,37433	0,49772
2007	0,48048	0,40177	0,40455	0,46780
2008	0,44073	0,40865	0,38846	0,46626
2009	0,40575	0,38496	0,37751	0,42289
2010	0,44892	0,40641	0,43860	0,41328
2011	0,44916	0,42685	0,40913	0,42087
2012	0,41692	0,41587	0,43368	0,42913
2013	0,37930	0,41755	0,40838	0,40497
2014	0,39977	0,43456	0,40448	0,37555
2015	0,44258	0,43418	0,37843	0,35325
2016	0,42028	0,45359	0,39204	0,34546
2017	0,41494	0,48930	0,39110	0,34222
2018	0,41779	0,45487	0,40445	0,34498
2019	0,40123	0,45298	0,44012	0,34686
2020	0,46135	0,45595	0,41913	0,34529

Джерело: розроблено автором

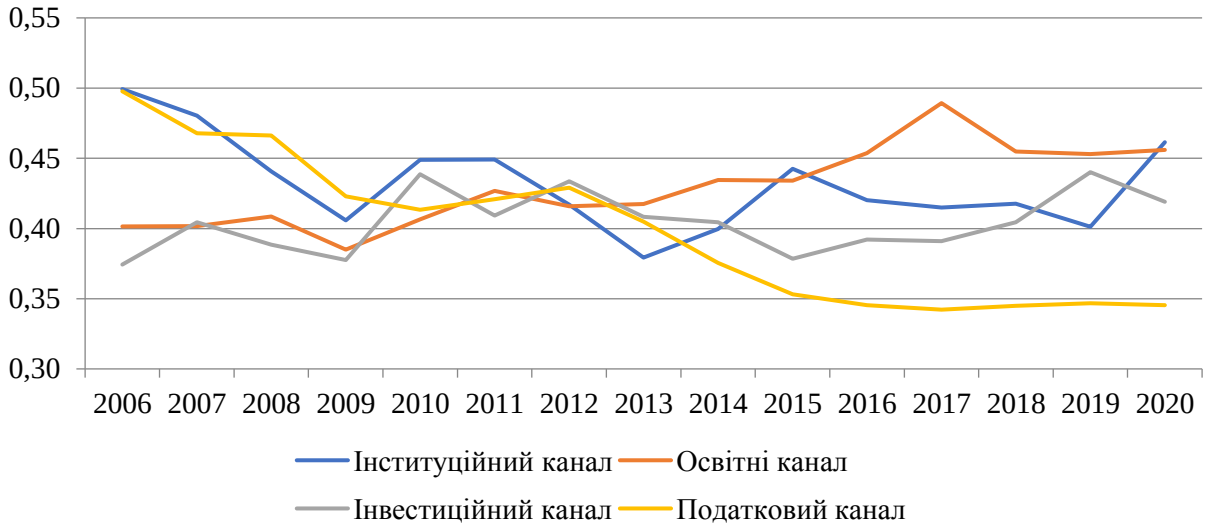


Рисунок 5.11 – Інтегральні показники каналів протидії легалізації

Джерело: розроблено автором

Відповідно до даних зображених на рисунку 5.11, можемо простежити динаміку зміни ефективності каналів протидії легалізації з 2006 по 2020 роки.

З 2009 по 2014 рік ефективність каналів коливалась на одному рівні, а після 2014 року можна простежити розкид ефективності каналів протидії легалізації. Розбіжності в ефективності каналів пояснюються активним впровадженням реформ в Україні після подій 2013-2014 років. Модернізація системи слідчих органів, які є частиною інституційного каналу відображуються у стрибок росту ефективності даного каналу після 2019 року.

Важливо зауважити, що зростання ефективності освітнього каналу протидії легалізації. Зростання фінансової грамотності, збільшення частки висококваліфікованих працівників з вищою освітою позитивно впливають на протидію легалізації незаконних доходів.

Для реалізації четвертого етапу науково-методичного підходу прогнозування ефективності каналів протидії легалізації доходів, отриманих незаконним шляхом, скористаємось модулем Fixed Nonlinear Regression програми STATISTICA.

Результати побудови нелінійної регресії для інституційного каналу наведені на рисунку 5.12.

	Regression Summary for Dependent Variable: IC R= ,70878241 R?= ,50237251 Adjusted R?= ,46409347 F(1,13)=13,124 p<,00309 Std.Error of estimate: ,02382					
N=15	Beta	Std.Err. of Beta	B	Std.Err. of B	t(13)	p-level
Intercept			0,411153	0,008403	48,92913	0,000000
1/IC	0,708782	0,195650	0,093783	0,025888	3,62270	0,003095

Рисунок 5.12 – Результати регресії для інституційного каналу

Джерело: розроблено автором

Відповідно до рисунку 5.12, формула 5.16 набуває вигляду (формула 5.19):

$$\widehat{IC} = 0{,}411 + \frac{0{,}094}{t} \qquad (5.19)$$

Адекватність розрахованої моделі підтверджується: стандартна похибка мала та рівна 0,024, значення F-критерію Фішера (13,124) свідчить про істотність моделі, а p-level < 0,05 свідчить про статистичну значущість результату при рівні довіри 95%.

Для інвестиційного каналу (рисунок К.10 Додатку К), формула 5.16 набуває вигляду (формула 5.20):

$$\widehat{INV} = 0{,}412 - \frac{0{,}036}{t} \tag{5.20}$$

Стандартна похибка моделі дорівнює 0,020, проте значення p-level = 0,124 та значення F-критерію Фішера (2,705) не дозволяють стверджувати про статистичну значущість результату при рівні довіри 95%. Дана модель є адекватною при рівні довіри 85%: F_{85} (2,34) < F (2,705). Тому приймаємо її зі значенням рівня довіри 85%.

Для освітнього каналу (рисунок К.11 Додатку К), формула 5.17 набуває вигляду (формула 5.21):

$$\widehat{EC} = 0{,}403 + 0{,}00032 * t^2 \tag{5.21}$$

Стандратна похибка для побудованої моделі дорівнює 0,015, p-level < 0,05, що свідчить про статистичну значущість отриманого результату. Значення F-критерію Фішера (33,018) з p<0,05 свідчить про адекватність моделі.

Для освітнього каналу (рисунок К.12 Додатку К), формула 3.18 набуває вигляду (формула 5.22):

$$\widehat{TC} = 0{,}554 - 0{,}057 * \sqrt{t} \tag{5.22}$$

Відповідно до значень стандартної похибки, яка дорівнює 0,014, F-критерію Фішера та t-статистиці Стьюдента, значення p-value для яких <0,05,

приходимо до висновку, що побудована модель є адекватною при рівні довіри 95% та може бути застосована для прогнозування. Прогнозні значення моделі наведені у таблиці 5.5.

Таблиця 5.5 – Прогнозні значення інтегральних показників ефективності каналів протидії легалізації доходів, отриманих незаконним шляхом.

Рік	Інституційний канал (IC)	Освітні канал (EC)	Інвестиційний канал (INV)	Податковий канал (TC)
2021	0,41702	0,48504	0,41004	0,32357
2022	0,41667	0,49566	0,41017	0,31649
2023	0,41636	0,50692	0,41029	0,30662
2024	0,41609	0,51882	0,41040	0,30293
2025	0,41584	0,53137	0,41049	0,29642

Джерело: розроблено автором

Для наочного зображення отриманих результатів побудуємо графік прогнозні значення інтегральних показників ефективності каналів протидії легалізації доходів, отриманих незаконним шляхом (рисунок 5.13).

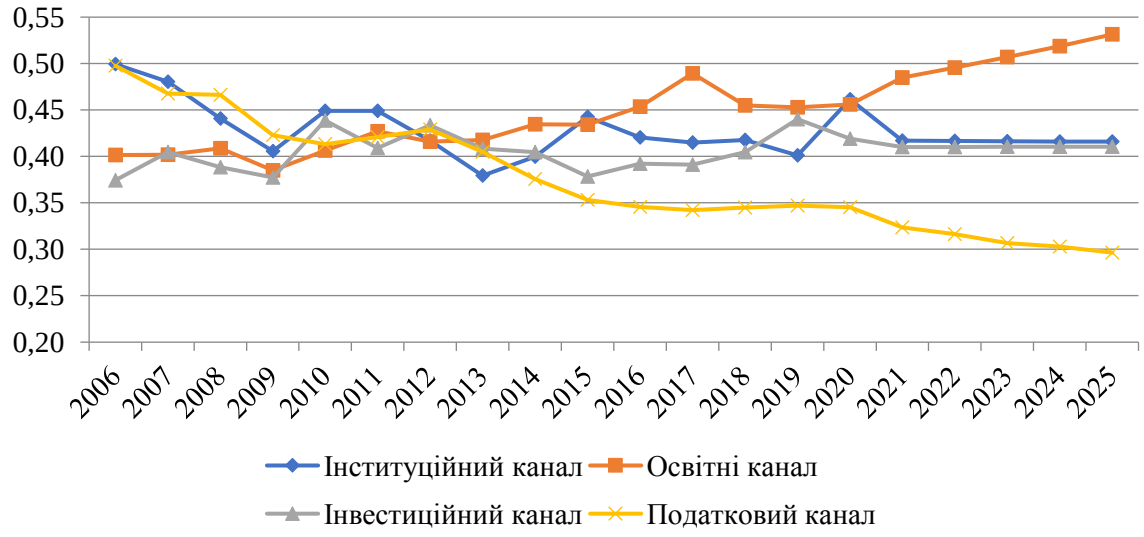


Рисунок 5.13 – Прогнозні значення інтегральних показників ефективності каналів протидії легалізації доходів, отриманих незаконним шляхом

Джерело: розроблено автором

Відповідно до отриманих прогнозних значень (таблиця 5.3, рисунок 5.13), можемо зробити висновок, що ефективність інституційного та інвестиційного каналів протидії легалізації доходів, отриманих незаконним шляхом до 2025 року буде майже сталою. Проте, інвестиційний канал зберігає позитивну динаміку росту, тоді як ефективність інституційного каналу буде поступово знижуватись. Ефективність освітнього каналу протидії легалізації незаконних доходів в період 2020-2025 рр. буде збільшуватись, а ефективність податкового каналу має тенденцію до зниження.

Відповідно до отриманих результатів, потребує модернізації податковий канал протидії легалізації доходів, отриманих незаконним шляхом, оскільки протягом всього досліджуваного періоду його ефективність постійно знижується, і очікувано буде знижуватись надалі.

Переходячи до п’ятого етапу науково-методичного підходу прогнозування ефективності каналів протидії легалізації доходів, отриманих незаконним шляхом, побудуємо матрицю парних порівнянь Сааті для визначення вагових коефіцієнтів загального інтегрального показника ефективності каналів протидії легалізації незаконних доходів (формули 5.13-5.14). Матриця Сааті наведена у таблиці 5.6.

Таблиця 5.6 – Оцінки пріоритетів, матриця парних порівнянь та вагові коефіцієнти для інституційного каналу

priority	Показник	Інституційний канал	Освітній канал	Інвестиційний канал	Податковий канал	w
1	Інституційний канал	1,00	4,00	3,00	2,00	0,393
4	Освітній канал	0,25	1,00	0,50	0,33	0,136
3	Інвестиційний канал	0,33	2,00	1,00	0,50	0,193
2	Податковий канал	0,50	3,00	2,00	1,00	0,278

Джерело: розроблено автором

Для розрахунку інтегрального показника оцінювання ефективності каналів протидії легалізації незаконних доходів скористаємось формулою

5.13. Результати розрахунків наведені у таблиці К.8 Додатку К та на рисунку 5.14.

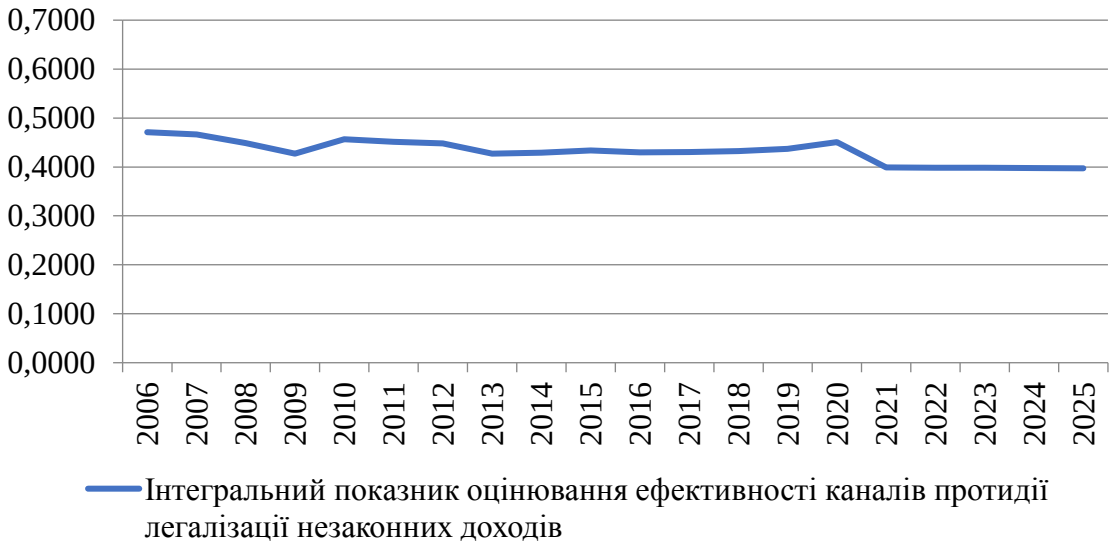


Рисунок 5.14 – Інтегральний показник оцінювання ефективності каналів протидії легалізації незаконних доходів

Джерело: розроблено автором

Відповідно до таблиці В.8 та рисунку 5.14, можна стверджувати про спадну тенденцію ефективності каналів протидії легалізації незаконних доходів, а саме спостерігається падіння показника після 2021 році на 0,052 пункти, а далі очікується зниження на 0,0004 одиниці кожного року. Незначне зниження свідчить про стабільну ефективність каналів протидії легалізації доходів, отриманих незаконним шляхом. Проте, дана стабільність забезпечується нівелюванням спаду ефективності податкового каналу ростом ефективності освітнього каналу, тоді як інституційний та інвестиційний канали мають сталу ефективність.

Податковий канал протидії легалізації характеризується значним податковим навантаженням, що спричиняє ріст тіньової економіки та стимулює накопичення незаконних доходів. Окрім цього, затрачений на сплату податків час, який рівний 41 робочому 8-ми годинному дню на рік також може бути оптимізований, шляхом запровадження цифрових рішень та спрощення процедур сплати податків.

Отже, за відсутності втручання у функціонування каналів протидії легалізації доходів, отриманих незаконним шляхом загальна ефективність системи протидії буде поступово зменшуватись. Окрім цього, побудована модель не враховує впливу соціально-економічних збурень, які стались в наслідок пандемії covid-19 та повномасштабного вторгнення росії в Україну, розміри впливу останнього наразі неможливо повністю оцінити.

Відповідно, щоб забезпечити ефективність функціонування системи протидії легалізації доходів, отриманих незаконним шляхом в першу чергу потрібно зосередитись на податковому каналі: зменшити податкове навантаження та складність адміністрування податків. Після чого доцільно продовжити реформування інституційного каналу.

5.4 Дорожня карта реформ національної системи протидії легалізації доходів одержаних незаконним шляхом

В умовах активної імплементації цифрових технологій в усі сфери соціально-економічного життя, вплив діджиталізації має бути враховано у процесі реформування системи протидії легалізації доходів. Широкомасштабна цифровізації, з одного боку, призвела до появи нових фінансових інструментів, які дозволяють легалізовувати доходи, отриманих незаконним шляхом, швидко та залишаючи при цьому мінімум цифрових слідів. Разом з тим, з іншого боку, активна діджиталізація економіки призводить до зростання масштабів фіксації фінансових операцій та мережі охоплення економічних агентів цифровими послугами, що ускладнює процес непомітної легалізації доходів, отриманих незаконним шляхом. Крім того, бурхливий розвиток цифрових технологій вимагає перманентної актуалізації можливих векторів реформування системи протидії легалізації доходів, отриманих незаконним шляхом, адже в умовах діджиталізації економіки майже кожного дня з’являються як нові ризики та загрози зростання масштабів

легалізації доходів, так і нові механізми стримування та протидії цим процесам.

Варто зауважити, що з рівнем лояльності фінансово-економічної системи до легалізації кримінальних доходів, отриманих злочинним шляхом, тісно пов'язані параметри диференціації деструктивного впливу пандемії COVID-19 на показники забезпечення національної безпеки держави. Цей причинно-наслідковий зв'язок значно пов'язаний з ухиленням від сплати податків та нелегальним наймом працівників, що в умовах викликів пандемії COVID-19 пов'язано зі зниженням ліквідності та рентабельності бізнесу, скороченням оплати праці, широкомасштабним вивільненням робочої сили через обмеження, спричинені локдауном. З одного боку, така нерегульована економічна діяльність може призвести до зменшення податкових надходжень, зниження податкової моралі та недотримання податкового законодавства, зростання лояльності суб'єктів економічних відносин до легалізації доходів, отриманих злочинним шляхом, збільшення витрат на контроль ухилення від сплати податків та зниження темпів економічного зростання. Крім того, зайнятість у нелегальній економічній діяльності з подальшою легалізацією отримуваних доходів, як правило, не передбачає імплементації схем соціального захисту працівників чи їх медичного страхування на випадок захворювання від COVID-19. Таким чином, передумови та наслідки легалізації доходів, отриманих злочинним шляхом, поширюються за межі економіки на охорону здоров'я та політичну систему. Для розробки політичних заходів, які відповідають рівню розвитку кожної країни та вразливості до COVID-19, необхідний аналіз причин і наслідків зростання лояльності суб'єктів економічних відносин до легалізації доходів, отриманих злочинним шляхом. Представників інституційного середовища повинні розглядати тренди до збільшення лояльності суб'єктів економічних відносин до легалізації доходів, отриманих злочинним шляхом, неофіційну зайнятість та ухилення від сплати податків як сигнал про необхідність покращення якості систем регулювання та державного управління, поліпшення стану підзвітності, публічності та

прозорості інституційного середовища, оптимізації податкової системи, кращого рівня фінансового моніторингу у контексті ризикових фінансових операцій, що мають підвищений ризик легалізації кримінальних доходів, отриманих злочинним шляхом.

Варто зазначити, що в умовах пандемії COVID-19 відбулося посилення регуляторного тиску на економічних агентів у сфері зайнятості, міграційних процесів, функціонування ринків товарів і послуг, що виступило тригером до переходу до «сірого» сегменту економічної системи і, як наслідок, подальшої необхідності легалізувати отримані від цієї економічної діяльності доходи. Інтенсифікації діджиталізації фінансових ринків, зокрема, активний розвиток ринків криптовалют, полегшили можливості легалізації доходів, отриманих злочинним шляхом (криптовалюти можна використовувати з розумним ступенем анонімності на десятках ринків у darknet). Ці ринки надають людям доступ до товарів і послуг, які є незаконними (наприклад, наркотики), суворо регульованими (наприклад, ліки, що відпускаються за рецептом) або дефіцитними (наприклад, маски для обличчя).

Пандемія COVID-19 призвела і до трансформації схем легалізації доходів. Так, змінилися схеми фішингу через SMS та електронні листи, пов’язані з COVID-19. Тепер це електронні листи з підробленими посиланнями на пакети державної фінансової допомоги, банків, що розподіляють допомогу тощо. Таким чином, цілком справедливо, що у контексті відновлення національної безпеки у період після пандемії COVID-19 важливе значення має адаптація систем протидії легалізації доходів та зниження рівня тіньової економіки до нових викликів, спричинених пандемією COVID-19.

