Міністерство освіти і науки України
Сумський державний університет

УДОСКОНАЛЕННЯ СИСТЕМИ ЗАПОБІГАННЯ ТА ПРОТИДІЇ ФІНАНСОВИМ КІБЕРШАХРАЙСТВАМ: ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ТА ПРАКТИЧНІ АСПЕКТИ

Монографія

За загальною редакцією

доктора економічних наук, професора А.О. Бойка,

докторки економічних наук, доцентки Г.М. Яровенко

УДК 336.71:004.056
У31

Рецензенти:
Наталія ВИГОВСЬКА докторка економічних наук, професорка кафедри фінансів та цифрової економіки Житомирської політехніки Міністерства освіти і науки України;
Інна ШКОЛЬНИК, докторка економічних наук, професорка кафедри фінансових технологій і підприємництва, проректорка з науково-педагогічної роботи Сумського державного університету політехніки Міністерства освіти і науки України;
Ірина ШАЛИГІНА, кандидатка економічних наук, доцентка кафедри фінансів, банківської справи та страхування Сумського національного аграрного університету Міністерства освіти і науки України

Рекомендовано до видання
вченою радою Сумського державного університету як монографія
(протокол № 4 від 9 листопада 2023 року)

У монографії наведено теоретико-методологічні й прикладні підходи щодо удосконалення системи запобігання та протидії фінансовим кібершахрайствам. У виданні розглянуто змістові аспекти кібершахрайств, дослідження основних передумов їх поширення. Особливу увагу приділено дослідженню фінансовим злочинам та пошуку механізмів протидії їм. У монографії обгрунтовано концепцію конвергенції системи фінансового моніторингу та кібершахрайства. У роботі запропоновано стратегічні засади забезпечення стійкості фінансового простору. Розрахована на широке коло читачів, які цікавляться питаннями кібербезпеки та протидії легалізації кримінальних доходів, а також викладачів, аспірантів і студентів.

Удосконалення системи запобігання та протидії фінансовим кібершахрайствам: теоретико-методологічні та практичні аспекти / за заг. ред. д-ра екон. наук, проф. А.О.Бойка та д-ра екон. наук, доц. Г.М.Яровенко. – Суми : Сумський державний університет, 2023. – 215 с.

ЗМІСТ

ВСТУП

Тема боротьби та протидії фінансовим кібершахрайствам є надзвичайно актуальною в сучасному світі. Це пов'язано із зростанням обсягів фінансових операцій та транзакцій, які здійснюються в інтернеті та електронній комерції. Цифрова трансформація суспільства призводить до збільшення використання онлайн-платежів та банківських послуг, що створює нові можливості для кіберзлочинців. Зростання кількості та складності фінансових інструментів і послуг також ускладнює боротьбу з кібершахрайствами. Кіберзлочинці постійно адаптуються та вдосконалюють свої методи шахрайства, використовуючи нові технології, соціальну інженерію та інші підходи. Їхні дії стають більш непередбачуваними і важкими для виявлення. Підвищення залежності від інтернету та кіберплатежів унаслідок глобальних подій, таких як пандемія COVID-19, робить суспільство ще більш уразливим перед фінансовими кіберзлочинцями. Зростає кількість фінансових шахрайств, спрямованих на використання ситуації кризи або паніки для обману людей та підприємств.