Отже, на рисунку 5.15 представлено дорожню карту реформування системи протидії легалізації доходів, отриманих незаконним шляхом, в умовах діджиталізації економіки та появи нових викликів сучасних світогосподарських відносин. Дорожня карта побудована як з рахуванням різноплановості проявів процесів протидії легалізації доходів, що виявляються

у низці проблемних аспектів системи, так і різновекторності впливу діджиталізації на процес протидії легалізації незаконних доходів. Інтеграція у єдину систему проблемних аспектів у сфері протидії легалізації незаконних доходів та заходів, що сприятиму їх нівелювання, що у тому числі мають діджитальну природу, дозволить досягнути низки позитивних результатів.

У контексті формалізації напрямків протидії легалізації незаконних доходів, можна виділити наступні три найважливіші складові: превентивний, комунікаційно-конгруентний та розслідувально-каральний. Так, у межах превентивного напрямку зосереджено ті проблемні аспекти системи та потенційні шляхи їх вирішення, що спрямовані на нівелювання зацікавленості економічних агентів до акумулювання незаконно отриманих доходів та їх подальшої легалізації. Комунікаційно-конгруентний напрямок передбачає визначення «вузьких місць» та розроблення заходів щодо їх усунення у сфері взаємодії та субординації між складовими інституційного середовища протидії легалізації незаконних доходів, а також налагодження та нівелювання прогалин у межах міжнародної співпраці у цьому напрямку. Розслідувально-каральний напрямок характеризує проблеми та шляхи їх усунення на тому етапі, коли запобігти чи попередити легалізацію незаконних доходів не вдалося, проте виникає необхідність формування якісної доказової бази складу злочину та винесення справедливого обвинувального вироку, зведення до мінімуму можливостей уникнення економічними агентами покарання за порушення законодавства у сфері легалізації кримінальних доходів. Разом з тим, ця система має бути побудована не на засадах обов’язкового пошуку «винних», а на професійному розслідуванні та справедливому покарані.

Отже, характеризуючи превентивний напрямок реформування системи протидії легалізації доходів, отриманих незаконним шляхом, в умовах діджиталізації економіки можна відмітити, що однією з важливих проблем системи є надмірне фокусування окремих інституцій на контрольній і каральній функціях, тоді як практично не вживаються заходи щодо попередження та усунення на етапі формування ризиків акумулювання

незаконних доходів та їх подальшої легалізації. Таким чином, до превентивного напрямку дорожньої карти реформування системи протидії легалізації доходів, отриманих незаконним шляхом, можна віднести переважно заходи економічного впливу.

Зокрема, однією з основоположних причин вимушеного здійснення незаконної господарської діяльності є недостатність ліквідних засобів для виконання податкових зобов'язань, або критично низька рентабельність бізнесу після сплати всіх платежів та податків. Надмірне податкове навантаження підриває засади партнерських відносин між державою та бізнесом. Таким чином, Державна податкова служба України значно меншою мірою виконує сервісну функцію, супроводжуючи процес адміністрування податків та задовольняючи індивідуально інформаційно-консультативні запити платників податків, а набагато більш широко виконує контрольну функцію, виступаючи при цьому як «watchdog», що має на меті виявити якомога більше кейсів порушення норм законодавства у сфері оподаткування та застосувати до «недобросовісних» платників податків відповідні санкції та стягнення. Занадто суворий контрольно-регуляторний тягар спонукає суб'єктів господарювання до уникнення оподаткування та ухилення від сплати податків. Зокрема, найбільш вразливою групою економічних агентів у цьому випадку є фізичні особи-підприємці, на яких покладено обов'язок щодо сплати єдиного податку навіть у випадку фактичної відсутності господарської діяльності.

З урахуванням визначених вище закономірностей, з метою недопущення застосування схем легалізації доходів, отриманих незаконним шляхом, варто розробити зміни до Податкового кодексу України та супутніх нормативно-правових актів, спрямованих на ефективне зниження рівня податкового навантаження на засадах збалансування економічних інтересів держави та бізнесу, а також розширення спектру дії податкової амністії. Наразі податкова амністія забезпечує можливість легалізувати активи, при придбанні яких не були сплачені податки і збори або сплачені не в повному обсязі, що дозволяє

суб’єкту уникнути фінансової, адміністративної та кримінальної відповідальності за умови погашення своїх зобов’язань перед державою. Для зниження рівня легалізації доходів, отриманих незаконним шляхом, доцільно розширити дію податкової амністії на доходи, отримані з порушенням інших норм вітчизняного законодавства, але з умовою не повторювати це правопорушення щонайменше протягом дії терміну позовної давності – 1095 днів – у випадку скоєння аналогічного правопорушення протягом 1095 днів суб’єкт повинен буде понести відповідальність як за цей злочин, так і за попередній. Скориставшись правом податкової амністії, особа декларує свої незаконні активи, сплачує суму податкового зобов’язання та передає інформацію про факти злочинів. Правоохоронні органи беруть під контроль діяльність цієї особи в подальшому, проте звільняють від відповідальності за вчинений злочини, до якого було застосовано амністію. Дія цього положення має поширюватися лише не легкі злочини та частково злочини середньої тяжкості.

В окремих випадках можливе несвідоме залучення легально діючих суб’єктів економіки до участі у схемах легалізації доходів, отриманих незаконним шляхом, через недобросовісних контрагентів, що обумовлено недостатньою поінформованістю цих суб’єктів про такі ризики, прогалинами у сфері фінансової та податкової грамотності, відсутністю доступу до інформації про недобросовісних контрагентів. З метою превенції цих кейсів у межах реформування системи протидії легалізації кримінальних доходів запропоновано активно поширювати програми покращення рівня фінансової та податкової грамотності. Зокрема, з урахуванням найбільш частих та нагальних питань, що платники податків задають через Загальнодоступний інформаційно-довідковий ресурс, а також з урахуванням найбільш поширених помилок, виявлених контролюючими органами у ході податкових перевірок, Державній податковій службі України спільно з Міністерством фінансів України (як органом виконавчої влади, уповноваженим на надання узагальнюючих податкових консультацій) запропоновано активно

використовувати не лише інструмент індивідуальних та узагальнюючих податкових консультацій, а проводити загальнодоступні спільні просвітницько-інформаційні вебінари з податкової грамотності, сфокусувавши увагу на найбільш проблемних аспектах.

У контексті нівелювання ризиків ненавмисної участі легальних суб'єктів економіки в операціях з легалізації доходів, отриманих незаконним шляхом, важливим напрямком реформування є створення єдиного реєстру / бази даних / платформи ідентифікації недобросовісних контрагентів, який буде містити як ту інформацію, що вже є у відкритих реєстрах (Opendatabot, YouControl, E-tender, Єдиний державний реєстр судових рішень, Єдиний реєстр боржників тозт), так і, зокрема, інформацію щодо порушення суб’єктом господарювання законодавства у сфері нарахування та сплати ПДВ (за аналогією до «білого» списку платників ПДВ, що створено у Польщі), історію виникнення та погашення в економічного агенту податкового боргу, історію судових позовів до контрагента тощо. Попри те, що на сьогоднішній день значний обсяг інформації, за яким можна зробити висновок про добросовісність контрагента є у публічному доступі чи може бути отримана на платній основі, проте узагальнення та аналіз цієї інформації потребує певної обізнаності та кваліфікації, а також може зайняти чимало часу. Саме тому створення єдиної платформи, реєстру чи бази даних, з якої після нескладної верифікації можна буде отримати комплексну інформацію про історія діяльності суб’єкта господарювання, по-перше, буде виступати ефективним стримуючим механізмом до участі в нелегальній господарській діяльності, а по-друге, дозволить менш досвідченим учасникам ринку уникнути неумисної участі в операціях з легалізації доходів, отриманих незаконним шляхом, через недобросовісних контрагентів.

У контексті характеристики комунікаційно-конгруентного напрямку реформування системи протидії легалізації доходів, отриманих незаконним шляхом, важливо ідентифікувати ті проблемні аспекти, що стосуються взаємодії всередині інституційного середовища системи протидії легалізації

доходів, отриманих незаконним шляхом, підзвітності, публічності та прозорості роботи цих інституцій, а також міжнародної співпраці у цьому напрямку з побудовою ефективної системи оперативного обміну інформацією щодо осіб, залучених до схем легалізації доходів.

Зокрема, за результатами SWOT-аналізу якості функціонування системи протидії легалізації доходів, отриманих незаконним шляхом, виявлено, що однією з нагальних проблем у розрізі комунікаційно-конгруентного напрямку є недосконалий розподіл повноважень та неефективна комунікація інституцій в системі протидії легалізації доходів, отриманих незаконним шляхом. Зокрема, варто зауважити, що ключовим суб'єктом інституційного середовища системи протидії легалізації доходів, отриманих незаконним шляхом, є Державна служба фінансового моніторингу України, проте виявленню кейсів схем легалізації доходів може сприяти тісна кооперація з такими інституціями як Державна податкова служба України, Міністерство фінансів України, Бюро економічної безпеки України, Національне антикорупційне бюро України, органи внутрішніх справ та ін. Разом з тим, цілком очевидною є проблема відсутності ефективної комунікації між цими органами, адже фактично кожен з них реалізує індивідуальний вектор фінансової чи економічної політики, тоді як синхронізації та синергія зусиль у цьому напрямку дозволило б досягти значно кращих позитивних результатів.

Таким чином, для вирішення цієї проблеми пропонується розроблення та імплементація стратегії обміну інформацією на різних рівнях з періодичним проведенням комунікаційних заходів. Зокрема, кооперація зусиль Бюро економічної безпеки України, Державної служби фінансового моніторингу України, Державної податкової служби України, Міністерства фінансів України та ін., а також науковців, які здійснюють якісні та комплексні дослідження у цьому напрямку, дозволить розширити типологізацію схем легалізації доходів, отриманих незаконним шляхом, з урахуванням аналізу не лише фінансових операцій, а й злочинів, що передували легалізації доходів. Крім того, варто перманентно та періодично організовувати конференції та

круглі столи, на яких будуть обговорюватися сучасні напрацювання у цьому напрямку та проводитися обмін кращими практиками та підходами до виявлення легалізаційних схем. Такі комунікаційно-конгруентні заходи мають, перш за все, реалізовуватися за принципом «закритого клубу» між фахівцями інституційного середовища системи протидії легалізації доходів, отриманих незаконним шляхом, проте окремі просвітницькі заходи повинні здійснюватися і для співробітників служб фінансового моніторингу фінансових посередників з метою підвищення кваліфікації їх персоналу для виявлення схем легалізації доходів, отриманих злочинним шляхом, та протидії ним.

Сучасні умови цифровізації суспільства також дозволяють вивести на новий рівень комунікативну співпрацю з міжнародними організаціями щодо протидії легалізації доходів, отриманих злочинним шляхом. Так, організація онлайн-конференцій між Комітетом експертів Ради Європи з оцінки заходів протидії відмиванню коштів та фінансуванню тероризму (MONEYVAL), Групи розробки фінансових заходів боротьби з відмиванням грошей (FATF), Державною службою фінансового моніторингу України, Бюро економічної безпеки України, Національним банком України сприятиме обміну знаннями та напрацюваннями щодо протидії легалізації незаконних доходів. Важливим вектором покращення ефективності функціонування системи протидії легалізації доходів, отриманих злочинним шляхом, є також створення онлайн та оффлайн курсів підвищення кваліфікації працівників відділів фінансового моніторингу банків, детективів Бюро економічної безпеки України з метою ознайомлення з новими схемами легалізації доходів, отриманих незаконним шляхом, змін в законодавстві по боротьбі з легалізацією незаконних доходів.

Важливими вектором вирішення проблеми неефективності обміну інформацією у сфері протидії легалізації доходів, отриманих злочинним шляхом, є створення єдиної бази даних у сфері протидії легалізації доходів, отриманих незаконним шляхом.

До стандартизованої системи є можливість інтегрувати державні реєстри, використання яких значно посилить політику «Знай свого клієнта». Важлива інформація з точки зору перевірки добросовісності клієнта може знаходитись у реєстрах: Єдиний державний реєстр осіб, які вчинили корупційні або пов'язані з корупцією правопорушення, Реєстр платників ПДВ, Єдиний ліцензійний реєстр, Єдиний державний реєстр судових рішень, Єдиний державний реєстр юридичних осіб та фізичних осіб-підприємців, База даних втрачених паспортів, Зниклі громадяни, Єдиний реєстр бюро кредитних історій, Перелік осіб, пов`язаних із здійсненням терористичної діяльності або стосовно яких застосовано міжнародні санкції, База даних експортерів, Єдиний державний реєстр виконавчих проваджень, Перелік організацій-виконавців, які заявили право на податкові пільги, Перелік суб'єктів господарської діяльності, що мають ліцензію на діяльність з випуску та проведення лотерей, Реєстр ліцензіатів, яким дозволена діяльність у сфері збору, обробки, переробки відходів дорогоцінних металів і дорогоцінного каміння, Електронна система розкриття інформації учасників фондового ринку ЕСКРІН, Реєстр дозволів на міжнародні перевезення, Дізнайся більше про свого бізнес-партнера, Реєстри учасників фондового ринку, Реєстри учасників фондового ринку, Реєстр підприємств, яким надано дозвіл на відкриття та експлуатацію митного складу, Єдиний реєстр розпорядників бюджетних коштів та одержувачів бюджетних коштів тощо. Автоматизоване використання інформації з даних реєстрів дозволить підтвердити чи спростувати подану клієнтом інформацію, встановивши для нього відповідний рівень ризику.

У сфері збору доказів та встановлення фактів легалізації доходів, отриманих незаконним шляхом, варто зосередитись на створенні інформаційної бази даних, яка пов'язує суб'єктів економічних відносин та їх контрагентів з фактами легалізації незаконних доходів, для побудови на основі неї інтелектуальних систем виявлення паттернів легалізації незаконних

доходів. Доцільно перекласти функції аналізу на Державну службу фінансового моніторингу та Бюро економічної безпеки.

Усе вищезазначене дозволить сформувати комплексне бачення стратегії залучення найбільш компетентних органів до розслідування операцій з легалізації доходів, отриманих незаконним шляхом, використання найбільш ефективних практик.

У контексті характеристики ефективності розслідувально-карального напрямку забезпечення протидії легалізації кримінальних доходів в Україні, можна відміти існування кількох критичних проблемних аспектів, серед яких: відсутність реально діючих інструментів контролю готівкового обігу в обсягах нижче встановленого порогу, трудомісткий та неефективний підхід до фінансового моніторингу, проблеми ідентифікації осіб, пов'язаних з публічними діячами у реалізації легалізаційних схем та низький рівень розкриття злочинів, пов'язаних з легалізацією доходів та майна, отриманих незаконним шляхом.

У контексті вирішення проблеми відсутності реально діючих інструментів контролю готівкового обігу в обсягах нижче встановленого порогу запропоновано здійснити масштабування системи національного банкоматного роумінгу шляхом залучення до неї всіх суб'єктів банківського ринку України. Це дозволить сформувати базу клієнтів, які вилучають з безготівкового обігу фінансові ресурси через банкомати інших банків, і спрогнозувати потенціал їх використання у легалізаційних схемах. Зокрема, впроваджена ініціатива «Національний банкоматний роумінг» може стати частиною об'єднаної міжбанківської системи обміну інформацією в межах стандартизованої банківської системи. Дозвіл знімати кошти клієнтам з банкомату будь-якого банку без комісії та з підвищеним лімітом суми зняття готівки в контексті протидії легалізації незаконних доходів має негативний вплив, оскільки збільшує обсяги готівки в обігу, проте з іншого боку, це стимулює учасників банківського ринку обмінюватись інформацією стосовно обсягів знятої готівки. У таких умовах недобросовісним банкам, які ігнорують

законодавство у сфері протидії легалізації доходів, отриманих незаконним шляхом, буде складніше приховувати участь своїх клієнтів у легалізаційних схемах, оскільки інші банки будуть мати інформацію про розміри оборотів готівки своїх клієнтів та клієнтів інших банків, що скористалися їх банкоматною мережею. У разі відмови банків від участі у національному банкоматному роумінгу чи загальній інформаційній системі щодо обігу готівки через банкомати, пропонується визначати політику банку як таку, що має підвищений ризик залучення до легалізації незаконних доходів, що, у свою чергу, має слугувати підставою для більш ретельної та прискіпливої уваги відповідних контролюючих органів до такого учасника банківського рикну.

Проблему надмірної трудомісткості та неефективності існуючого підходу до фінансового моніторингу запропоновано вирішувати шляхом імплементації інтелектуальної моделі автоматизованої системи виявлення паттернів легалізації доходів залежно від фінансової поведінки клієнта. Так, варто відзначити, що розроблені на основі великих даних алгоритми оцінки ризику легалізації незаконних доходів враховують детальну інформацію про клієнта та його поведінку, але не всі банківські системи мають технічну змогу збирати цю інформацію. Саме тому для підвищення ефективності виявлення ризикових операцій доцільно запровадити автоматичні системи оцінки ризику легалізації на основі сучасних програм зі штучним інтелектом, побудованим на основі великих даних про транзакції клієнтів. Впровадження інтелектуальних систем дозволить виявляти паттерни фінансових операцій в залежності від фінансової поведінки клієнта чи контрагента, що сприятиме відмові від бінарних характеристик обов’язкового фінансового моніторингу, неефективність якого було нами емпірично доведено (результати представлено у розділі 2 дисертаційної роботи). Зокрема, основним мотивом визнання неефективності чинного підходу до фінансового моніторингу є те, що він генерує велику кількість операцій, що підлягають обов’язковому фінансовому моніторингу, але не є такими, що направлені на легалізацію. Як

наслідок, інформація про ці операції передається Державній службі фінансового моніторингу України, де після аналізу та опрацювання даних за мільйонами операцій встановлюється, що лише десятки з них мають реальний ризик легалізації доходів, отриманих незаконним шляхом.

Серйозною проблемою чинної системи протидії легалізації доходів, отриманих незаконним шляхом, є відсутність ефективних механізмів ідентифікації осіб, пов'язаних з публічними діячами, у реалізації легалізаційних схем. Для вирішення цієї проблеми запропоновано запровадити практику використання методів машинного навчання на основі великих даних та аналізу даних з відкритих джерел (OSINT) для побудови графів залежностей між фізичними особами з метою встановлення на цій основі кола пов'язаних з публічними діячами осіб. Дана розробка зможе аналізувати записи у соціальних мережах, сайтах новин, світлин публічних діячів і найближче коло їх знайомств. Наразі багато банківських установ здійснюють аналіз осіб з ідентичними з публічними діячами прізвищем та ім'ям, щоб встановити з ними родинні зв'язки. Однак, використання OSINT дозволить поліпшити якість роботи відповідних органів та служб у цьому напрямку, оскільки легалізація доходів, одержаних незаконним шляхом, не завжди здійснюється виключно через осіб, пов'язаних родинними зв'язками. Зокрема, ризик залучення до цих схем осіб з найближчого оточення (друзів, кумів, колег тощо) є доволі високим, проте залишається поза увагою. Таким чином, використання OSINT дозволить поліпшити точність та ефективність ідентифікації учасників легалізаційних схем, пов'язаних з публічними особами.

Ще однією важливою проблемою системи протидії легалізації доходів, одержаних незаконним шляхом, є низький рівень розкриття злочинів, пов'язаних з легалізацією доходів та майна, отриманих незаконним шляхом, що пов'язано з нераціональною диференціацією підслідності таких злочинів за різними органів. Зокрема, варто зауважити, що злочини у сфери легалізації кримінальних доходів можуть знаходитися у сфері компетентності одразу

кількох інституцій серед яких Бюро економічної безпеки, Національне антикорупційне бюро, або за підслідністю органу, який розслідує злочин, що передував легалізації, або за органом, який розпочав досудове розслідування. Відповідно, фактично будь-який слідчий орган може розслідувати факти легалізації доходів, отриманих незаконним шляхом. Це породжує проблему недостатньої кваліфікації працівників всіх слідчих органів для розслідування легалізації доходів, отриманих незаконним шляхом, а отже знижує якість самого розслідування. Для вирішення цієї проблеми запропоновано закріпити підслідність злочинів легалізації незаконних доходів за Бюро економічної безпеки України, адже легалізація незаконних доходів напряму пов'язана з тіньовим сектором економіки та економічною безпекою держави. Крім того, важливо продовжувати роботу, спрямовану на усунення законодавчих прогалин та неточностей з метою забезпечення визнання правою системою України легалізації доходів, отриманих незаконним шляхом, як самостійного злочину. Так, відповідно до ратифікованої в Україні у 2010 році Варшавської конвенції, для визнання особи винною у легалізації доходів, отриманих незаконним шляхом, не потрібне попереднє або одночасне засудження за злочин, що передував легалізації таких доходів. Разом з тим, проведений аналіз інституційних змін у системі протидії легалізації доходів, одержаних незаконним шляхом, та судової практики за 2019–2022 рр. виявлено лише поодинокі випадки винесення обвинувальних вироків саме виключно за ст. 209 Кримінального кодексу України «Легалізація (відмивання) доходів, одержаних злочинним шляхом». Визнання правою системою України легалізації доходів, отриманих незаконним шляхом, як самостійного злочину з одночасним закріплення підслідності цих злочинів за Бюро економічної безпеки України дозволить скоротити терміни та підвищити ефективність розкриття злочинів легалізації доходів та майна, отриманих злочинним шляхом.

Таким чином, узагальнюючи все вище викладене, варто відмітити, що реформування системи протидії легалізації доходів, отриманих незаконним

шляхом, має передбачати врахування проблемних аспектів функціонування цієї системи за превентивним, комунікаційно-конгруентним та розслідувально-каральним напрямками, а врахування описаних вище пропозицій щодо їх усунення дозволить досягнути помітних результатів. Справедливо також зауважити, що більшість напрямків реформування системи протидії легалізації доходів, отриманих незаконним шляхом, стали можливими лише в умовах діджиталізації, що переконливо підтверджує вагомість процесів цифровізації у розбудові цієї системи.

ВИСНОВКИ

На основі проведеного бібліометричного аналізу наукових публікацій присвячених вивченню питання кіберзагроз та інших споріднених понять у системі економічних відносин виявлено, що протягом останніх десяти років науковий інтерес до вивчення питань кіберзагроз постійно та динамічно зростає. Основою бібліометричного аналізу виступила міжнародна база даних наукових публікацій Scopus. У 2022 році опубліковано 690 наукових публікацій з досліджуваної тематики, що на 88,5% більше порівняно з 2018 роком. Науковці з США, Великобританії та Індії є найбільш активними у дослідженні питання кібербезпеки та кіберзахисту.

За результатами аналізу частоти використання ключових слів у наукових статтях, присвячених питанням кібербезпеки в економічному вимірі та проіндексованих у наукометричній базі даних Scopus, у роботі сформовано 4 наукових кластери: 1) кластер, присвячений вивченню кібербезпеки та складові її забезпечення; 2) кластер, сфокусований на дослідженні та пошуку засобів та технологій ідентифікації кіберзагроз, а також протидії кібератакам; 3) кластер, який спеціалізується на вивченні об'єктів кіберзахисту, які мають пріоритетне значення в умовах діджиталізації економіки; 4) кластер, присвячений дослідженню впливу кіберзагроз на життєдіяльність людини. За результатами контекстуально-часового аналізу з питань кібершахрайств встановлено, що протягом 2019-2020 років основна увага почала приділятися технологіям та засобам забезпечення кібербезпеки, а починаючи з 2021 року науковий інтерес був зміщений на дослідження кіберфізичних систем, використання технологій штучного інтелекту для протидії кібератакам, вивчення ролі кіберзахисту при впровадженні інтернету речей.

Кіберзагрозу запропоновано розглядати як дію наявних та/або потенційно можливих дестабілізуючих факторів та умов навмисного або випадкового порушення безпеки функціонування громадянина, економічних суб'єктів та держави у кіберпросторі. У роботі проведено змістову

розмежування таких понять як «кіберзагроза», «кіберінцидент», «кібератака», «кіберзлочин». Розширено перелік об’єктів кібербезпеки за рахунок інформаційно-комунікаційних засобів фізичних осіб, які використовуються ними для реалізації суспільно та життєвоважливих потреб під час використання кіберпростору.

У роботі визначено основні чинники та передумови зростання кіберінцидентів на глобальному рівні, а саме: потужний розвиток електронних обчислювальних машин, мобільних пристроїв, збільшення кількості пристроїв, підключених до мережі Інтернет; неможливість відслідкувати територію / країну здійснення кібератаки; збільшення кількості користувачів соціальних мереж, які містять персональні дані; використання застарілого та неліцензійного програмного забезпечення; стрімке зростання технологій Інтернет речей; збільшення питомої ваги бізнес-процесів, які передаються на управління третім особам; використання хмарних технологій для зберігання та передачі даних; розширене використання робототехніки або алгоритмів для здійснення автоматичної торгівлі та розробки додатків; збільшення використання віртуальних та цифрових валют.

Аналіз значущих кіберінцидентів у світі протягом 2005-2020 рр. виявлено, що 41,8% кіберіндидентів здійснено резидентами з Китаю, при цьому 40% з них були направлені на об’єкти критичної інфраструктури у сфері публічного управління та 36% – на об’єкти приватного сектору. Крім Китаю, найбільшими спонсорами кібератак у світі є росія та Іран, сукупно на ці три країни припадає 78,5% від всіх кіберінцидентів. Встановлено, що переважна більшість кібератак були здійснені у формі шпіонажу. Найбільша кількість кіберінцидентів у світі була реалізована у вівторок, при цьому фіксуючи збільшення даних протиправних дій у такі дні як 19,24,25.

Для визначеня детермінантів пощирення кіберзагроз побудовано SVM-моделі машинного навчання двох типів (epsilon-SVM regression та nu-SVM regression) в розрізі чотирьох специфікацій опорних векторів: лінійні, поліноміальні, радіально -базисні функції (RBF) та сигмоподібні на основі

дослідження даних вибіркової сукупності країн світу. За результатами емпіричного дослідження причин стрімкого поширення кібершахрайств у фінансовому секторі економіки шляхом використання сигмоїдної nu-SVM regression моделі встановлено, що основними драйверами зростання кібершахрайства є частка населення, яка користується онлайн банкінгом, рівень навичок в Інтернеті, інтенсивність онлайн діяльності.

У роботі проведено типологізацію країн за рівнем участі їх резидентів у здійсненні фінансових кібернетичних шахрайств на основі аналізу показників, що характеризують різні види злочинності та активність кримінальних угруповувань в країні, а також стану корупції, активності на даркнет-ринку, рівня кіберзлочинності та накладення на країну міжнародних санкцій. За результатами використання ітеративного дівізівного методу k-середніх та дерев класифікацій виокремлено 2 групи кластерів: 1-й кластер (14 країн: Данія, Естонія, Фінляндія, Франція, Німеччина, Латвія та інші) та 2 -й кластер (20 країн: Албанія, Білорусь, Кіпр, Угорщина, Молдова, Мороко, Україні та інші).

Для віднесення країн до кластеру 1 необхідними та достатніми є наступні умови: значення змінної «ризик корупції та хабарів» має приймати значення більше 56,500, значення змінної «загальний дохід, який отримано на даркнет-ринку» – менше 5,4100, значення змінної «міжнародні санкції, які накладені на країну» – менше 0,05, значення змінної інтегрального рівня активності кримінальних угруповувань, яке приймає значення менше 0,504, значення змінної інтегрального рівня характеристики різних видів злочинності – не більше 0,590. За протилежних умов вищезазначених індикаторів країни віднесено до кластеру 2.

У роботі запропоновано методику та оцінено узагальнюючий рівень кіберзагроз у розрізі країн Європи, який у 2020 році варіюється від 2,4 ум. од до 74,9 ум.од. та свідчить про нерівномірність здійснення кібератак серед досліджуваних країн. Найбільший рівень кіберзагроз зафіксовано у таких країнах як Іспанія (74,9 ум.од.), Німеччина (63,3 ум.од.), Італія (57,7 ум.од.),

а менший рівень загроз у кіберпросторі – в Хорватії (4,3 ум.од.), Польща (2,4 ум.од.) та Словаччина (8,9 ум.од.).

Розроблено науково-методичний підхід до оцінювання та прогнозування ризику кібершахрайств у сфері фінансових послуг на основі базових восьми індикаторів з використанням нейронної мережі: стать власника банківської картки, його вік, номер банківського рахунку, сума транзакції, вид категорій/товару, година проведення операції, день тижня проведення операції та індикатор шахрайства. 54.2% власників банківських карток, за допомогою яких здійснювалися шахрайські транзакції, були жінки. Середній вік держателів банківських карток, які здійснювали шахрайські фінансові транзакції, становив 50 років. Найбільший обсяг незаконних транзакцій реалізується проходить на купівлю продуктів харчування та товарів. Для вчасної ідентифікації ризику шахрайства з банківськими платіжними картками проведено навчання нейронної мережі на основі тестової вибірки.

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.

Характеризуючи імпульси активізації злочинності, доведено наступне: на кількість злочинів легалізації кримінальних доходів від’ємний вплив має кількість повідомлень про підозрілі операції, якщо вони менші за 1836938 одиниць, натомість додатній вплив буде мати мультиплікативний ефект фінтеху та обсягів торгів на біржі, за умови що перший показник буде мати значення більше 0,56 а другий – менше 22330,43; діяльність страхових

компаній веде до зменшення фінансових правопорушень, за умови що показник діяльності страхових компаній буде менший за 0,2395, в іншому випадку, діяльність страхових компаній не буде мати впливу. Мультиплікативний додатній ефект на фінансові правопорушення будуть мати загальний обсяг торгів на біржі з діяльністю страхових компаній, якщо обсяг торгів буде перевищувати 7464,63, а показник діяльності страхових компаній буде меншим за 0,2395. Додатній вплив на кількість фінансових правопорушень буде мати рівень розвитку фінтех, при тому, якщо значення показника буде від 0,3714 до 0,5575, то вплив буде у вигляді підсумку двох термів, а якщо перевищить значення у 0,5575 одиниць, то тільки одного.

У роботі запропоновано методику для оцінювання інтегрального показника кібервразливості споживачів фінансових послуг методом мультиплікативної згортки Кіні 17 нормалізованих індикаторів. Апробація запропонованого методичного підходу засвідчила, що рівень кібервразливості споживачів фінансових послуг у країнах Європи становить у середньому 11%, що дозволяє стверджувати про усвідомленість населенням європейський країн наявних загроз у віртуальному просторі, способів захисту від кіберзлочинності. Проте рівень кібервразливості споживачів фінансових послуг у розрізі країн ЄС не є однорідним, а саме найменшим ризик стати жертвою кібершахрайства мають громадяни таких країн як Данія, Нідерланди, Швеція. До країн з найвищими значеннями розрахованого рівня кібервразливості споживачів фінансових послуг (18%) належать: Іспанія, Італія, Румунія.

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.

Інституційна складова системи протидії легалізації доходів, отриманих незаконним шляхом за 2015-2021 рр., зазнала суттєвих змін через появу нових органів протидії економічним злочинам та перерозподіл функціональних обов'язків між існуючими. Проте зростання кількості покарань й обсягів повернутих грошей до державного бюджету України не спостерігалось. Було встановлено, що час, який проходить від початку вчинення злочину з метою легалізації незаконних доходів до винесення судом обвинувального вироку найчастіше триває роками. Розмір інтервалу у таблиці виживання складає 500 днів (1 рік і 4 місяці), при тому, що за цей період лише 19,3% кримінальних проваджень завершаються обвинувальним вироком суду. В межах другого інтервалу частка кримінальних проваджень з обвинувальним вироком склала 81,8% від тих проваджень, які залишаться після першого часового інтервалу. Відповідно тільки після того, як мине 2 роки 9 місяців частка закритих проваджень буде складати 37%, а на п'ятому інтервалі досягне 62%. Отже, результат діяльності інституційної складової системи протидії легалізації доходів, отриманих незаконним шляхом прослідковується тільки через 2 роки 9 місяців після того, як злочин буде вчинено. Згідно з аналізом результатів за методом Каплана-Майєра, зі збільшенням часу між моментом вчинення злочину та моментом винесення обвинувального вироку суду зменшується ймовірність того, що не буде винесено обвинувальний вирок суду, проте процес займає роки

Відповідно до майбутнього розвитку подій, якщо не буде втручання в систему протидії легалізації доходів, одержаних незаконним шляхом, очікується поступове зниження ефективності інституційного, інвестиційного та податкового каналів протидії легалізації незаконних доходів. Позитивну тенденцію зберігає лише освітній канал протидії легалізації. Розглянувши їх сукупний тренд, встановлено, що ефективність системи протидії легалізації

доходів, одержаних незаконним шляхом буде знижуватись, отже актуальності набуває необхідність її всебічного удосконалення.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Доценко Т. В. Удосконалення системи фінансового моніторингу як інструмент забезпечення економічної безпеки національної економіки : дис. … д-ра філософії : 051. Суми, 2021. 305 с.

2. Миненко С. В. Трансформація системи протидії легалізації кримінальних доходів в умовах діджиталізації національної економіки : дис. … д-ра філософії : 051. Суми, 2022. 204 с.

3. Пігуль Є.І. Моделювання впливу цифровізації на розвиток фінансових технологій: робота на здобуття кваліфікаційного ступеня магістра : 051, наук. кер. В. В. Боженко. Суми: Сумський державний університет, 2021. 80 с.

4. Скринька Л.О. Економіко-математичне моделювання ефективності національної системи протидії кібершахрайствам та легалізації кримінальних доходів на основі методів виживання: робота на здобуття кваліфікаційного ступеня магістра : 051, наук. кер. О. В. Кузьменко. Суми: Сумський державний університет, 2021. 59 с.

5. Von Solms R., Van Niekerk J. From information security to cyber security. *Computers and Security*. 2013. Vol. 38. P. 97–102. URL: https://doi.org/10.1016/j.cose.2013.04.004.

6. Alhogail A., Alsabih A. Applying machine learning and natural language processing to detect phishing email. *Computers and Security*. 2021. P. 110. URL: https://doi.org/10.1016/j.cose.2021.102414.

7. Akhta S., Sheorey P. A., Bhattacharya S., Ajith K. V. V. Cyber security solutions for businesses in financial services: Challenges, opportunities, and the way Forward. *International Journal of Business Intelligence Research.* 2021. Vol. 12, no. 1. URL: https://doi.org/10.4018/IJBIR.20210101.oa5.

8. Ying W., Jia S., Du, W. Digital enablement of blockchain: Evidence from HNA group. *International Journal of Information Management*. 2018. Vol. 39. P. 1-4. URL: https://doi.org /10.1016/j. ijinfomgt.2017.10.004.

9. Al-Tahat S., Moneim O. A. The impact of artificial intelligence on the correct application of cyber governance in Jordanian commercial banks. *International Journal of Scientific and Technology Research*. 2020. Vol 9, no. 3. URL: http://www.class.jpu.edu.jo/juris/uploads/publication/sidr/20210623-0526041053.pdf.

10. Noor U., Anwar Z., Amjad T., Choo K. K. R. A machine learning-based FinTech cyber threat attribution framework using high-level indicators of compromise. *Future Generation Computer Systems.* 2019. Vol. 96. URL: https://doi.org/10.1016/j.future.2019.02.013.

11. Berdyugin A. A., Revenkov P. V. Cyberattack risk assessment in electronic banking technologies (the case of software implementation). *Finance: Theory and Practice*. 2020. Vol. 24, no. 6. URL: https://doi.org/10.26794/2587-5671-2020-24-6-51-60.

12. Mousa M., Sai A.A., Salhin G. An Exploration for the Motives behind Enhancing Senior Banker's Level of Organizational Resilience: A Holistic Case Study. *Journal of Intercultural Management.* 2017. Vol. 9, no. 4. URL: https://doi.org/10.1515/joim-2017-0025.

13. Yerdon V. A., Lin J., Wohleber R. W., Matthews G., Reinerman-Jones L., Hancock P. A. Eye-Tracking Active Indicators of Insider Threats: Detecting Illicit Activity During Normal Workflow. *IEEE Transactions on Engineering Management.* 2021. URL: https://doi.org/10.1109/TEM.2021.3059240.

14. Chen D., Wawrzynski P., Lv Z. Cyber security in smart cities: A review of deep learning-based applications and case studies. *Sustainable Cities and Society*. 2021. Vol. 66. URL: https://doi.org/10.1016/j.scs.2020.102655.

15. Singh S. K., Jeong Y. S., Park J. H. A deep learning-based IoT-oriented infrastructure for secure smart City. *Sustainable Cities and Society*. 2020. Vol. 60. URL: https://doi.org/10.1016/j.scs.2020.102252.

16. Tweneboah-Koduah S., Atsu F., Prasad R. Reaction of stock volatility to data breach: An event study. *Journal of Cyber Security and Mobility*. 2020. Vol. 9, no. 3. URL: https://doi.org/10.13052/JCSM2245-1439.931.

17. Arcuri M. C., Gai L., Ielasi F., Ventisette E. Cyber attacks on hospitality sector: stock market reaction. *Journal of Hospitality and Tourism Technology*. 2020. Vol. 11, no. 2. URL: https://doi.org/10.1108/JHTT-05-2019-0080.

18. Lowry P. B., Zhang J., Wang C., & Siponen M. Why do adults engage in cyberbullying on social media? An integration of online disinhibition and deindividuation effects with the social structure and social learning model. I*nformation Systems Research*. 2016. Vol. 27, no. 4. P. 962–986. URL: https://doi.org/10.1287/isre.2016.0671.

19. Andreou P. C., Anyfantaki S. Financial literacy and its influence on internet banking behavior. *European Management Journal*. 2021. Vol. 39, no. 5. URL: https://doi.org/10.1016/j.emj.2020.12.001.

20. Carlton M., Levy Y., Ramim M. Mitigating cyber attacks through the measurement of non-IT professionals' cybersecurity skills. *Information and Computer Security*. 2019. Vol. 27, no. 1. URL: https://doi.org/10.1108/ICS-11-2016-0088.

21. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII: веб-сайт. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 01.11.2022).

22. Overview and concepts ISO/IEC TS 27100:2020. *ISO*. URL: https://www.iso.org/obp/ui/#iso:std:iso-iec:ts:27100:ed-1:v1:en (Last accessed: 02.11.2022).

23. Li Y., Liu, Q. A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*. 2021. Vol. 7. P. 8176–8186. URL: https://doi.org/10.1016/j.egyr.2021.08.126.

24. What is a cyberattack? *IBM*. URL: https://www.ibm.com/topics/cyber-attack (Last accessed: 02.11.2022).

25. Motsch W., David A., Sivalingam K., Wagner A., Ruskowski M. Approach for dynamic price-based demand side management in cyber-physical production systems. *In Procedia Manufacturing*. 2020. Vol. 51. P. 1748–1754. URL: https://doi.org/10.1016/j.promfg.2020.10.243.