Актуальність теми також підтримується зростанням рівня фінансових збитків, які завдаються в результаті фінансових кібершахрайств. Фінансові втрати можуть бути надзвичайно значними, якщо не приділяти відповідну увагу протидії цьому виду злочинності. Боротьба з фінансовим кібершахрайством стає надзвичайно важливою для забезпечення фінансової стабільності і довіри до цифрових фінансових систем. Її необхідність для банків підсилюється через декілька ключових факторів. По-перше, спостерігається зростання популярності онлайн-фінансів, коли все більше клієнтів користуються онлайн-банкінгом та мобільними додатками для управління своїми фінансами. Ця тенденція надає кіберзлочинцям нові можливості для атак на банківські системи та клієнтів. По-друге, зловмисники постійно вдосконалюють свої методи атак, використовуючи соціальну інженерію, фішинг, шкідливе програмне забезпечення та інші техніки для вторгнень в банківські системи, що робить боротьбу з ними надзвичайно складною. По-третє, фінансові кібершахрайства завдають значних збитків банкам, втрачаючи не лише кошти через незаконний доступ до рахунків клієнтів, але і змушуючи витрачати гроші на відновлення систем безпеки та компенсації постраждалим клієнтам. Крім того, кібершахрайства можуть серйозно підірвати репутацію банку, особливо якщо інциденти стають системними. Це може призвести до втрати довіри клієнтів та інвесторів. Нарешті, фінансові злочини стали поширеними та доступними для зловмисників різного рівня кваліфікації, і це робить боротьбу з ними надзвичайно важливою для збереження стабільності фінансових ринків.

На макрорівні актуальність теми боротьби та протидії фінансовим кібершахрайствам стає ще більш важливою і комплексною, оскільки вплив кіберзлочинності на економіку та суспільство стає суттєвим. Фінансові

кібершахраї можуть призводити до значних економічних втрат як національного, так і глобального масштабу. Вони створюють загрозу фінансовій стабільності, особливо коли банки та інші фінансові установи стають жертвами масштабних атак. Крім того, фінансові кіберзлочини можуть фінансувати терористичні групи та інші загрози національній безпеці, спричиняючи серйозні геополітичні конфлікти. Втрата довіри в систему фінансових послуг також є серйозною проблемою, яка може відлякувати клієнтів та інвесторів. Крім того, кіберзлочини можуть мати каскадний вплив на інші галузі, такі як страхування, інвестиції, ринок праці та бізнес-процеси, що робить боротьбу з ними надзвичайно важливою для економіки в цілому.

Таким чином, дана монографія присвячена актуальній на сьогоднішній день проблемі. Вона складається з двох розділів. Перший розділ «Теоретико-методологічні та практичні аспекти дослідження кібершахрайств у сфері фінансових послуг» присвячений розкриттю сутності кібершахрайств, їх видам та визначальним передумовам їх поширення в фінансовому секторі економіки, характеристики сучасного стану та тенденціям поширення кіберзлочинності в Україні та світі, Due Diligence як інструменту протидії фінансовим кібершахрайствам, оцінюванню ефективності системи протидії легалізації кримінальних доходів. У другій частині «Напрями розвитку системи запобігання та протидії фінансовим кібершахрайствам: конвергенція, інструментарій та управління» зосереджено увагу на обґрунтуванні концепції конвергенції системи фінансового моніторингу та кібершахрайств, модернізації інструментарію протидії легалізації кримінальних доходів та кібершахрайствам, формуванню управлінських засад забезпечення стійкості фінансового кіберпростору на мікро- та макрорівні.

Окремі підрозділи монографії підготували: пункти 1.1.1, 1.2.1, вступ та висновки – доктор економічних наук, професор Бойко А.О., підрозділи 2.1, 2.2, 2.3, вступ та висновки - докторка економічних наук, доцентка Яровенко Г.М.; пункт 2.3.2 – докторка економічних наук, професорка Васильєва Т.А.; пункт 2.1.2 - докторка економічних наук, професорка Кузьменко О.В.; пункт 2.1.2 - доктор економічних наук, професор Лєонов С.В.; пункт 2.1.2 – кандидатка педагогічних наук, доцентка Перхун Л.П., пункти 1.3.1, 1.3.2 – кандидатка педагогічних наук, доцентка Боженко В.В., пункт 1.3.3 – доктор філософії Миненко С.В., пункт 1.4 – докторка філософії Доценко Т.В., пункти 1.1.1, 1.1.2, 1.2.1 – асистент Кушнерьов О.С., пункт 1.2.2 – аспірантка Доля Ю.В., пункти 2.1.3, 2.2.1 – викладач-стажистка Колотіліна О.В., пункт 1.4 – магістрантка кафедри економічної кібернетики Бережна Д.Є., пункт 2.1.3 – магістрантка кафедри економічної кібернетики Рапута А.О.