26. Перелік категорій кіберінцидентів. *Державна служба спеціального зв'язку та захисту інформації України*: веб-сайт. URL: https://www.cip.gov.ua/ua/news/perelik-kategorii-kiberincidentiv (дата звернення: 01.11.2022).

27. Діордіца І. В. Поняття та зміст кіберзлочинності. *Глобальна організація союзницького лідерства* : веб-сайт. URL: http://goal-int.org/ponyattya-ta-zmist-kiberzlochinnosti (дата звернення: 01.11.2022).

28. Загуменний О.О. Співвідношень понять «кіберзлочинність» і «компютерні злочини». *Процесуальне та техніко-криміналістичне забезпечення досудового розслідування*. 2019. URL: https://univd.edu.ua/general/publishing/konf/28_11_2019/pdf/21.pdf.

29. Кримінальний кодекс України: Закон від 05.04.2001 № 2341-III: веб-сайт. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text (дата звернення: 01.11.2022).

30. Козирєва В.П., Гаврилішин А.П. Кіберправопорушення як загроза економічній безпеці України. *Юридичний вісник*. 2020. № 1 (54). С. 148-155. URL: https://doi.org/10.18372/2307-9061.54.14553.

31. Островий О.В. Дослідження проблематики забезпечення кібернетичної безпеки в роботах українських науковців: джерельний аналіз. Менеджер. *Вісник Донецького державного університету управління» (серії «Економіка»).* 2018. № 1(78). С. 157-164. URL: https://164-Article%20Text-533-1-10-20201021.pdf.

32. Кузьменко О.Ю., Малюк О.В., Чернишова О.О. Кібербезпека бізнесу під час війни. *Економіка та суспільство.* 2022. № 44. URL: https://economyandsociety.in.ua/index.php/journal/article/view/1790/1725.

33. Ескалація кіберзагроз національним інтересам України та правові аспекти кіберзахисту: монографія / О. Д. Довгань, І. М. Доронін; НАПрН України, НДІІП. Київ : Видавничий дім «АртЕк», 2017. 107 с.

34. ENISA THREAT LANDSCAPE 2021. *European Union Agency for Cybersecurity*. 2021. URL: https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends (Last accessed: 02.11.2022).

35. Yevseiev S., Rzayev K., Mammadova T., Samedov F., Romashchenko N. Класифікатор кіберзагроз інформаційних ресурсів автоматизованих банківських систем. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка».* 2018. № 2(2). С. 47–67. URL: https://doi.org/10.28925/2663-4023.2018.2.4767.

36. Jouini M., Rabai L. B. A., Aissa A. B. Classification of security threats in information systems. In Procedia Computer Science. 2014. Vol. 32. P. 489–496. URL: https://doi.org/10.1016/j.procs.2014.05.452.

37. Nish A., Naumann S., Muir J. Enduring Cyber Threats and Emerging Challenges to the Financial Sector. *Carnegie Endowment for International Peace*. 2020. URL: https://carnegieendowment.org/2020/11/18/enduring-cyber-threats-and-emerging-challenges-to-financial-sector-pub-83239.

38. Лисенко С.М., Харченко В.С., Бобровнікова К.Ю., Щука Р.В. Резильєнтність комп'ютерних систем в умовах кіберзагроз: таксономія та онтологія. *Радіоелектронні і комп'ютерні системи*. 2020. № 1(93). С. 17-28. URL: http://dx.doi.org/10.32620/reks.2020.1.02.

39. The Global Covid-19 FinTech Regulatory Rapid Assessment Report. *World Bank Group and the University of Cambridge*. URL: https://www.jbs.cam.ac.uk/wp-content/uploads/2020/10/2020-ccaf-report-fintech-regulatory-rapid-assessment.pdf (Last accessed: 02.11.2022).

40. X-Force Threat Intelligence Index 2021. *IBM Security*. URL: https://www.ibm.com/downloads/cas/M1X3B7QG (Last accessed: 02.11.2023).

41. Боженко В.В., Кушнерьов О.С., Кільдей А.Д. Детермінанти поширення кіберзлочинності у сфері фінансових послуг. *Економічний форум*. 2021. № 4. С. 116-121. URL: https://doi.org/10.36910/6775-2308-8559-2021-4-16.

42. The Top Threat Actors Targeting Financial Services Organizations. *Insights*. 2018. URL: https://intsights.com/blog/the-top-threat-actors-targeting-financial-services-organizations (Last accessed: 20.11.2022).

43. The Mobile Economy 2020. *GSM Association*. URL: https://www.gsma.com/mobileeconomy/wp-content/uploads/2020/03/GSMA_MobileEconomy2020_Global.pdf (Last accessed: 20.11.2022).

44. Europeans' attitudes towards cyber security. Special Eurobarometer 499. *European Commision*. 2020. URL: https://europa.eu/eurobarometer/surveys/detail/2249 (Last accessed: 20.11.2023).

45. Global Social Network Users 2020. *eMarketer*. URL: https://www.emarketer.com/content/global-social-network-users-2020 (Last accessed: 20.11.2022).

46. Use of Internet of Things in enterprises. E*urostat*. URL: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Use_of_Internet_of_Things_in_enterprises#Enterprises_using_IoT (Last accessed: 20.11.2022).

47. Cloud computing - statistics on the use by enterprises. *Eurostat*. URL: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Cloud_computing_-_statistics_on_the_use_by_enterprises (Last accessed: 20.11.2022).

48. Cloud Computing. *Grand View Research*. URL: https://www.grandviewresearch.com/industry-analysis/cloud-computing-industry# (Last accessed: 20.11.2022).

49. World Robotics Report 2020. *International Federation of Robotics*. URL: https://ifr.org/downloads/press2018/Presentation_WR_2020.pdf (Last accessed: 20.11.2022).

50. European Repository of Cyber Incidents. *EuRepoc Data*. URL: https://eurepoc.eu/databases (Last accessed: 20.11.2023).

51. Ransomware Statistics, Trends and Facts for 2023 and Beyond. *Cloudwards*. URL: https://www.cloudwards.net/ransomware-statistics/ (Last accessed: 20.11.2022).

52. Prieto Curiel R. Weekly Crime Concentration. *Journal of Quantitative Criminology.* 2023. Vol. 39, No. 1. P. 97–124. URL: https://doi.org/10.1007/s10940-021-09533-6.

53. Bernasco W., Ruiter S., Block R. Do Street Robbery Location Choices Vary Over Time of Day or Day of Week? A Test in Chicago. *Journal of Research in Crime and Delinquency*. 2017. Vol. 54, No. 2. P. 244–275. URL: https://doi.org/10.1177/0022427816680681.

54. Haberman C. P., Ratcliffe J. H. Testing for Temporally Differentiated Relationships among Potentially Criminogenic Places and Census Block Street Robbery Counts. *Criminology*. 2015. Vol. 53, No. 3. P. 457–483. URL: https://doi.org/10.1111/1745-9125.12076.

55. 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. Vol. 66, No. 3. P. 425-430. URL: https://doi.org/10.24425-ijet.2020.131895/715.

56. 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. Vol. 2845. P.181-192. URL: https://essuir.sumdu.edu.ua/bitstream-download/123456789/91725/1/Kuzmenko_cyberrisk.pdf;jsessionid=9731632C866444CF7172A4366C04B164.

57. Кузьменко О.В., Доценко Т.В., Боженко В.В., Світлична А.О. Закономірності здійснення кібератак в країнах ЄС на основі використання асоціативних правил. *Вісник СумДУ. Серія Економіка.* 2021. № 1. С. 95-103. URL: https://essuir.sumdu.edu.ua/handle/123456789/83946.

58. Internet Crime Report. *Federal Bureau of Investigation*. URL: https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf (Last accessed: 20.11.2022).

59. Chakrabarty K. C. Fraud in the banking sector – causes, concerns and cures. *Bank for international Settlements. New Delhi*. 2013. URL: https://www.bis.org/review/r130730a.pdf (Last accessed: 15.05.2021).

60. Мельник С.С. Сутність фінансового шахрайства в комерційному банку. *Науковий вісник* Ужгородського національного університету. 2016. № 6, ч. 2. С. 91–95. URL: http://nbuv.gov.ua/UJRN/Nvuumevcg_2016_6(2)__23.

61. Звіт про роботу системи виявлення вразливостей і реагування на кіберінциденти та кібератаки 2022. *Оперативний центр реагування на кіберінциденти Державного центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації України*: веб-сайт. URL: https://nsarchive.gwu.edu/sites/default/files/documents/rr9q9n-glu5j/2023-01-00-SSCIP-Vulnerability-Detection-System-and-Response-to-Cyber-Incidents-and-Cyber-Attacks-%20via-website.pdf (Дата звернення: 15.05.2021).

62. Звіт про роботу системи виявлення вразливостей і реагування на кіберінциденти та кібератаки 2023. *Оперативний центр реагування на кіберінциденти Державного центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації України*: веб-сайт. URL: https://scpc.gov.ua/api/files/a7de388d-14d3-4248-b8be-ada8b5cb0710 (Дата звернення: 15.05.2021).

63. Which countries have the worst (and best) cybersecurity? *Comparitech.* URL: https://www.comparitech.com/blog/vpn-privacy/cybersecurity-by-country/ (Last accessed: 15.10.2022).

64. Digital Economy and Society Index. *European Commission*. URL: https://digital-strategy.ec.europa.eu/en/policies/desi (Last accessed: 15.10.2022).

65. Waldrop M. How to hack the hackers: The human side of cybercrime. *EconPapers*. 2016. Vol. 533, No. 7602. P.164-167. URL: https://doi.org/10.1038/533164a.

66. Global Organized Crime Index. *Global Initiative.* URL: https://ocindex.net/report/2023/0-3-contents.html (Last accessed: 15.10.2022).

67. Significant Cyber Incidents. *Center for Strategic and International stidies.* URL: https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents (Last accessed: 20.10.2022).

68. Report on card fraud in 2020 and 2021. *European Central Bank*. URL: https://www.ecb.europa.eu/pub/cardfraud/html/ecb.cardfraudreport202305~5d832 d6515.en.html (Last accessed: 01.02.2023).

69. Global Payment Fraud Statistics, Trends & Forecasts. *Merchant Savvy*. URL: https://www.merchantsavvy.co.uk/payment-fraud-statistics/ (Last accessed: 25.08.2022).

70. Платіжні картки в України. *Національний банк України*: веб-сайт. URL: https://bank.gov.ua/ua/news/all/platijni-kartki-v-ukrayini-i-pivrichchya-2021-roku (Дата звернення: 25.08.2022).

71. 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 01.02.2022).

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

73. The Global State of Digital in October 2022. Global Digital Insights. URL: https://datareportal.com/reports/digital-2022-global-overview-report (Last accessed: 30.08.2022).

74. 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, No. 4. P. 119-124. http://doi.org/10.21272/fmir.6(4).119-124.2022.

75. Тихомирова Є. Соціальна інженерія. *In Advances in Technology and Science.* 2021. P. 225–228. URL: https://isg-konf.com/wp-content/uploads/2021/03/XII-ConferenceMarch-16-192021-book.pdf.

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

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

78. 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 (Дата звернення 01.04.2022).

79. 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, No. 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.

80. Cinelli M., De Francisci Morales G., Galeazzi A., Quattrociocchi W., Starnini M. The echo chamber effect on social media. *Proceedings of the National Academy of Sciences*. 2021. Vol. 118, No. 9. Article e2023301118.

81. Salahdine F., Kaabouch N. Social Engineering Attacks: A Survey. *Future Internet*. 2019. Vol. 11, No. 4. 89 P. URL: https://doi.org/10.3390/fi11040089.

82. 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. С. 190–192. URL: https://sci.ldubgd.edu.ua/bitstream/123456789/4729/1/aktualn_problemi_upravl_nnya_nformac_ycnoyu_bezpekoyu_derzhavi.pdf.

83. Василик А. В., Іщенко О. В. Використання соціальних мереж у сучасному рекрутингу України. *Економічний простір*. 2018. № 131. С. 53–63. URL: http://www.prostir.pdaba.dp.ua/index.php/journal/article/view/205.

84. Втрачені можливості: українці надають більшу перевагу розважальним соцмережам, ніж професійному LinkedIn. *GlobalLogic Ukraine*:

веб-сайт. URL: https://www.globallogic.com/ua/about/news/social-networks-and-opportunitites/ (Last accessed: 30.08.2022).

85. Download Instagram Photos and Metadata. *Instaloader*. URL: https://instaloader.github.io/ (Last accessed: 30.08.2022).

86. Data Mining. *Orange Data Mining*. URL: https://orangedatamining.com (Last accessed: 30.08.2022).

87. Кузьменко О.В., Миненко С.В., Доценко Т.В., Шрамко Е.В. Взаємозалежність FinTech інновацій, фінансових, кібернетичних злочинів та легалізації кримінальних доходів за посередництва фінансових установ. *Вісник СумДУ*. 2021. № 1. С. 195-207. URL: http://doi.org/10.21272/1817-9215.2021.1-23.

88. Кузьменко О.В., Миненко С.В., Доценко Т.В. Кібершахрайства, фінансові правопорушення та легалізація кримінальних доходів в умовах цифровізації економіки України. *Науковий погляд: економіка та управління.* 2021. №3 (72). С. 9-21.

89. Belen Suarez Lopez, David Issó García, Antonio Vargas Alcaide. Blockchain Technology Facing Socioeconomic Challenges. Promise versus Probability. *SocioEconomic Challenges*. 2019. Vol. 3, No. 4. P. 13-24. URL: http://doi.org/10.21272/sec.3(4).13-24.2019.

90. Araujo Ricardo. Assessing the efficiency of the anti-money laundering regulation: an incentive-based approach. *Journal of Money Laundering Control.* 2008. Vol. 11. P. 67-75. URL: http://doi.org/10.1108/13685200810844505.

91. Zarutska E., Pavlova T., Sinyuk A. Structural-functional analysis as innovation in public governance (case of banking supervision). Marketing and Management of Innovations. 2018. Vol. 4. P.349-360. URL: https://doi.org/10.21272/mmi.2018.4-30.

92. Опитування про системні ризики фінансового сектору. Травень 2023 *Національний банк України.* URL: https://bank.gov.ua/ua/news/all/opituvannya-pro-sistemni-riziki-finansovogo-sektoru-traven-2023-roku

93. Про затвердження Положення про здійснення контролю за дотриманням банками вимог законодавства з питань інформаційної безпеки, кіберзахисту та електронних довірчих послуг: Постанова НБУ № 4 від 16 січня 2021 року. *Національний банк України*: веб-сайт. URL: https://bank.gov.ua/admin_uploads/law/16012021_4.pdf (Дата звернення 01.04.2022).

94. Guidance on cyber resilience for financial market infrastructures. *CPMI-IOSCO*. 2016. URL: https://www.bis.org/cpmi/publ/d146.pdf (Last accessed: 30.08.2022).

95. Cyber resilience oversight expectations for financial market infrastructures. *ECB.* 2018. URL: https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf (Last accessed: 30.08.2022).

96. Cyber-resilience: Range of practicesю December 2018. *Basel Committee on Banking Supervision.* URL: https://www.bis.org/bcbs/publ/d454.pdf (Last accessed: 30.08.2022).

97. Europeans' attitudes towards cyber security. Special Eurobarometer 499. *European Commision.* 2020. URL: https://europa.eu/eurobarometer/surveys/detail/2249 (Last accessed: 30.08.2022).

98. Cebrián E., Domenech J. Is Google Trends a quality data source? *Applied Economics Letters*. 2023. Vol. 30, No. 6. P. 811–815. URL: https://doi.org/10.1080/13504851.2021.2023088.

99. Cervellin G., Comelli I., Lippi G. Is Google Trends a reliable tool for digital epidemiology? Insights from different clinical settings. *Journal of Epidemiology and Global Health*. 2017. Vol. 7, No. 3. P. 185–189. URL: https://doi.org/10.1016/j.jegh.2017.06.001.

100. Sivesind T. E., Szeto M. D., Kim W., Dellavalle R. P. Google Trends in Dermatology: Scoping Review of the Literature. *JMIR Dermatology*. 2021. URL: https://doi.org/10.2196/27712.

101. Senecal C., Mahowald M., Lerman L., Lopes-Jimenez F., Lerman A. Increasing utility of Google Trends in monitoring cardiovascular disease. *Digital Health.* 2021. Vol. 7. URL: https://doi.org/10.1177/20552076211033420.

102. Zhang H., Wang Y., Zheng Q., Tang K., Fang R., Wang Y., Sun Q. Research Interest and Public Interest in Melanoma: A Bibliometric and Google Trends Analysis. *Frontiers in Oncology*. 2021. Vol. 11. URL: https://doi.org/10.3389/fonc.2021.629687.

103. Borup D., Schütte E. C. M. In Search of a Job: Forecasting Employment Growth Using Google Trends. *Journal of Business and Economic Statistics*. 2022. Vol. 40, No. 1. P. 186–200. URL: https://doi.org/10.1080/07350015.2020.1791133.

104. Havranek T., Zeynalov A. Forecasting tourist arrivals: Google Trends meets mixed-frequency data. *Tourism Economics*. 2021. Vol. 27, No. 1. P. 129–148. URL: https://doi.org/10.1177/1354816619879584.

105. Simionescu M., Cifuentes-Faura J. Forecasting National and Regional Youth Unemployment in Spain Using Google Trends. *Social Indicators Research*. 2022. Vol. 164, No. 3. P. 1187–1216. URL: https://doi.org/10.1007/s11205-022-02984-9.

106. Кудь А. А. Феномен віртуальних активів: економічний та правовий аспекти. Харків. 2020. URL: IJES.2020.4.2.pdf (culturehealth.org).

107. 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.

108. Bank of international settlements. *Annual Economic Report 2022 of the BIS.* 2022. URL: https://www.bis.org/publ/arpdf/ar2022e.pdf (Last accessed: 30.08.2022).

109. DeFi risks and the decentralisation illusion. *Bank of international settlements.* 2021. URL: https://www.bis.org/publ/qtrpdf/r_qt2112b.htm (Last accessed: 30.08.2022).

110. Кудь О. О., Кучерявенко, М. П., Смичок ,Є. М. Цифрові активи та їх правове регулювання у світі розвитку технології блокчейн : монографія. Харків : Право, 2019. 216 с.

111. Милош Д.В., Герасенко В.П. Перспективы развития цифровых финансовых активов. *Економічний вісник університету*. 2020. № 44. С. 56-63. URL: https://cyberleninka.ru/article/n/perspektivy-razvitiya-tsifrovyh-finansovyh-aktivov/viewer.

112. Про віртуальні активи: Закон України від 17.02.2022 № 2074-IX. *Верховна рада України*: веб-сайт. URL: https://tinyurl.com/r76rpn6f (Дата звернення 01.04.2022).

113. Класифікація віртуальних активів в Україні. *Вища школа адвокатури НААУ*. 2021. URL: https://tinyurl.com/574pv2x4 (Дата звернення 01.04.2022).

114. Central Bank Digital Currency. Which countries are using, launching, piloting their own digital currencies. *EuroNews.* 2022. URL: https://www.euronews.com/next/2022/03/09/cbdcs-these-are-the-countries-are-using-launching-or-piloting-their-own-digital-currencies (Last accessed: 30.08.2022).

115. Today's Cryptocurrency Prices by Market Cap. *CoinMarketCap*. URL: https://coinmarketcap.com (Last accessed: 01.02.2023).

116. Can every currency of the world be a stablecoin? *The Economic Times.* 2022. URL: https://tinyurl.com/23uwbdcs (Last accessed: 01.02.2023).

117. Types of Blockchains: PoW, PoS, and Private. *Gemini*. URL: https://www.gemini.com/cryptopedia/blockchain-types-pow-pos-private (Last accessed: 01.02.2023).