Монографія виконана в рамках держбюджетних науково-дослідних робіт: «Кібербезпека в боротьбі з банківськими шахрайствами: захист споживачів фінансових послуг та зростання фінансово-економічної безпеки України» (номер державної реєстрації 0121U109559), «Data-Mining для протидії кібершахрайствам та легалізації кримінальних доходів в умовах цифровізації фінансового сектору економіки України» (номер державної реєстрації

0121U100467), «Моделювання механізмів детінізації та декорумпізації економіки для забезпечення національної безпеки: вплив трансформації фінансових поведінкових патернів» (номер державної реєстрації 0122U000783).

РОЗДІЛ 1
ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ТА ПРАКТИЧНІ АСПЕКТИ ДОСЛІДЖЕННЯ КІБЕРШАХРАЙСТВ У СФЕРІ ФІНАНСОВИХ ПОСЛУГ

1.1. Сутність кібершахрайств, їх види та визначальні передумови їх поширення в фінансовому секторі економіки

1.1.1. Бібліометричний аналіз дослідження кібершахрайств у системі фінансово-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.

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%.

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

Ключові слова	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 авторами на основі наукометричної бази Scopus

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 рециденства 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 схожишими 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.

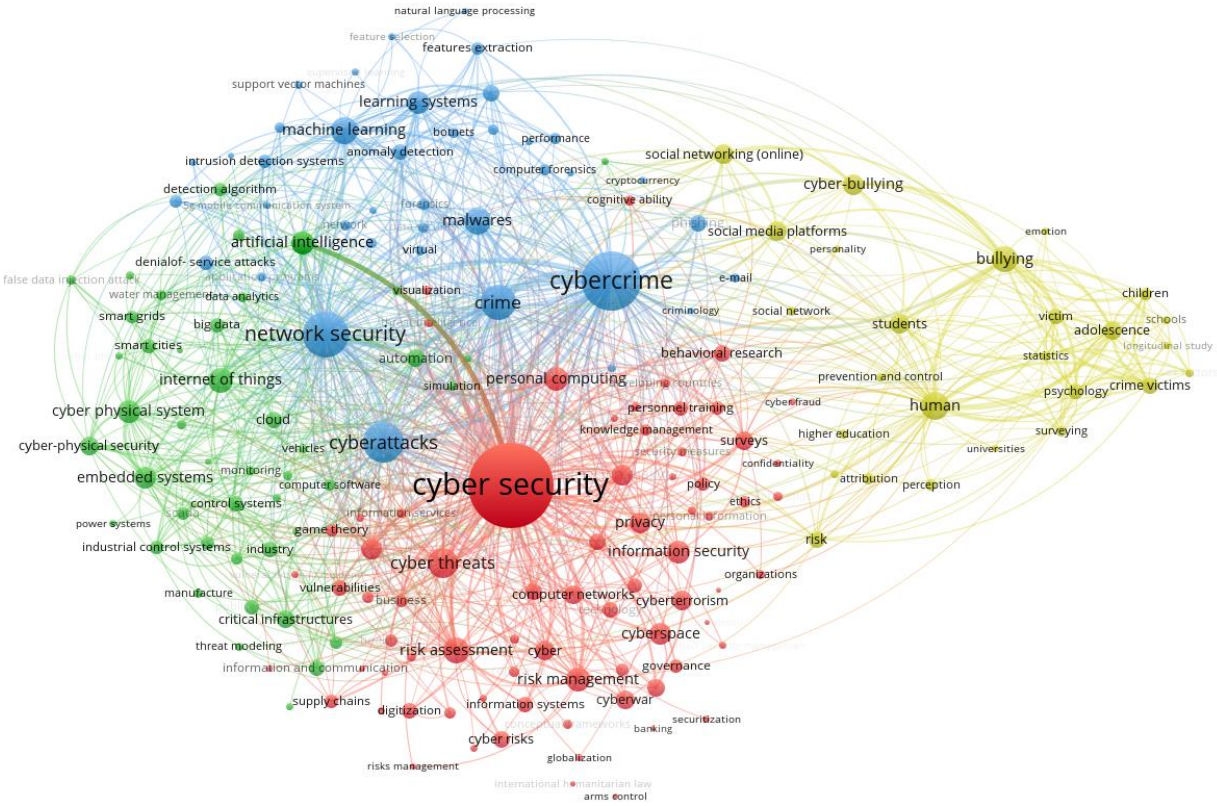


Рисунок 1.1 – Результати бібліометричного аналізу наукових праць з питань кібербезпеки в економічному вимірі у виданнях, що індексуються наукометричною базою даних Scopus

Джерело: складено автором з використанням інструментарію VOSViewerv.1.6.10

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.

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 Von Solms & Van Niekerk (2013), 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 Alhogail & Alsabih (2021) 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 Akhta et al. (2021) представлено результати опитування 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 (Ying et al 2018) у своєму тематичному дослідженні довели, що блокчейн здатний захистити конфіденційну інформацію, а також усунути посередництво будь-яких установ.

У роботі Al-Tahat & Moneim (2020) проаналізовано сфери практичного застосування нейронних мереж та генетичних алгоритмів в системі управління інформаційною безпекою комерційних банків. У роботі Noor et al. (2019) побудовано фазові профілі кібершахраїв на основі аналізу моделей їх атак шляхом використання техніки розподільної семантики обробки природної мови. А. Бердюгін та П.Ревенков (2020) розробили за допомогою Borland Delphi програмне забезпечення для кількісної оцінки ймовірності ризику кібератак на технології електронного банківського обслуговування.

У роботі Mousa et al (2017) обґрунтовано необхідність посилення інформаційної безпеки серед працівників фінансових установ. Yerdon (2021) 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 Chen et al (2021) 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, Singh et al (2020) 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 & С. Тосун (2020), М. Аркурі (2020) 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 (Lowry et al., 2016). Найчастішою причиною зараження шкідливим програмним забезпеченням і порушення конфіденційності є соціальні мережі (Onete et al., 2020).

На думку П. Андреу і С. Аніфантакі (2021) 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 Carlton et al. (2019)визначено набір навичок кібербезпеки не-IT-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).