118. Cambrige Bitcoin Electricity Consumption Index. CCAF. URL: https://ccaf.io/cbeci/index (Last accessed: 01.02.2023).

119. Jaag C., Bach C. Cryptocurrencies: New Opportunities for Postal Financial Services. 2015. URL: www.swiss-economics.ch (Last accessed: 01.02.2023).

120. 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 (Last accessed: 01.02.2023).

121. Zhao L. The function and impact of cryptocurrency and data technology in the context of financial technology: Introduction to the issue. *Financial Innovation*. 2021. Vol. 7, No. 1. URL: https://doi.org/10.1186/s40854-021-00301-w.

122. Liu X. F., Ren H., Liu S., Jiang X. Characterizing key agents in the cryptocurrency economy through blockchain transaction analysis. *EPJ Data Science*. 2021. Vol. 10, No. 1. URL: https://doi.org/10.1140/epjds/s13688-021-00276-9.

123. Bailey A. M., Rettler B., Warmke C. Philosophy, politics, and economics of cryptocurrency II: The moral landscape of monetary design. *Philosophy Compass*. 2021. Vol. 16, No. 11. URL: https://doi.org/10.1111/phc3.12784.

124. López-Martín C., Benito Muela S., Arguedas R. Efficiency in cryptocurrency markets: New evidence. *Eurasian Economic Review*. 2021. Vol. 11, No. 3. P. 403-431. URL: https://doi.org/10.1007/s40822-021-00182-5.

125. 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. Vol. 9, No. 9. URL: https://doi.org/10.3390/risks9090163.

126. 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. Vol. 4, No. 1. P. 158-179. URL: https://doi.org/10.3905/jfds.2021.1.080.

127. Fang F., Ventre C., Basios M., Kanthan L., Martinez-Rego D., Wu F., Li L. Cryptocurrency trading: A comprehensive survey. *Financial Innovation*. 2022. Vol. 8, No. 1. URL: https://doi.org/10.1186/s40854-021-00321-6.

128. Bziker Z. The status of cryptocurrency in morocco. *Research in Globalization*. 2021. Vol. 3. URL: https://doi.org/10.1016/j.resglo.2021.100040.

129. Widjaja G. Cryptocurrency and the role of indonesian central bank. *Journal of Legal, Ethical and Regulatory Issues*. 2021. Vol. 24, No. 2. P. 1-8. URL: https://doi.org/10.24191/abrij.v5i2.9997.

130. Riley J. The current status of cryptocurrency regulation in china and its effect around the world. *China and WTO Review*. 2021. Vol. 7, No. 1. P. 135-152. URL: https://doi.org/10.14330/cwr.2021.7.1.06.

131. Ukwueze F. O. Cryptocurrency: Towards regulating the unruly enigma of fintech in nigeria and south africa. *Potchefstroom Electronic Law Journal*. 2021. Vol. 24. URL: https://doi.org/10.17159/1727-3781/2021/V24I0A10743.

132. Delva Benavides J. E., Torres Amaya F. E. Legal, tax and accounting treatment of cryptocurrencies in mexico. *Global Jurist*. 2021. URL: https://doi.org/10.1515/gj-2021-0061.

133. Nghiem H., Muric G., Morstatter F., Ferrara E. Detecting cryptocurrency pump-and-dump frauds using market and social signals. *Expert Systems with Applications*. 2021. Vol. 182. URL: https://doi.org/10.1016/j.eswa.2021.115284.

134. Teichmann F. M. J., Falker M. Cryptocurrencies and financial crime: Solutions from liechtenstein. *Journal of Money Laundering Control*. 2021. Vol. 24, No. 4. P. 775-788. URL: https://doi.org/10.1108/JMLC-05-2020-0060.

135. Huang S. Cryptocurrency and crime. FinTech, artificial intelligence and the law: Regulation and crime prevention. 2021. P. 125-143. URL: https://dokumen.pub/fintech-artificial-intelligence-and-the-law-regulation-and-crime-prevention-2021003918-2021003919-9780367897659-9781032012469-9781003020998.html.

136. 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. URL: https://doi.org/10.1109/SIST50301.2021.9465983.

137. Dupuis D., Gleason K. Money laundering with cryptocurrency: Open doors and the regulatory dialectic. *Journal of Financial Crime*. 2021. Vol. 28. No. 1. P. 60-74. URL: https://doi.org/10.1108/JFC-06-2020-0113.

138. 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. Vol. 11, No. 1. URL: https://doi.org/10.1186/s40163-021-00163-8.

139. Ren B., Lucey B. Do clean and dirty cryptocurrency markets herd differently? *Finance Research Letters*. 2022. Vol. 47. URL: https://doi.org/10.1016/j.frl.2022.102795.

140. 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. Vol. 179. URL: https://doi.org/10.1016/j.techfore.2022.121632.

141. Lucey B. M., Vigne S. A., Yarovaya L., Wang Y. The cryptocurrency uncertainty index. *Finance Research Letters*. 2022. Vol. 45. URL: https://doi.org/10.1016/j.frl.2021.102147.

142. 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. Vol. 66, No. 3. P. 425-430. URL: тhttps://doi.org/10.24425-ijet.2020.131895/715.

143. 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.

144. Ethereum Fraud Detection Dataset. *Kaggle.* URL: https://www.kaggle.com/datasets/vagifa/ethereum-frauddetection-dataset (Last accessed: 01.02.2023).

145. Fong J. Global cybercrime report: which countries are most at risk in 2023? *SEON*. URL: https://seon.io/resources/global-cybercrime-report/ (Last accessed: 18.07.2023).

146. e-Governance Academy Foundation. *NCSI*. URL: https://ncsi.ega.ee/ncsi-index/ (Last accessed: 18.07.2023).

147. Global Cybersecurity Index 2020. Geneva, Switerland : International Telecommunication Union, 2023. 172 p. URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf.

148. Frisby J. Cybersecurity Exposure Index (CEI) 2020. *PasswordsManagers.co.* URL: https://passwordmanagers.co/cybersecurity-exposure-index/ (Last accessed: 18.07.2023).

149. Cryptocurrency ownership data. Cryptocurrency across the world. *Triple-A.* URL: https://triple-a.io/crypto-ownership-data/ (Last accessed: 18.07.2023).

150. Individuals' level of digital skills. *Eurostat.* URL: https://ec.europa.eu/eurostat/web/products-datasets/-/isoc_sk_dskl_i21 (Last accessed: 18.07.2023).

151. Flash Eurobarometer FL509 : Retail Financial Services and Products. *data.europa.eu.* URL: https://data.europa.eu/data/datasets/s2666_fl509_eng?locale=en (Last accessed: 18.07.2023).

152. Grauer K., Jardine E. Cryptocurrencies and drugs: Analysis of cryptocurrency use on darknet markets in the EU and neighbouring countries. *The European Monitoring Centre for Drugs and Drug Addiction (EMCDDA)*. 2022. 42 p.

153. E-banking and e-commerce. *Eurostat.* URL: https://ec.europa.eu/eurostat/web/products-datasets/-/isoc_bde15cbc (Last accessed: 18.07.2023).

154. Schneider F., Asllani A. Taxation of the informal economy in the EU. *European Parllament. Subcommittee on tax matters (FISC),* 2022. 128 p. URL:

https://www.europarl.europa.eu/RegData/etudes/STUD/2022/734007/IPOL_STU(2022)734007_EN.pdf.

155. 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.

156. Małecka M. Values in economics: a recent revival with a twist. *Journal of Economic Methodology*. 2021. Vol. 28, No. 1. P. 88-97. URL: https://doi.org/10.1080/1350178X.2020.1868776 (Дата звернення: 20.07.2023).

157. Генеральна прокуратура України: офіційний веб сайт. URL: https://www.gp.gov.ua/ua/1stat (Дата звернення: 20.07.2023).

158. Державна служба статистика України: офіційний веб-сайт. URL: http://www.ukrstat.gov.ua/ (Дата звернення: 20.07.2023).

159. Державна служба фінансового моніторингу України: офіційний веб-сайт. URL: https://fiu.gov.ua/pages/dijalnist/funkcional/statistika-ta-infografika (Дата звернення: 20.07.2023).

160. Звіт Державної служби фінансового моніторингу за 2021 рік. *Державна служба фінансового моніторингу*. 2022. URL: https://fiu.gov.ua/assets/userfiles/0350/zvity/zvit2021ukr.pdf.

ДОДАТКИ

Додаток А

Таблиця А.1 – Статистична база характеристики детермінант поширення кіберзагроз станом на 2020 рік

		I1	I2	I3	I4	I5	I6	I7	I8	I9	I10	I11	I12	I13	I14	I15
Австрія	AUS	1,82	0,02	0	0,2	0,06	2,87	5,51	1,39	0,05	0,15	0,16	0,38	0,62	10,17	22321
Бельгія	BEL	2,85	0,02	0,01	0,2	0,05	4,39	5,85	1,98	0,08	0,2	0,13	0,25	0,28	16,4	49342
Болгарія	BGR	3,5	0,03	0,01	0,5	0,16	4,83	15,43	0,66	0,24	0,56	0,17	0,5	0,38	11,35	301
Хорватія	HRV	2,54	0,02	0,01	0,3	0,08	3,89	7,39	1,04	0,1	0,36	0,13	1,3	0,37	9,15	8418
Данія	DNK	1,33	0	0	0,1	0,02	1,33	2,83	1,42	0,02	0,11	0,07	0,07	0,06	3,26	9208
Фінляндія	FIN	1,06	0,02	0,01	0,3	0,06	2,73	5,77	0,39	0,02	0,36	0,09	0,23	0,01	7,14	1994
Франція	FRA	2,56	0,01	0	0,2	0,08	6,71	6,45	2,53	0,46	0,16	4,03	5,97	1,12	17,9	30485
Німеччина	DEU	1,63	0,02	0,01	0,3	0,06	3,54	4,94	1,8	0,66	0,12	4,67	10,97	7,28	9,68	314459
Греція	GRC	2,75	0,01	0	0,5	0,14	5,39	13,27	1,4	2,52	0,49	0,19	0,21	1,75	16	10677
Угорщина	HUN	3,34	0	0	0,2	0,12	4,33	12,7	1,83	0,3	0,42	0,35	0,83	0,34	15,1	2546
Ірландія	IRL	2,12	0	0,01	0,1	0,04	1,35	3,49	1,63	0,04	0,19	0,33	0,25	0,06	3,42	22331
Італія	ITA	3,26	0,31	0,02	0,5	0,12	4,38	10,74	2,32	1,56	0,22	1,35	1,02	5,45	15,45	578779
Латвія	LVA	3,36	0,02	0	0,3	0,16	7,31	13,95	0,61	0,1	0,73	0,06	0,91	0,3	12,86	78
Нідердланди	NLD	1,66	0,02	0,01	0,2	0,05	1,66	4,24	1,1	0,28	0,19	1,86	4	0,26	4,84	15537
Польща	POL	2,79	0,09	0,01	0,3	0,09	3,69	7,54	1,48	0,61	0,37	0,48	2,05	0,65	12,7	5976
Португалія	PRT	3,38	0,01	0,01	0,9	0,12	5,34	11,5	2,2	0,1	0,44	0,17	0,35	1,88	19,73	2299
Румунія	ROU	5,04	0,02	0,02	0,4	0,04	5,3	14,4	1,32	0,58	0,14	0,29	0,49	0,98	5,76	2812
Словаччина	SVK	3,5	0,03	0,01	0,3	0,11	3,43	8,24	1,24	0,09	0,5	0,04	0,19	0,09	12,94	450
Іспанія	ESP	4,31	0,22	0,01	0,3	0,09	5,92	11,63	2,27	0,7	0,36	0,72	2,66	8,48	13,49	1825476
Швеція	SWE	1,78	0,01	0,01	0,2	0,03	1,435	3,34	1,54	0,28	0,18	0,38	0,19	0,05	3,35	3337
Великобританія	GBR	2,26	0,03	0,01	0,2	0,05	2,71	4,77	1,65	0,89	0,2	1,69	1,04	1,07	9,75	11228

Додаток Б

Таблиця Б.1 – Нормалізовані значення показників 1-ої та 2-ї групи

	X1_1	X1_2	X1_3	X1_4	X1_5	X1_6	X1_7	X1_8	X1_9	X2_1	X2_2	X2_3	X2_4
Албанія	0,3	-0,3	0,1	-0,3	0,0	0,3	0,8	0,3	-0,8	0,5	1,0	0,5	-1,0
Білорусь	0,0	0,3	-0,4	-0,8	-0,1	-0,3	-1,0	-0,8	0,0	-0,3	-0,1	1,0	-0,1
Хорватія	0,1	-0,6	0,2	-0,7	-0,3	0,0	0,3	-0,3	0,2	-0,3	0,6	0,3	-0,3
Кіпр	0,1	-0,9	-0,5	-0,5	-0,9	-1,0	-0,1	-0,8	-0,8	-0,4	-0,1	-0,3	0,6
Чехія	-0,1	-0,3	-0,4	0,3	-0,6	-0,2	-0,1	-0,1	0,6	-0,5	-0,1	0,1	-0,3
Данія	-0,3	-0,4	-0,8	-0,8	-0,9	0,0	0,3	-0,5	0,0	0,0	-0,6	-0,9	-0,3
Єгипет	0,0	0,4	-1,0	0,2	-0,4	0,2	-1,0	0,3	0,8	-0,5	0,1	0,7	-0,1
Естонія	-0,7	-0,7	-0,8	-1,0	-0,6	-0,7	-0,5	-0,5	0,6	-0,5	-0,1	-0,9	-0,1
Фінляндія	-0,9	-0,9	-1,0	-1,0	-0,9	-0,5	-0,3	-1,0	-0,2	-0,5	-1,0	-1,0	-0,8
Франція	0,3	0,1	-0,1	0,3	-0,3	0,3	0,6	0,1	0,2	0,3	0,6	-0,6	0,6
Грузія	-1,0	-1,0	-0,2	-0,3	-0,6	-0,5	-1,0	-1,0	-0,4	-0,6	-1,0	-0,6	-0,8
Німеччина	0,4	0,1	-0,8	-0,3	-0,8	-0,2	0,6	-0,5	0,4	0,0	0,6	-0,9	0,5
Греція	0,6	-0,6	-0,7	-0,7	-0,6	0,3	-0,5	-0,5	-1,0	-0,5	0,6	0,6	0,3
Угорщина	0,1	-0,6	-0,2	0,0	-0,5	-0,2	0,1	-0,3	0,2	-1,0	-0,6	0,5	-0,1
Італія	0,3	0,0	-0,5	-0,3	0,0	-0,2	1,0	-0,5	0,0	1,0	-1,0	0,3	0,6
Йорданія	0,0	0,3	-0,2	-0,3	-1,0	-0,5	-0,6	-0,1	0,4	-0,9	0,8	0,3	-0,3
Латвія	-0,6	-0,6	-1,0	-0,8	-0,9	-0,2	0,1	-0,3	0,0	-0,4	-0,8	-0,9	-0,3
Литва	-0,9	-0,9	-1,0	-0,8	-0,9	-0,3	-0,1	-0,8	-0,4	-0,4	-0,6	-0,3	-0,8
Мальта	-0,4	-0,9	-1,0	0,2	-0,1	-0,7	0,1	-0,6	0,2	-0,9	0,8	0,6	-0,1
Молдова	-0,4	-0,1	-0,5	-0,8	-0,6	-0,7	-0,8	-0,6	0,0	-0,3	-0,6	0,5	-0,1
Морокко	0,3	-0,7	-0,4	0,0	-0,6	-0,7	0,5	1,0	0,4	-1,0	0,6	0,5	-0,5
Нідерланди	-0,3	-0,1	-0,4	-0,2	-0,4	-0,3	0,8	-0,3	1,0	-0,1	0,3	-0,7	-0,3
Норвегія	-0,6	-0,6	-0,5	-0,2	-0,5	0,0	-0,1	-0,8	-0,2	-0,1	-0,6	-0,9	-0,5
Польща	-0,3	-0,6	-0,7	-0,7	0,0	-0,3	-0,1	-0,3	0,6	-0,8	0,1	-0,5	-0,6
Португалія	-0,4	-0,4	-0,2	-0,3	-0,6	-0,2	0,1	-0,6	-0,2	-0,1	0,3	-0,2	-0,1
Росія	0,1	-0,3	1,0	1,0	-0,1	0,7	-0,1	-0,5	1,0	-0,1	1,0	0,9	-0,1
Сербія	0,3	0,6	-0,1	-0,2	-0,4	0,7	0,3	-0,1	0,4	0,3	0,8	0,7	0,5
Словенія	0,0	-0,6	-0,7	-0,5	-0,8	-0,3	-0,1	-0,5	0,2	-0,5	-0,3	0,2	-0,1
Іспанія	0,4	-0,4	-0,2	0,2	-0,9	0,5	0,8	0,3	-0,4	0,3	0,6	-0,1	0,8
Швеція	0,0	0,1	-0,7	-0,3	-0,9	-0,3	-0,1	-0,5	0,2	0,1	0,1	-0,7	0,3
Туніс	0,4	-0,1	-0,2	-0,3	-0,1	-1,0	-0,6	-0,5	-0,4	-1,0	-0,6	0,1	-0,8
Туреччина	1,0	1,0	-0,1	-0,5	1,0	1,0	-0,3	-0,5	0,2	0,8	1,0	1,0	-0,1
Україна	0,3	0,7	0,7	-0,2	0,4	0,0	-0,5	-0,5	-0,6	0,3	0,8	0,7	0,3
Великобританія	-0,1	-0,6	-0,5	-0,2	-0,9	-0,2	0,6	-0,6	0,2	-0,3	0,6	-0,6	1,0

Додаток В

Результати побудови нейромережевих моделей для оцінювання ризику фінансового кібершахрайства

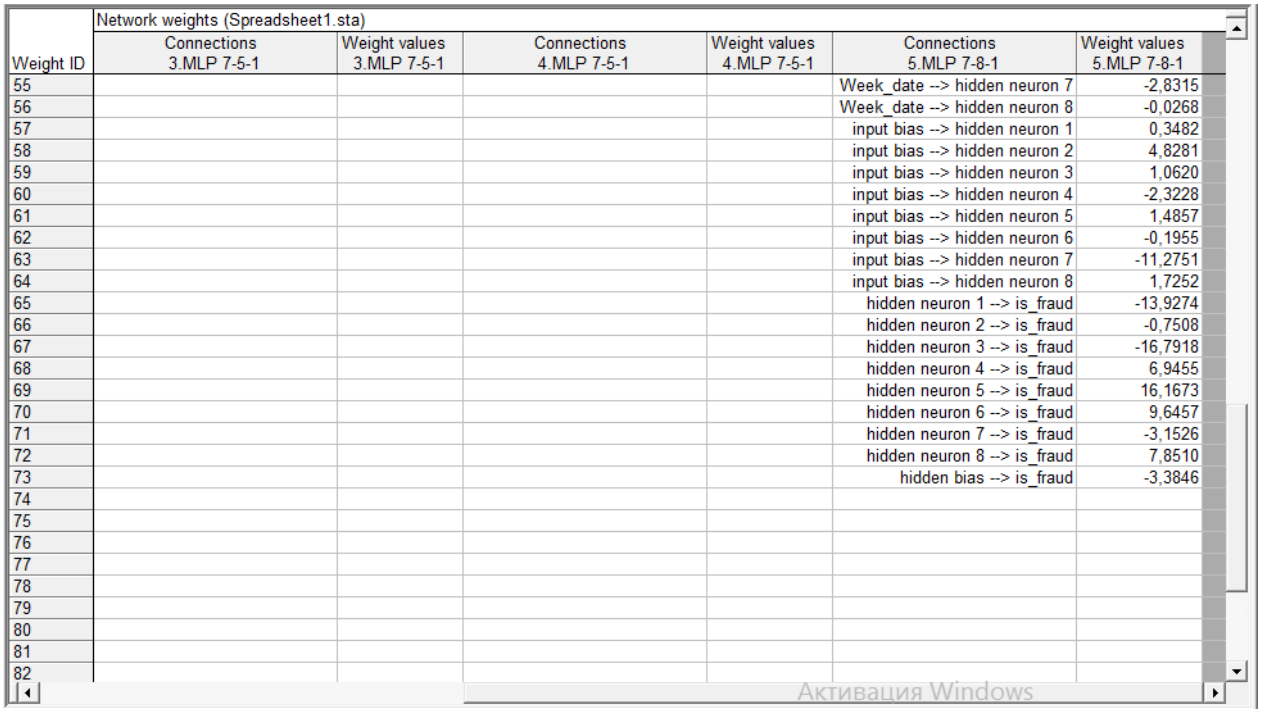
Network weights (Spreadsheet1.sta)

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 В.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 В.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

Додаток Г

Таблиця Г.1 – Індикатори, що характеризують рівень кібервразливості споживачів фінансових послуг

	R1	R2	R3	R4	R5	R6	R7	R8	R9	R10	R11	R12	R13	R14	R15	R16	R17
BE	46%	46%	27%	9%	27%	14%	43%	28%	50%	49%	7%	29%	17%	27%	1%	54%	29%
BG	32%	52%	15%	11%	25%	9%	32%	17%	36%	32%	2%	22%	7%	12%	7%	66%	19%
CZ	36%	37%	27%	7%	26%	6%	31%	23%	43%	34%	5%	24%	7%	19%	2%	54%	24%
DK	27%	39%	25%	2%	41%	19%	34%	41%	59%	58%	9%	27%	25%	31%	6%	19%	14%
D-W	42%	57%	35%	3%	50%	17%	25%	43%	51%	59%	18%	36%	17%	31%	2%	41%	22%
DE	41%	57%	36%	4%	48%	17%	26%	42%	50%	57%	17%	34%	16%	30%	4%	42%	20%
D-E	39%	55%	41%	6%	39%	14%	32%	36%	45%	49%	15%	24%	9%	26%	10%	50%	15%
EE	25%	33%	34%	3%	33%	16%	41%	32%	64%	50%	12%	27%	18%	23%	6%	42%	24%
IE	52%	53%	36%	11%	28%	18%	35%	30%	38%	35%	9%	25%	14%	26%	2%	39%	28%
EL	44%	57%	23%	22%	40%	9%	46%	15%	47%	56%	4%	16%	4%	17%	4%	57%	40%
ES	49%	53%	20%	8%	19%	7%	26%	21%	33%	29%	5%	17%	8%	22%	9%	55%	14%
FR	43%	49%	31%	7%	24%	14%	42%	29%	50%	45%	8%	35%	13%	29%	4%	46%	17%
HR	40%	49%	13%	9%	24%	8%	22%	15%	27%	30%	14%	14%	5%	15%	1%	60%	30%
IT	41%	40%	23%	8%	18%	8%	27%	18%	31%	29%	4%	15%	8%	12%	2%	67%	22%
CY	43%	60%	22%	16%	39%	6%	44%	22%	47%	33%	6%	17%	5%	17%	7%	50%	24%
LV	29%	38%	49%	2%	23%	8%	35%	27%	43%	34%	8%	18%	12%	15%	10%	50%	24%
LT	36%	44%	39%	12%	42%	5%	37%	17%	45%	57%	6%	20%	10%	16%	4%	42%	17%
LU	42%	44%	34%	9%	26%	17%	35%	31%	55%	51%	9%	37%	22%	28%	3%	37%	30%
HU	35%	31%	18%	12%	20%	9%	20%	13%	25%	33%	9%	17%	8%	13%	1%	59%	23%
MT	31%	45%	26%	4%	19%	11%	44%	34%	45%	45%	3%	29%	10%	22%	4%	32%	44%
NL	44%	48%	39%	5%	59%	22%	45%	56%	64%	60%	7%	42%	31%	46%	3%	27%	31%
AT	27%	34%	41%	12%	32%	20%	25%	28%	42%	54%	14%	30%	20%	23%	6%	46%	34%
PL	24%	32%	31%	6%	25%	8%	27%	19%	35%	33%	6%	17%	10%	17%	1%	43%	20%
PT	32%	54%	15%	11%	33%	10%	34%	20%	43%	35%	2%	15%	4%	15%	13%	57%	18%
RO	40%	34%	10%	13%	13%	6%	13%	14%	23%	28%	5%	18%	7%	13%	4%	67%	14%
SI	43%	47%	22%	9%	28%	11%	33%	23%	46%	42%	5%	20%	5%	20%	7%	56%	25%
SK	37%	31%	24%	3%	16%	6%	29%	15%	35%	45%	3%	17%	5%	18%	2%	54%	23%
FI	39%	43%	28%	2%	42%	28%	36%	46%	59%	53%	10%	37%	22%	22%	5%	31%	34%
SE	42%	43%	26%	6%	55%	30%	37%	51%	60%	52%	30%	40%	34%	37%	2%	28%	18%
UK	46%	44%	42%	10%	29%	19%	35%	34%	40%	36%	6%	27%	16%	21%	3%	29%	32%

Таблиця Г.2 – Асоціативні правила причинно-наслідковості зв’язків між індикаторами кібервразливості споживачів фінансових послуг

Body	==>	Head	Support, %	Confidence, %
0,053493<AEP1<=0,087964	==>	0,036834<HS1<=0,053611	20,00000	55,5556
0,036834<HS1<=0,053611	==>	0,053493<AEP1<=0,087964	20,00000	71,4286
0,056192<MS2<=0,071812	==>	0,053493<AEP1<=0,087964	20,00000	83,3333
0,053493<AEP1<=0,087964	==>	0,056192<MS2<=0,071812	20,00000	55,5556
0,019518<HC3<=0,040831	==>	0,053493<AEP1<=0,087964	20,00000	55,5556
0,053493<AEP1<=0,087964	==>	0,019518<HC3<=0,040831	20,00000	55,5556
0,019420<G2<=0,039332	==>	0,053493<AEP1<=0,087964	20,00000	62,5000
0,053493<AEP1<=0,087964	==>	0,019420<G2<=0,039332	20,00000	55,5556
0,023606<DPB2<=0,051124	==>	0,019420<G2<=0,039332	24,00000	75,0000
0,019420<G2<=0,039332	==>	0,023606<DPB2<=0,051124	24,00000	75,0000
0,023606<DPB2<=0,051124	==>	0,019420<G2<=0,039332, 0,019518<HC3<=0,040831	20,00000	62,5000
0,019518<HC3<=0,040831	==>	0,019420<G2<=0,039332, 0,023606<DPB2<=0,051124	20,00000	55,5556
0,019518<HC3<=0,040831, 0,023606<DPB2<=0,051124	==>	0,019420<G2<=0,039332	20,00000	83,3333
0,019420<G2<=0,039332	==>	0,019518<HC3<=0,040831, 0,023606<DPB2<=0,051124	20,00000	62,5000
0,019420<G2<=0,039332, 0,023606<DPB2<=0,051124	==>	0,019518<HC3<=0,040831	20,00000	83,3333
0,019420<G2<=0,039332, 0,019518<HC3<=0,040831	==>	0,023606<DPB2<=0,051124	20,00000	71,4286
0,023606<DPB2<=0,051124	==>	0,019420<G2<=0,039332, 0,023642<HS4<=0,045705	20,00000	62,5000
0,023642<HS4<=0,045705	==>	0,019420<G2<=0,039332, 0,023606<DPB2<=0,051124	20,00000	83,3333
0,023642<HS4<=0,045705, 0,023606<DPB2<=0,051124	==>	0,019420<G2<=0,039332	20,00000	83,3333
0,019420<G2<=0,039332	==>	0,023642<HS4<=0,045705, 0,023606<DPB2<=0,051124	20,00000	62,5000
0,019420<G2<=0,039332, 0,023606<DPB2<=0,051124	==>	0,023642<HS4<=0,045705	20,00000	83,3333
0,019420<G2<=0,039332, 0,023642<HS4<=0,045705	==>	0,023606<DPB2<=0,051124	20,00000	100,0000
0,023606<DPB2<=0,051124	==>	0,019420<G2<=0,039332, 0,023642<HS4<=0,045705, 0,019518<HC3<=0,040831	20,00000	62,5000
0,019518<HC3<=0,040831	==>	0,019420<G2<=0,039332, 0,023642<HS4<=0,045705, 0,023606<DPB2<=0,051124	20,00000	55,5556
0,019518<HC3<=0,040831, 0,023606<DPB2<=0,051124	==>	0,019420<G2<=0,039332, 0,023642<HS4<=0,045705	20,00000	83,3333
0,023642<HS4<=0,045705	==>	0,019420<G2<=0,039332, 0,019518<HC3<=0,040831, 0,023606<DPB2<=0,051124	20,00000	83,3333
0,023642<HS4<=0,045705, 0,023606<DPB2<=0,051124	==>	0,019420<G2<=0,039332, 0,019518<HC3<=0,040831	20,00000	83,3333
0,023642<HS4<=0,045705, 0,019518<HC3<=0,040831	==>	0,019420<G2<=0,039332, 0,023606<DPB2<=0,051124	20,00000	83,3333
0,023642<HS4<=0,045705, 0,019518<HC3<=0,040831, 0,023606<DPB2<=0,051124	==>	0,019420<G2<=0,039332	20,00000	83,3333

Body	==>	Head	Support, %	Confidence, %
0,019420<G2<=0,039332	==>	0,023642<HS4<=0,045705, 0,019518<HC3<=0,040831, 0,023606<DPB2<=0,051124	20,00000	62,5000
0,019420<G2<=0,039332, 0,023606<DPB2<=0,051124	==>	0,023642<HS4<=0,045705, 0,019518<HC3<=0,040831	20,00000	83,3333
0,019420<G2<=0,039332, 0,019518<HC3<=0,040831	==>	0,023642<HS4<=0,045705, 0,023606<DPB2<=0,051124	20,00000	71,4286
0,019420<G2<=0,039332, 0,019518<HC3<=0,040831, 0,023606<DPB2<=0,051124	==>	0,023642<HS4<=0,045705	20,00000	100,0000
0,019420<G2<=0,039332, 0,023642<HS4<=0,045705	==>	0,019518<HC3<=0,040831, 0,023606<DPB2<=0,051124	20,00000	100,0000
0,019420<G2<=0,039332, 0,023642<HS4<=0,045705, 0,023606<DPB2<=0,051124	==>	0,019518<HC3<=0,040831	20,00000	100,0000
0,019420<G2<=0,039332, 0,023642<HS4<=0,045705, 0,019518<HC3<=0,040831	==>	0,023606<DPB2<=0,051124	20,00000	100,0000
0,019518<HC3<=0,040831	==>	0,019420<G2<=0,039332	28,00000	77,7778
0,019420<G2<=0,039332	==>	0,019518<HC3<=0,040831	28,00000	87,5000
0,019518<HC3<=0,040831	==>	0,019420<G2<=0,039332, 0,012580<HC2<=0,033788	20,00000	55,5556
0,012580<HC2<=0,033788	==>	0,019420<G2<=0,039332, 0,019518<HC3<=0,040831	20,00000	71,4286
0,012580<HC2<=0,033788, 0,019518<HC3<=0,040831	==>	0,019420<G2<=0,039332	20,00000	83,3333
0,019420<G2<=0,039332	==>	0,012580<HC2<=0,033788, 0,019518<HC3<=0,040831	20,00000	62,5000
0,019420<G2<=0,039332, 0,019518<HC3<=0,040831	==>	0,012580<HC2<=0,033788	20,00000	71,4286
0,019420<G2<=0,039332, 0,012580<HC2<=0,033788	==>	0,019518<HC3<=0,040831	20,00000	100,0000
0,019518<HC3<=0,040831	==>	0,019420<G2<=0,039332, 0,023642<HS4<=0,045705	20,00000	55,5556
0,023642<HS4<=0,045705	==>	0,019420<G2<=0,039332, 0,019518<HC3<=0,040831	20,00000	83,3333
0,023642<HS4<=0,045705, 0,019518<HC3<=0,040831	==>	0,019420<G2<=0,039332	20,00000	83,3333
0,019420<G2<=0,039332	==>	0,023642<HS4<=0,045705, 0,019518<HC3<=0,040831	20,00000	62,5000
0,019420<G2<=0,039332, 0,019518<HC3<=0,040831	==>	0,023642<HS4<=0,045705	20,00000	71,4286
0,019420<G2<=0,039332, 0,023642<HS4<=0,045705	==>	0,019518<HC3<=0,040831	20,00000	100,0000
0,019518<HC3<=0,040831	==>	0,019420<G2<=0,039332, 0,021421<MS1<=0,042453	20,00000	55,5556
0,021421<MS1<=0,042453	==>	0,019420<G2<=0,039332, 0,019518<HC3<=0,040831	20,00000	83,3333
0,021421<MS1<=0,042453, 0,019518<HC3<=0,040831	==>	0,019420<G2<=0,039332	20,00000	83,3333
0,019420<G2<=0,039332	==>	0,021421<MS1<=0,042453, 0,019518<HC3<=0,040831	20,00000	62,5000
0,019420<G2<=0,039332, 0,019518<HC3<=0,040831	==>	0,021421<MS1<=0,042453	20,00000	71,4286
0,019420<G2<=0,039332, 0,021421<MS1<=0,042453	==>	0,019518<HC3<=0,040831	20,00000	100,0000

Body	==>	Head	Support, %	Confidence, %
0,019518<HC3<=0,040831	==>	0,019420<G2<=0,039332, 0,011420<A5<=0,034840	20,00000	55,5556
0,011420<A5<=0,034840	==>	0,019420<G2<=0,039332, 0,019518<HC3<=0,040831	20,00000	83,3333
0,011420<A5<=0,034840, 0,019518<HC3<=0,040831	==>	0,019420<G2<=0,039332	20,00000	100,0000
0,019420<G2<=0,039332	==>	0,011420<A5<=0,034840, 0,019518<HC3<=0,040831	20,00000	62,5000
0,019420<G2<=0,039332, 0,019518<HC3<=0,040831	==>	0,011420<A5<=0,034840	20,00000	71,4286
0,019420<G2<=0,039332, 0,011420<A5<=0,034840	==>	0,019518<HC3<=0,040831	20,00000	100,0000
0,012580<HC2<=0,033788	==>	0,019420<G2<=0,039332	20,00000	71,4286
0,019420<G2<=0,039332	==>	0,012580<HC2<=0,033788	20,00000	62,5000
0,023642<HS4<=0,045705	==>	0,019420<G2<=0,039332	20,00000	83,3333
0,019420<G2<=0,039332	==>	0,023642<HS4<=0,045705	20,00000	62,5000
0,021421<MS1<=0,042453	==>	0,019420<G2<=0,039332	20,00000	83,3333
0,019420<G2<=0,039332	==>	0,021421<MS1<=0,042453	20,00000	62,5000
0,017056<SPC5<=0,039673	==>	0,019420<G2<=0,039332	20,00000	62,5000
0,019420<G2<=0,039332	==>	0,017056<SPC5<=0,039673	20,00000	62,5000
0,011420<A5<=0,034840	==>	0,019420<G2<=0,039332	20,00000	83,3333
0,019420<G2<=0,039332	==>	0,011420<A5<=0,034840	20,00000	62,5000
0,019518<HC3<=0,040831	==>	0,011420<A5<=0,034840	20,00000	55,5556
0,011420<A5<=0,034840	==>	0,019518<HC3<=0,040831	20,00000	83,3333
0,019529<DAI4<=0,038758	==>	0,017056<SPC5<=0,039673	20,00000	71,4286
0,017056<SPC5<=0,039673	==>	0,019529<DAI4<=0,038758	20,00000	62,5000
0,023606<DPB2<=0,051124	==>	0,017056<SPC5<=0,039673	24,00000	75,0000
0,017056<SPC5<=0,039673	==>	0,023606<DPB2<=0,051124	24,00000	75,0000
0,019518<HC3<=0,040831	==>	0,017056<SPC5<=0,039673	24,00000	66,6667
0,017056<SPC5<=0,039673	==>	0,019518<HC3<=0,040831	24,00000	75,0000
0,023606<DPB2<=0,051124	==>	0,021421<MS1<=0,042453	20,00000	62,5000
0,021421<MS1<=0,042453	==>	0,023606<DPB2<=0,051124	20,00000	83,3333
0,023606<DPB2<=0,051124	==>	0,021421<MS1<=0,042453, 0,019518<HC3<=0,040831	20,00000	62,5000
0,019518<HC3<=0,040831	==>	0,021421<MS1<=0,042453, 0,023606<DPB2<=0,051124	20,00000	55,5556
0,019518<HC3<=0,040831, 0,023606<DPB2<=0,051124	==>	0,021421<MS1<=0,042453	20,00000	83,3333
0,021421<MS1<=0,042453	==>	0,019518<HC3<=0,040831, 0,023606<DPB2<=0,051124	20,00000	83,3333
0,021421<MS1<=0,042453, 0,023606<DPB2<=0,051124	==>	0,019518<HC3<=0,040831	20,00000	100,0000
0,021421<MS1<=0,042453, 0,019518<HC3<=0,040831	==>	0,023606<DPB2<=0,051124	20,00000	83,3333
0,023606<DPB2<=0,051124	==>	0,021421<MS1<=0,042453, 0,023642<HS4<=0,045705	20,00000	62,5000
0,023642<HS4<=0,045705	==>	0,021421<MS1<=0,042453, 0,023606<DPB2<=0,051124	20,00000	83,3333
0,023642<HS4<=0,045705, 0,023606<DPB2<=0,051124	==>	0,021421<MS1<=0,042453	20,00000	83,3333
0,021421<MS1<=0,042453	==>	0,023642<HS4<=0,045705, 0,023606<DPB2<=0,051124	20,00000	83,3333
0,021421<MS1<=0,042453, 0,023606<DPB2<=0,051124	==>	0,023642<HS4<=0,045705	20,00000	100,0000