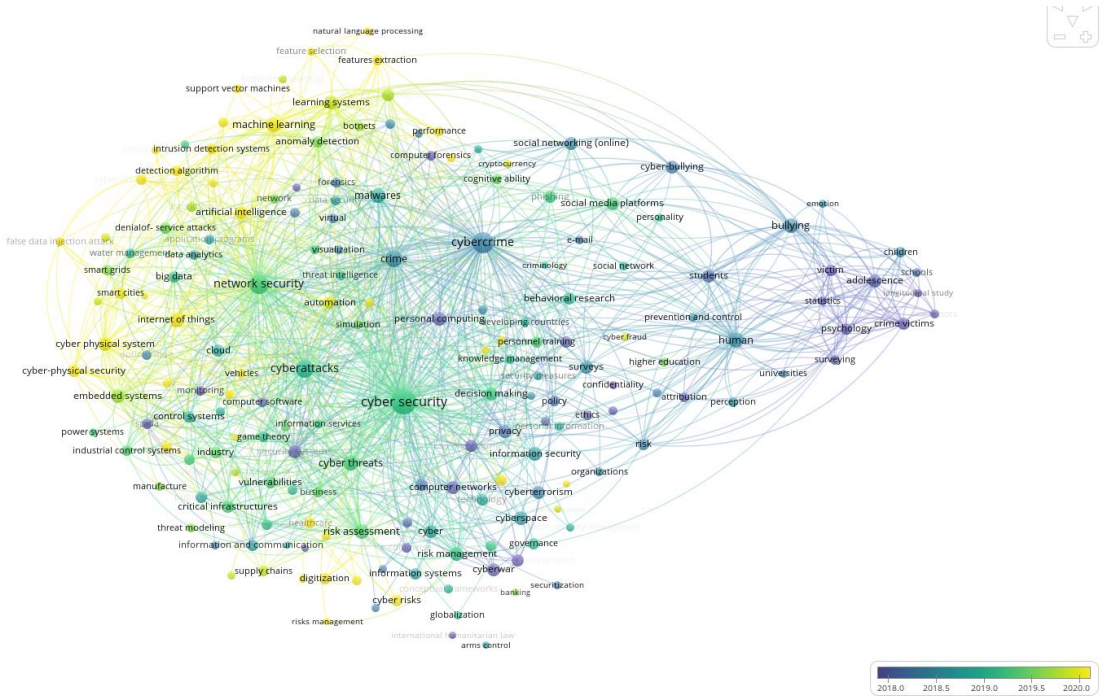


Рисунок 1.2 – Візуалізаційна карта контекстуально-часового виміру досліджень з питань кібербезпеки в контексті економічних відносин
Джерело: складено автором з використанням інструментарію VOSViewerv.1.6.10

Отже, за результатами контекстуально-часового аналізу з питань ефективності 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.

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 аціональної економіки з урахуванням стрімких темпів впровадження цифрованих інновацій та технологій в екосистему.

1.1.2. Загальна характеристика кібершахрайств та передумов їх поширення

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», 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» 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 Li & Liu (2023), 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. У роботі (Motsch et al., 2020) 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 IT-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.

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 (Діордіца, Загуменний (2019)). 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. 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).

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. (Козирєва та Гаврилішин, 2020). 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).

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.

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

Джерело: власна розробка автора

У Законі України «Про основні засади забезпечення кібербезпеки України» 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 (Островий, 2018; Кузьменко та ін., 2022) 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».

Рисунок 1.4 – Види кіберзагроз та кібератак

* кібератака фактично вплинула на конфіденційність, цілісність або доступність даних

Джерело: складено автором на основі Довгань & Доронін (2017), ENISA, Yevseiev et al (2018), Jouini et al (2014), Uma & Padmavathi (2013)

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 (Nish, 2020):

– 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 (Лисенко та ін., 2020). 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.

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. Сучасний стан та тенденції поширення кіберзлочинності в Україні та світі

1.2.1. Тенденції розвитку кібершахрайських операцій у фінансовій сфері

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 (Боженко та ін., 2021).

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 (GSM Association, The Mobile Economy 2020).

– 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 (Special Eurobarometer).

– 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%.

– 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% (Eurostat).

– 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%). Проте протягом 2023-2030 рр. очікується збільшення використання хмарних технологій у бізнес-процесах приблизно на 14,1% (Eurostat).

– 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 (Eurostat).

– 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). 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. 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 госплдарювання (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.