Body	==>	Head	Support, %	Confidence, %
0,021421<MS1<=0,042453, 0,023642<HS4<=0,045705	==>	0,023606<DPB2<=0,051124	20,00000	100,0000
0,023606<DPB2<=0,051124	==>	0,021421<MS1<=0,042453, 0,023642<HS4<=0,045705, 0,019518<HC3<=0,040831	20,00000	62,5000
0,019518<HC3<=0,040831	==>	0,021421<MS1<=0,042453, 0,023642<HS4<=0,045705, 0,023606<DPB2<=0,051124	20,00000	55,5556
0,019518<HC3<=0,040831, 0,023606<DPB2<=0,051124	==>	0,021421<MS1<=0,042453, 0,023642<HS4<=0,045705	20,00000	83,3333
0,023642<HS4<=0,045705	==>	0,021421<MS1<=0,042453, 0,019518<HC3<=0,040831, 0,023606<DPB2<=0,051124	20,00000	83,3333
0,023642<HS4<=0,045705, 0,023606<DPB2<=0,051124	==>	0,021421<MS1<=0,042453, 0,019518<HC3<=0,040831	20,00000	83,3333
0,023642<HS4<=0,045705, 0,019518<HC3<=0,040831	==>	0,021421<MS1<=0,042453, 0,023606<DPB2<=0,051124	20,00000	83,3333
0,023642<HS4<=0,045705, 0,019518<HC3<=0,040831, 0,023606<DPB2<=0,051124	==>	0,021421<MS1<=0,042453	20,00000	83,3333
0,021421<MS1<=0,042453	==>	0,023642<HS4<=0,045705, 0,019518<HC3<=0,040831, 0,023606<DPB2<=0,051124	20,00000	83,3333
0,021421<MS1<=0,042453, 0,023606<DPB2<=0,051124	==>	0,023642<HS4<=0,045705, 0,019518<HC3<=0,040831	20,00000	100,0000
0,021421<MS1<=0,042453, 0,019518<HC3<=0,040831	==>	0,023642<HS4<=0,045705, 0,023606<DPB2<=0,051124	20,00000	83,3333
0,021421<MS1<=0,042453, 0,019518<HC3<=0,040831, 0,023606<DPB2<=0,051124	==>	0,023642<HS4<=0,045705	20,00000	100,0000
0,021421<MS1<=0,042453, 0,023642<HS4<=0,045705	==>	0,019518<HC3<=0,040831, 0,023606<DPB2<=0,051124	20,00000	100,0000
0,021421<MS1<=0,042453, 0,023642<HS4<=0,045705, 0,023606<DPB2<=0,051124	==>	0,019518<HC3<=0,040831	20,00000	100,0000
0,021421<MS1<=0,042453, 0,023642<HS4<=0,045705, 0,019518<HC3<=0,040831	==>	0,023606<DPB2<=0,051124	20,00000	100,0000
0,019518<HC3<=0,040831	==>	0,021421<MS1<=0,042453	24,00000	66,6667
0,021421<MS1<=0,042453	==>	0,019518<HC3<=0,040831	24,00000	100,0000
0,019518<HC3<=0,040831	==>	0,021421<MS1<=0,042453, 0,012580<HC2<=0,033788	20,00000	55,5556
0,012580<HC2<=0,033788	==>	0,021421<MS1<=0,042453, 0,019518<HC3<=0,040831	20,00000	71,4286
0,012580<HC2<=0,033788, 0,019518<HC3<=0,040831	==>	0,021421<MS1<=0,042453	20,00000	83,3333
0,021421<MS1<=0,042453	==>	0,012580<HC2<=0,033788, 0,019518<HC3<=0,040831	20,00000	83,3333
0,021421<MS1<=0,042453, 0,019518<HC3<=0,040831	==>	0,012580<HC2<=0,033788	20,00000	83,3333
0,021421<MS1<=0,042453, 0,012580<HC2<=0,033788	==>	0,019518<HC3<=0,040831	20,00000	100,0000
0,019518<HC3<=0,040831	==>	0,021421<MS1<=0,042453, 0,023642<HS4<=0,045705	20,00000	55,5556
0,023642<HS4<=0,045705	==>	0,021421<MS1<=0,042453, 0,019518<HC3<=0,040831	20,00000	83,3333

Body	==>	Head	Support, %	Confidence, %
0,023642<HS4<=0,045705, 0,019518<HC3<=0,040831	==>	0,021421<MS1<=0,042453	20,00000	83,3333
0,021421<MS1<=0,042453	==>	0,023642<HS4<=0,045705, 0,019518<HC3<=0,040831	20,00000	83,3333
0,021421<MS1<=0,042453, 0,019518<HC3<=0,040831	==>	0,023642<HS4<=0,045705	20,00000	83,3333
0,021421<MS1<=0,042453, 0,023642<HS4<=0,045705	==>	0,019518<HC3<=0,040831	20,00000	100,0000
0,012580<HC2<=0,033788	==>	0,021421<MS1<=0,042453	20,00000	71,4286
0,021421<MS1<=0,042453	==>	0,012580<HC2<=0,033788	20,00000	83,3333
0,023642<HS4<=0,045705	==>	0,021421<MS1<=0,042453	20,00000	83,3333
0,021421<MS1<=0,042453	==>	0,023642<HS4<=0,045705	20,00000	83,3333
0,019518<HC3<=0,040831	==>	0,001923<HS3<=0,020802	20,00000	55,5556
0,001923<HS3<=0,020802	==>	0,019518<HC3<=0,040831	20,00000	100,0000
0,023606<DPB2<=0,051124	==>	0,023642<HS4<=0,045705	24,00000	75,0000
0,023642<HS4<=0,045705	==>	0,023606<DPB2<=0,051124	24,00000	100,0000
0,023606<DPB2<=0,051124	==>	0,023642<HS4<=0,045705, 0,019518<HC3<=0,040831	24,00000	75,0000
0,019518<HC3<=0,040831	==>	0,023642<HS4<=0,045705, 0,023606<DPB2<=0,051124	24,00000	66,6667
0,019518<HC3<=0,040831, 0,023606<DPB2<=0,051124	==>	0,023642<HS4<=0,045705	24,00000	100,0000
0,023642<HS4<=0,045705	==>	0,019518<HC3<=0,040831, 0,023606<DPB2<=0,051124	24,00000	100,0000
0,023642<HS4<=0,045705, 0,023606<DPB2<=0,051124	==>	0,019518<HC3<=0,040831	24,00000	100,0000
0,023642<HS4<=0,045705, 0,019518<HC3<=0,040831	==>	0,023606<DPB2<=0,051124	24,00000	100,0000
0,023606<DPB2<=0,051124	==>	0,023642<HS4<=0,045705, 0,012580<HC2<=0,033788	20,00000	62,5000
0,012580<HC2<=0,033788	==>	0,023642<HS4<=0,045705, 0,023606<DPB2<=0,051124	20,00000	71,4286
0,012580<HC2<=0,033788, 0,023606<DPB2<=0,051124	==>	0,023642<HS4<=0,045705	20,00000	100,0000
0,023642<HS4<=0,045705	==>	0,012580<HC2<=0,033788, 0,023606<DPB2<=0,051124	20,00000	83,3333
0,023642<HS4<=0,045705, 0,023606<DPB2<=0,051124	==>	0,012580<HC2<=0,033788	20,00000	83,3333
0,023642<HS4<=0,045705, 0,012580<HC2<=0,033788	==>	0,023606<DPB2<=0,051124	20,00000	100,0000
0,023606<DPB2<=0,051124	==>	0,023642<HS4<=0,045705, 0,012580<HC2<=0,033788, 0,019518<HC3<=0,040831	20,00000	62,5000
0,019518<HC3<=0,040831	==>	0,023642<HS4<=0,045705, 0,012580<HC2<=0,033788, 0,023606<DPB2<=0,051124	20,00000	55,5556
0,019518<HC3<=0,040831, 0,023606<DPB2<=0,051124	==>	0,023642<HS4<=0,045705, 0,012580<HC2<=0,033788	20,00000	83,3333
0,012580<HC2<=0,033788	==>	0,023642<HS4<=0,045705, 0,019518<HC3<=0,040831, 0,023606<DPB2<=0,051124	20,00000	71,4286
0,012580<HC2<=0,033788, 0,023606<DPB2<=0,051124	==>	0,023642<HS4<=0,045705, 0,019518<HC3<=0,040831	20,00000	100,0000
0,012580<HC2<=0,033788, 0,019518<HC3<=0,040831	==>	0,023642<HS4<=0,045705, 0,023606<DPB2<=0,051124	20,00000	83,3333

Body	==>	Head	Support, %	Confidence, %
0,012580<HC2<=0,033788, 0,019518<HC3<=0,040831, 0,023606<DPB2<=0,051124	==>	0,023642<HS4<=0,045705	20,00000	100,0000
0,023642<HS4<=0,045705	==>	0,012580<HC2<=0,033788, 0,019518<HC3<=0,040831, 0,023606<DPB2<=0,051124	20,00000	83,3333
0,023642<HS4<=0,045705, 0,023606<DPB2<=0,051124	==>	0,012580<HC2<=0,033788, 0,019518<HC3<=0,040831	20,00000	83,3333
0,023642<HS4<=0,045705, 0,019518<HC3<=0,040831	==>	0,012580<HC2<=0,033788, 0,023606<DPB2<=0,051124	20,00000	83,3333
0,023642<HS4<=0,045705, 0,019518<HC3<=0,040831, 0,023606<DPB2<=0,051124	==>	0,012580<HC2<=0,033788	20,00000	83,3333
0,023642<HS4<=0,045705, 0,012580<HC2<=0,033788	==>	0,019518<HC3<=0,040831, 0,023606<DPB2<=0,051124	20,00000	100,0000
0,023642<HS4<=0,045705, 0,012580<HC2<=0,033788, 0,023606<DPB2<=0,051124	==>	0,019518<HC3<=0,040831	20,00000	100,0000
0,023642<HS4<=0,045705, 0,012580<HC2<=0,033788, 0,019518<HC3<=0,040831	==>	0,023606<DPB2<=0,051124	20,00000	100,0000
0,019518<HC3<=0,040831	==>	0,023642<HS4<=0,045705	24,00000	66,6667
0,023642<HS4<=0,045705	==>	0,019518<HC3<=0,040831	24,00000	100,0000
0,019518<HC3<=0,040831	==>	0,023642<HS4<=0,045705, 0,012580<HC2<=0,033788	20,00000	55,5556
0,012580<HC2<=0,033788	==>	0,023642<HS4<=0,045705, 0,019518<HC3<=0,040831	20,00000	71,4286
0,012580<HC2<=0,033788, 0,019518<HC3<=0,040831	==>	0,023642<HS4<=0,045705	20,00000	83,3333
0,023642<HS4<=0,045705	==>	0,012580<HC2<=0,033788, 0,019518<HC3<=0,040831	20,00000	83,3333
0,023642<HS4<=0,045705, 0,019518<HC3<=0,040831	==>	0,012580<HC2<=0,033788	20,00000	83,3333
0,023642<HS4<=0,045705, 0,012580<HC2<=0,033788	==>	0,019518<HC3<=0,040831	20,00000	100,0000
0,012580<HC2<=0,033788	==>	0,023642<HS4<=0,045705	20,00000	71,4286
0,023606<DPB2<=0,051124	==>	0,012580<HC2<=0,033788	20,00000	62,5000
0,012580<HC2<=0,033788	==>	0,023606<DPB2<=0,051124	20,00000	71,4286
0,023606<DPB2<=0,051124	==>	0,012580<HC2<=0,033788, 0,019518<HC3<=0,040831	20,00000	62,5000
0,019518<HC3<=0,040831	==>	0,012580<HC2<=0,033788, 0,023606<DPB2<=0,051124	20,00000	55,5556
0,019518<HC3<=0,040831, 0,023606<DPB2<=0,051124	==>	0,012580<HC2<=0,033788	20,00000	83,3333
0,012580<HC2<=0,033788	==>	0,019518<HC3<=0,040831, 0,023606<DPB2<=0,051124	20,00000	71,4286
0,012580<HC2<=0,033788, 0,023606<DPB2<=0,051124	==>	0,019518<HC3<=0,040831	20,00000	100,0000
0,012580<HC2<=0,033788, 0,019518<HC3<=0,040831	==>	0,023606<DPB2<=0,051124	20,00000	83,3333
0,019518<HC3<=0,040831	==>	0,012580<HC2<=0,033788	24,00000	66,6667
0,012580<HC2<=0,033788	==>	0,019518<HC3<=0,040831	24,00000	85,7143
0,012587<SU2<=0,031392	==>	0,019518<HC3<=0,040831	20,00000	83,3333

Body	==>	Head	Support, %	Confidence, %
0,019518<HC3<=0,040831	==>	0,012587<SU2<=0,031392	20,00000	55,5556
0,037186<SU1<=0,059862	==>	0,019518<HC3<=0,040831	20,00000	100,0000
0,019518<HC3<=0,040831	==>	0,037186<SU1<=0,059862	20,00000	55,5556
0,016892<A6<=0,035008	==>	0,019518<HC3<=0,040831	20,00000	100,0000
0,019518<HC3<=0,040831	==>	0,016892<A6<=0,035008	20,00000	55,5556
0,019529<DAI4<=0,038758	==>	0,019518<HC3<=0,040831	20,00000	71,4286
0,019518<HC3<=0,040831	==>	0,019529<DAI4<=0,038758	20,00000	55,5556
0,023606<DPB2<=0,051124	==>	0,019518<HC3<=0,040831	24,00000	75,0000
0,019518<HC3<=0,040831	==>	0,023606<DPB2<=0,051124	24,00000	66,6667
0,019529<DAI4<=0,038758	==>	0,023606<DPB2<=0,051124	20,00000	71,4286
0,023606<DPB2<=0,051124	==>	0,019529<DAI4<=0,038758	20,00000	62,5000
0,045453<C3<=0,066084	==>	0,036882<C2<=0,061094	20,00000	100,0000
0,036882<C2<=0,061094	==>	0,045453<C3<=0,066084	20,00000	83,3333

Додаток Д

Таблиця Д.1 – Вхідні дані оцінювання ефективності інституційних змін у системі протидії легалізації кримінальних доходів на основі побудови таблиць виживаності

Дата початку вчинення злочину	Дата вироку суду	Day_1	Month_1	Year_1	Day_1	Month_1	Year_1	Суміжні статті	NRA	ALL	FSR	ND	NIILE	Censored	NYCV
21.02.2022	03.08.2022	21	2	2022	3	8	2022	190	1	37755,47	0	2	26	1	3
15.08.2019	29.07.2022	15	8	2019	29	7	2022	190	1	1416140	0	3	68	1	4
10.09.2018	26.10.2021	10	9	2018	26	10	2021	255	1	359345949,1	10983,68	1	12	1	5
29.12.2016	03.09.2021	29	12	2016	3	9	2021	191	1	131072	-5720	1	1	0	0
10.06.2020	23.10.2021	10	6	2020	23	10	2021	191	1	54700	0	1	4	0	0
01.09.2020	01.07.2021	1	9	2020	1	7	2021	200	1	257550,00	5000	1	0	1	5
01.07.2014	02.07.2019	1	7	2014	2	7	2019	205	1	1180080,00	47139	1	1	1	3
01.06.2019	05.10.2021	1	6	2019	5	10	2021	246	1	1080730,00	0	1	0	1	5
12.06.2017	30.08.2021	12	6	2017	30	8	2021	191	1	67229,19	0	1	0	1	3
04.04.2019	31.10.2019	4	4	2019	31	10	2019	369-2	1	16000,00	12750	1	0	1	3
01.08.2015	20.05.2019	1	8	2015	20	5	2019	205	1	195346709,95	0	2	0	1	5
02.09.2015	29.03.2019	2	9	2015	29	3	2019	205	1	1074833,00	803800	1	0	1	3
01.01.2014	20.05.2020	1	1	2014	20	5	2020	255	1	20426692,00	1059884,41	1	0	1	5
01.10.2019	19.10.2021	1	10	2019	19	10	2021	366, 246	2	1161220,28	0	1	0	1	5
01.01.2014	20.02.2020	1	1	2014	20	2	2020	255	1	49180588,00	2080786	1	0	1	5
01.01.2014	03.12.2019	1	1	2014	3	12	2019	255	1	33255064,00	850000	1	0	1	5
01.08.2019	29.12.2020	1	8	2019	29	12	2020	204, 366	2	127420	2615,2	1	0	1	3
01.03.2020	17.11.2020	1	3	2020	17	11	2020	190, 358	2	512679,00	0	1	1	1	5
01.07.2016	10.06.2021	1	7	2016	10	6	2021	212	1	10940221,00	255000	1	0	1	5
30.12.2015	10.12.2019	30	12	2015	10	12	2019	190, 358	2	1830770,00	13502,86	1	1	1	4
01.03.2020	12.03.2021	1	3	2020	12	3	2021	190, 358	2	876679	0	1	3	1	5

Дата початку вчинення злочину	Дата вироку суду	Day_1	Month_1	Year_1	Day_1	Month_1	Year_1	Суміжні статті	NRA	ALL	FSR	ND	NIILE	Censored	NYCV
01.12.2020	27.03.2022	1	12	2020	27	3	2022	190	1	447610	0	1	1	1	5
01.02.2017	13.01.2020	1	2	2017	13	1	2020	307, 255	2	33563227	0	1	0	1	2
19.04.2021	16.06.2021	19	4	2021	16	6	2021	119, 185	2	8530,73	7155,73	1	1	1	4
06.10.2016	15.06.2022	6	10	2016	15	6	2022	190, 358	2	4577500	5652	1	1	1	4
01.01.2019	08.11.2021	1	1	2019	8	11	2021	205-1, 366	2	93 363 870,92	0	1	0	1	5
01.06.2020	18.05.2021	1	6	2020	18	5	2021	190, 361	2	103 264	3922,08	1	1	1	6
15.08.2019	29.07.2022	15	8	2019	29	7	2022	190	1	1068000	0	3	67	1	4
06.01.2016	24.12.2020	6	1	2016	24	12	2020	200	1	3998900	140396	1	0	1	3
08.05.2015	02.09.2021	8	5	2015	2	9	2021		0	46 402 556,07	0	2	0	1	5
12.01.2016	15.06.2020	12	1	2016	15	6	2020	200	1	3227400	136000	1	0	1	3
01.01.2018	05.12.2019	1	1	2018	5	12	2019	255,307	2	32934053	3537678,128	1	0	1	2
23.03.2018	24.12.2021	23	3	2018	24	12	2021	200, 358	2	15152600	91280	1	0	1	5
01.01.2019	27.10.2021	1	1	2019	27	10	2021	204	1	2925562,44	24711,84	1	0	1	3
28.11.2017	13.06.2022	28	11	2017	13	6	2022	190, 358	2	506779,72	583625	1	0	0	0
02.05.2019	26.07.2021	2	5	2019	26	7	2021	191	1	273817,00	6280	1	1	1	5
04.06.2015	29.12.2021	4	6	2015	29	12	2021	240	1	1484795,6	10491,00	1	1	0	0
08.05.2015	06.10.2020	8	5	2015	6	10	2020	212	1	165155583,00	26275000,00	2	0	1	5
28.08.2006	22.09.2021	28	8	2006	22	9	2021	191, 366	2	5 353 266,26	-2368,80	2	0	0	0
01.02.2017	12.06.2019	1	2	2017	12	6	2019	255, 190, 205-1, 205	3	5175648	49643,96	2	15	1	5
10.08.2015	22.02.2022	10	8	2015	22	2	2022	191, 366	1	77538,07	0,00	1	1	0	0
15.02.2009	24.05.2022	15	2	2009	24	5	2022	190, 366	1	25365683	96160,00	2	1	0	0

Додаток К

Таблиця К.1 – Вхідні показники інституційного та освітнього каналів протидії легалізації доходів, отриманих незаконним шляхом

Рік	Inst1	Inst2	Inst3	Inst4	Inst5	Inst6	E1	E2	E3
2006	841589	47110	**618,008**	163	8	1	13,923	2740342	38,143
2007	1000848	53300	720,5	271	40	25	14,036	2819248	37,322
2008	1062373	65200	59,1	354	117	77	13,558	2847713	37,163
2009	877433	59900	5561,4	504	150	119	15,055	2798693	36,416
2010	806414	**57050**	213,4	345	106	65	**14,270**	2635004	35,278
2011	1079451	54200	344,9	203	142	37	13,484	2566279	33,236
2012	967821	98500	475,48	248	175	99	13,666	2390989	35,897
2013	982141	**213750**	598,68	813	177	115	13,868	2205595	**34,604**
2014	1287496	329000	3070,22	540	79	156	13,121	2146028	**33,084**
2015	4357117	87500	5492,61	356	58	70	13,341	1776190	32,017
2016	6319776	45800	21600	270	42	47	12,353	1689724	30,044
2017	8013029	59400	3342,2	306	63	115	13,019	1667288	14,419
2018	9969792	347400	**4356,1**	374	32	21	12,751	1614636	28,379
2019	11437374	92200	5370	354	74	78	13,160	1601557	27,164
2020	4725537	68000	2700	314	38	28	13,086	**1536736**	**26,464**

Таблиця К.2 – Вхідні показники інвестиційного та податкового каналів протидії легалізації доходів, отриманих незаконним шляхом

Рік	Invest1	Invest2	Invest3	Invest4	Invest5	T1	T2	T3	T4	T5
2006	24,543	-0,119	5,009	-3583000000	**57,695**	12,3	2085	57,3	5,6	113
2007	27,781	0,656	6,853	-5753000000	57,64	12,4	2085	57	3,4	113
2008	27,393	0,424	5,688	1280000000	56,79	12,5	2085	56,6	3,3	113
2009	17,068	0,095	3,923	1533000000	58,37	12,3	860	57,2	2,9	113
2010	18,372	0,490	4,568	-4342000000	56,46	12,3	736	57,2	2,6	113
2011	20,444	0,113	4,256	-1569000000	55,73	10,4	657	55,5	4,1	117
2012	19,615	0,537	4,477	-4689000000	57,14	12,2	657	57,1	3,9	117
2013	16,426	0,226	2,367	-8787000000	59,13	11,6	488	55,4	3,7	69
2014	13,396	0,410	0,634	2700000000	57,88	11,3	386	54,4	2,4	45
2015	15,933	0,042	-0,218	-367000000	59,12	9,5	346	52,7	2	27
2016	21,724	0,185	4,422	-293000000	57,62	9	346	52,2	2	16
2017	19,965	0,209	3,283	-1800000000	58,71	8,7	355,5	52,3	1,9	16
2018	18,588	0,089	3,801	-2080000000	57,03	11,9	327,5	37,8	1,8	16
2019	14,890	0,404	3,766	-5134000000	56,99	11	327,5	41,7	1,8	15
2020	8,932	0,231	0,194	829000000	**56,936**	10,2	327,5	45,2	1,7	15

Таблиця К.3 – Нормалізовані показники

Рік	Inst1 _norm	Inst2 _norm	Inst3 _norm	Inst4 _norm	Inst5 _norm	Inst6 _norm	E1 _norm	E2 _norm	E3 _norm
2006	0,003	0,004	0,026	0,000	0,000	0,000	0,581	0,918	1,000
2007	0,018	0,025	0,031	0,166	0,189	0,155	0,623	0,978	0,965
2008	0,024	0,064	0,000	0,294	0,645	0,490	0,446	1,000	0,959
2009	0,007	0,047	0,255	0,525	0,840	0,761	1,000	0,963	0,927
2010	0,000	0,037	0,007	0,280	0,580	0,413	0,709	0,838	0,879
2011	0,026	0,028	0,013	0,062	0,793	0,232	0,419	0,785	0,793
2012	0,015	0,175	0,019	0,131	0,988	0,632	0,486	0,652	0,905
2013	0,017	0,557	0,025	1,000	1,000	0,735	0,561	0,510	0,851
2014	0,045	0,939	0,140	0,580	0,420	1,000	0,284	0,465	0,787
2015	0,334	0,138	0,252	0,297	0,296	0,445	0,366	0,183	0,742
2016	0,519	0,000	1,000	0,165	0,201	0,297	0,000	0,117	0,659
2017	0,678	0,045	0,152	0,220	0,325	0,735	0,247	0,100	0,000
2018	0,862	1,000	0,199	0,325	0,142	0,129	0,147	0,059	0,588
2019	1,000	0,154	0,247	0,294	0,391	0,497	0,299	0,049	0,537
2020	0,369	0,074	0,123	0,232	0,178	0,174	0,271	0,000	0,508

Таблиця К.4 – Нормалізовані показники

Рік	Invest1 _norm	Invest2 _norm	Invest3 _norm	Invest4 _norm	Invest5 _norm	T1 _norm	T2 _norm	T3 _norm	T4 _norm	T5 _norm
2006	0,828	1,000	0,739	0,453	0,578	0,053	0,000	0,000	0,000	0,039
2007	1,000	0,000	1,000	0,264	0,562	0,026	0,000	0,015	0,564	0,039
2008	0,979	0,299	0,835	0,876	0,312	0,000	0,000	0,036	0,590	0,039
2009	0,432	0,724	0,586	0,898	0,776	0,053	0,697	0,005	0,692	0,039
2010	0,501	0,214	0,677	0,387	0,215	0,053	0,768	0,005	0,769	0,039
2011	0,611	0,700	0,633	0,628	0,000	0,553	0,813	0,092	0,385	0,000
2012	0,567	0,153	0,664	0,357	0,415	0,079	0,813	0,010	0,436	0,000
2013	0,398	0,555	0,366	0,000	1,000	0,237	0,909	0,097	0,487	0,471
2014	0,237	0,316	0,120	1,000	0,632	0,316	0,967	0,149	0,821	0,706
2015	0,371	0,793	0,000	0,733	0,997	0,789	0,989	0,236	0,923	0,882
2016	0,679	0,607	0,656	0,739	0,556	0,921	0,989	0,262	0,923	0,990
2017	0,585	0,577	0,495	0,608	0,876	1,000	0,984	0,256	0,949	0,990
2018	0,512	0,732	0,568	0,584	0,382	0,158	1,000	1,000	0,974	0,990
2019	0,316	0,325	0,563	0,318	0,371	0,395	1,000	0,800	0,974	1,000
2020	0,000	0,548	0,058	0,837	0,355	0,605	1,000	0,621	1,000	1,000

Eigenvalues of correlation matrix, and related statistics Active variables only				
Value number	Eigenvalue	% Total variance	Cumulative Eigenvalue	Cumulative %
1	3,490651	69,81302	3,490651	69,8130
2	0,764161	15,28321	4,254812	85,0962
3	0,382302	7,64605	4,637114	92,7423
4	0,289698	5,79395	4,926812	98,5362
5	0,073188	1,46377	5,000000	100,0000

Рисунок К.1 – Власні значення і відсоток поясненої дисперсії за методом головних компонент для податкового каналу

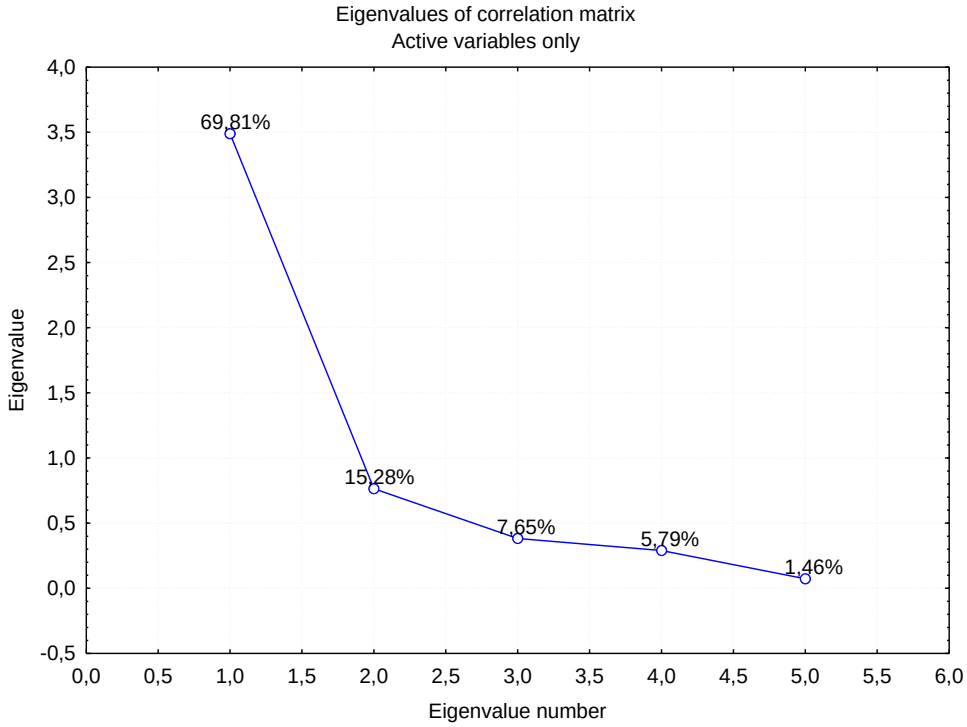


Рисунок К.2 – Графік кам’янистого осипу для податкового каналу

Variable contributions, based on correlations					
Variable	Factor 1	Factor 2	Factor 3	Factor 4	Factor 5
T1	0,154974	0,493308	0,175073	0,010224	0,166420
T2	0,197663	0,040884	0,633876	0,125247	0,002331
T3	0,168052	0,441904	0,043636	0,155511	0,190898
T4	0,219958	0,021461	0,025185	0,704348	0,029047
T5	0,259353	0,002444	0,122230	0,004669	0,611304

Рисунок К.3 – Внески змінних у кожен фактор для податкового каналу

Value number	Eigenvalues of correlation matrix, and related statistics Active variables only			
	Eigenvalue	% Total variance	Cumulative Eigenvalue	Cumulative %
1	2,434898	81,16325	2,434898	81,1633
2	0,411683	13,72278	2,846581	94,8860
3	0,153419	5,11397	3,000000	100,0000

Рисунок К.4 – Власні значення і відсоток поясненої дисперсії за методом головних компонент для освітнього каналу

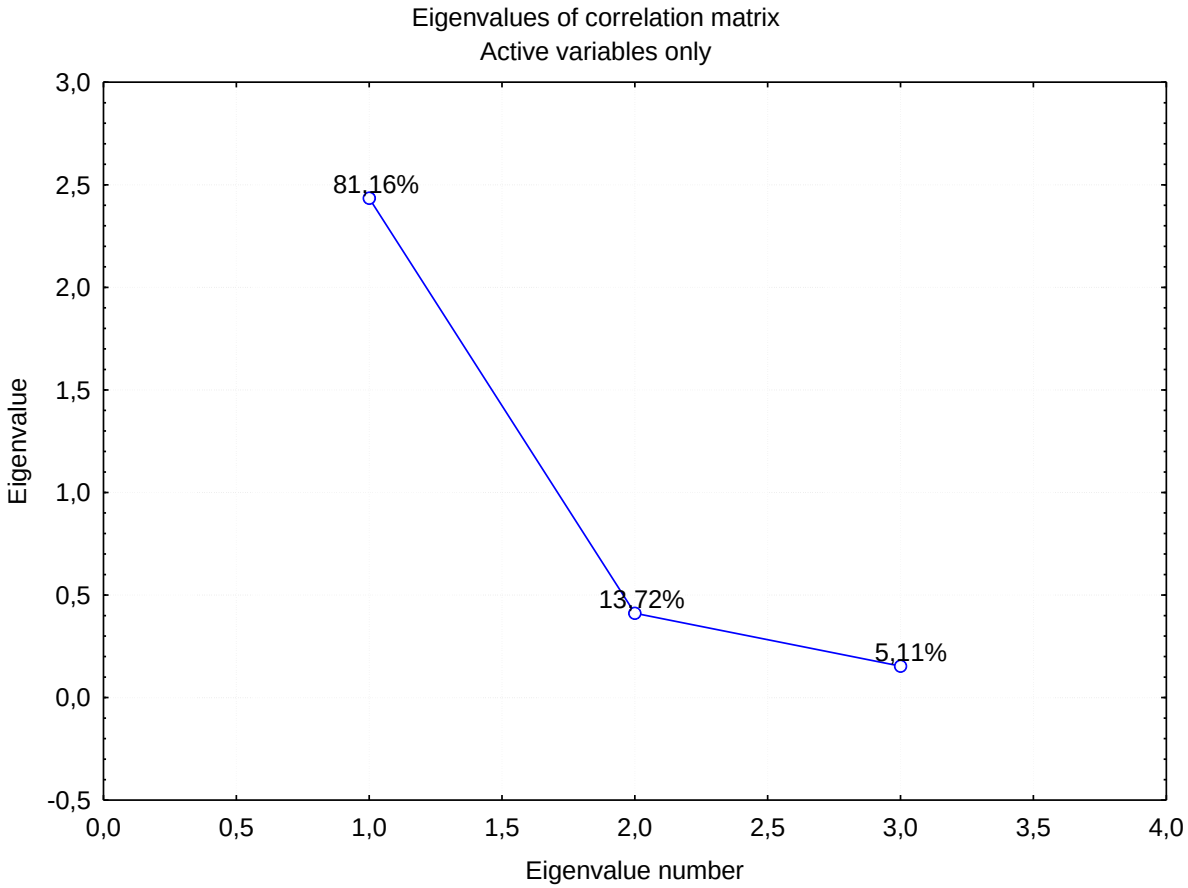


Рисунок К.5 – Графік кам’янистого осипу для освітнього каналу

Variable	Variable contributions, based on correlations		
	Factor 1	Factor 2	Factor 3
E1	0,315392	0,491821	0,192786
E2	0,371058	0,000076	0,628866
E3	0,313549	0,508103	0,178348

Рисунок К.6 – Внески змінних у кожен фактор для освітнього каналу

Value number	Eigenvalues of correlation matrix, and related statistics Active variables only			
	Eigenvalue	% Total variance	Cumulative Eigenvalue	Cumulative %
1	2,268103	45,36206	2,268103	45,3621
2	1,088213	21,76426	3,356316	67,1263
3	0,977441	19,54882	4,333757	86,6751
4	0,583772	11,67544	4,917529	98,3506
5	0,082471	1,64942	5,000000	100,0000

Рисунок К.7 – Власні значення і відсоток поясненої дисперсії за методом головних компонент для інвестиційного каналу

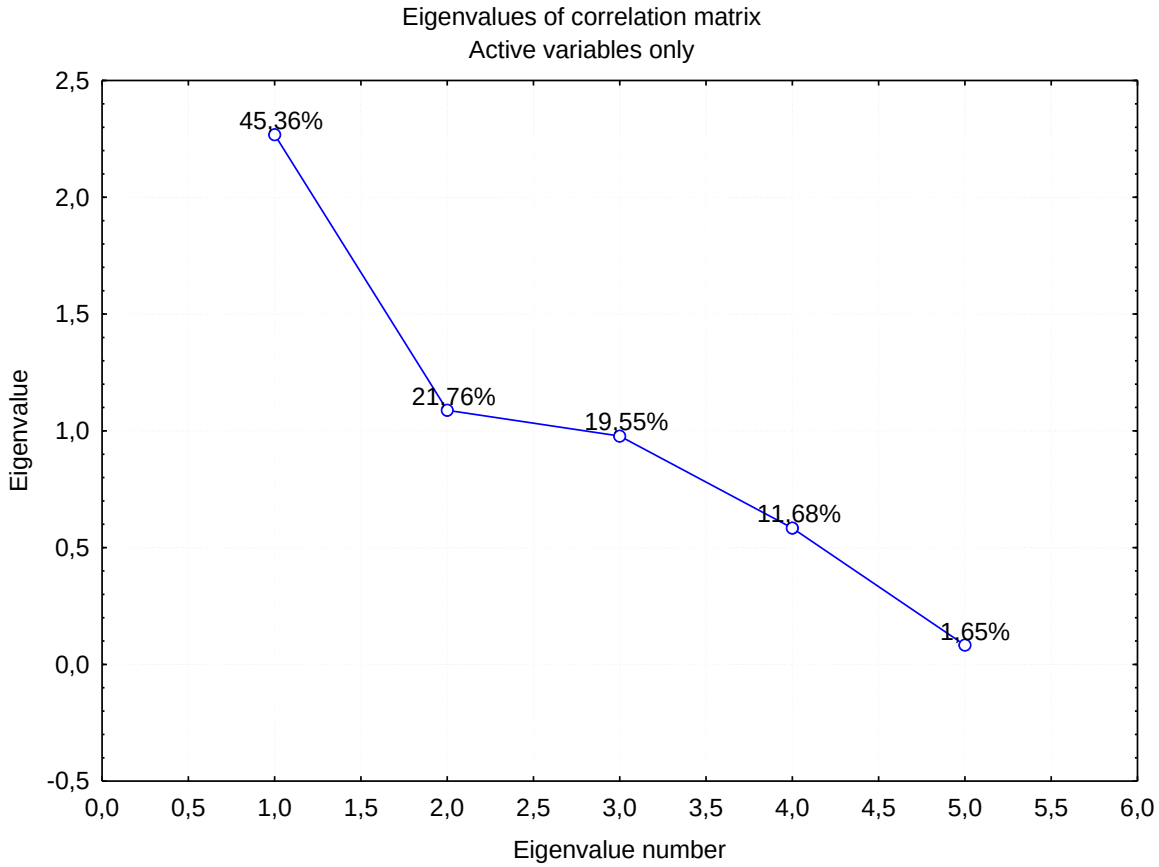


Рисунок К.8 – Графік кам’янистого осипу для інвестиційного каналу

Variable	Variable contributions, based on correlations				
	Factor 1	Factor 2	Factor 3	Factor 4	Factor 5
Invest1	0,296882	0,022485	0,233781	0,073432	0,373419
Invest2	0,118791	0,026782	0,517341	0,335035	0,002050
Invest3	0,397352	0,000285	0,054194	0,000548	0,547620
Invest4	0,094025	0,391802	0,184658	0,304629	0,024886
IInvest5	0,092950	0,558645	0,010025	0,286355	0,052025

Рисунок К.9 – Внески змінних у кожен фактор для інвестиційного каналу

Таблиця К.5 – Оцінки пріоритетів, матриця парних порівнянь та вагові коефіцієнти для податкового каналу

priority	Показник	T1	T2	T3	T4	T5	w
0,2157	T1	1,00	7,00	0,50	5,00	3,00	0,299
0,1695	T2	0,14	1,00	0,17	0,20	0,14	0,046
0,2172	T3	2,00	6,00	1,00	7,00	2,00	0,363
0,1843	T4	0,20	5,00	0,14	1,00	0,20	0,085
0,2132	T5	0,33	7,00	0,50	5,00	1,00	0,207

Таблиця К.6 – Оцінки пріоритетів, матриця парних порівнянь та вагові коефіцієнти для освітнього каналу

priority	Показник	E1	E2	E3	w
0,3154	E1	1,00	0,17	3,00	0,2708
0,3711	E2	6,00	1,00	5,00	0,5357
0,3135	E3	0,33	0,20	1,00	0,1935

Таблиця К.7 – Оцінки пріоритетів, матриця парних порівнянь та вагові коефіцієнти для інвестиційного каналу

priority	Показник	Invest1	Invest2	Invest3	Invest4	Invest5	w
0,2137	Invest1	1,00	5,00	0,20	7,00	4,00	0,3015
0,1856	Invest2	0,20	1,00	0,17	0,33	0,25	0,0649
0,2203	Invest3	5,00	6,00	1,00	0,25	5,00	0,3166
0,1892	Invest4	0,14	3,00	4,00	1,00	0,25	0,1503
0,1912	Invest5	0,25	4,00	0,20	4,00	1,00	0,1667

Таблиця К.8 – Значення інтегрального показника оцінювання ефективності каналів протидії легалізації незаконних доходів

Рік	Інтегральний показник оцінювання ефективності каналів протидії легалізації незаконних доходів
2006	0,4710
2007	0,4663
2008	0,4488
2009	0,4274
2010	0,4568
2011	0,4514
2012	0,4480
2013	0,4274
2014	0,4294
2015	0,4336
2016	0,4301
2017	0,4306
2018	0,4325

Продовження таблиці К.8

2019	0,4373
2020	0,4508
2021	0,3988
2022	0,3985
2023	0,3983
2024	0,3977
2025	0,3972