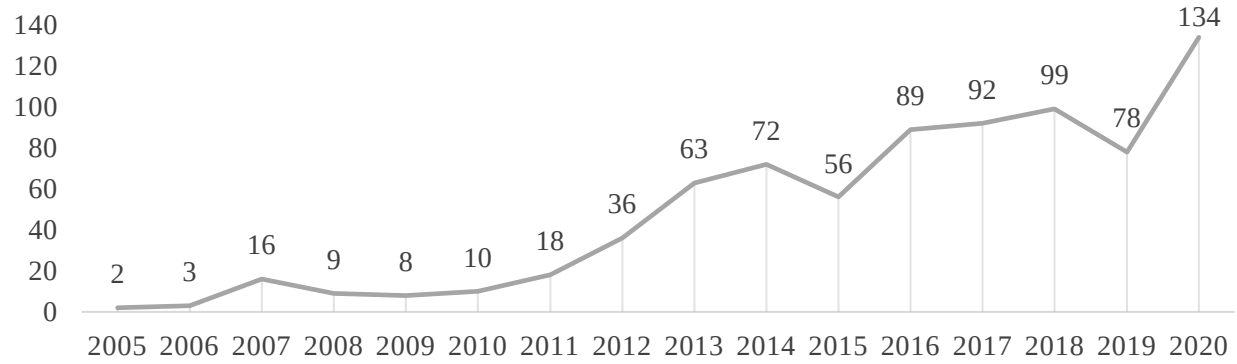


Рисунок 1.5 – Динаміка значущих кіберінцидентів у світі протягом 2005-2020 років

Джерело: складено автором на основі база даних Європейського репозитарію кіберінцидентів

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 (рис. 1.6). 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 інфраструктури США (149 інцидентів або 18,9% від загального обсягу).

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

Джерело: складено автором на основі база даних Європейського репозитарію кіберінцидентів

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 (рис. 1.7).

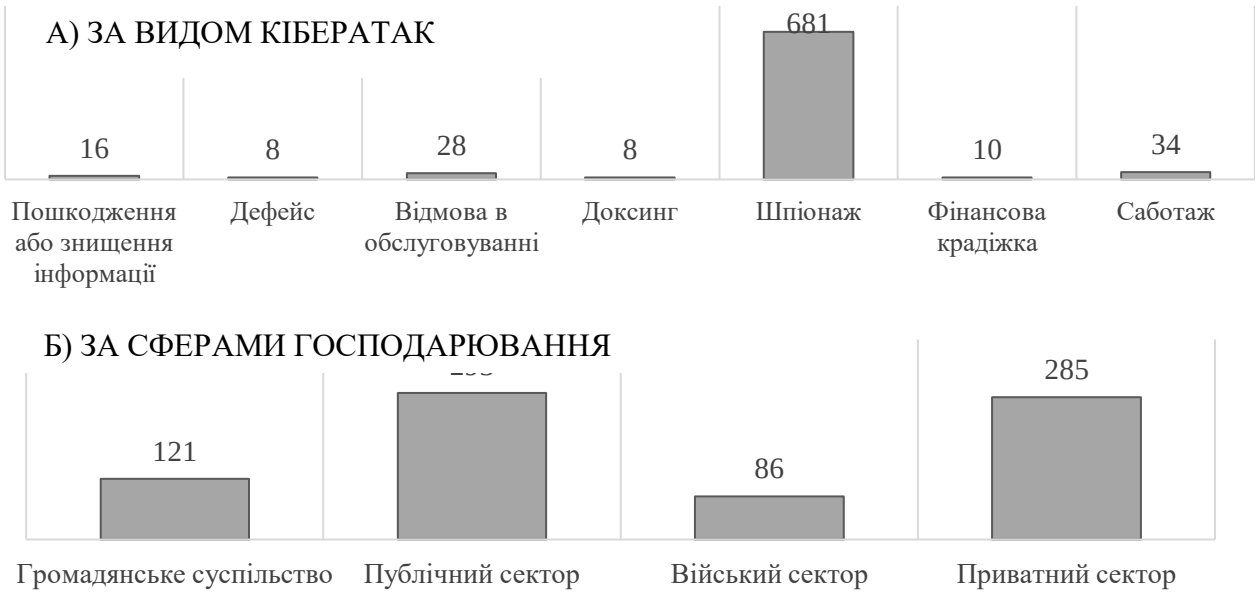


Рисунок 1.7 – Структура кіберінцидентів у період з 2005 по 2020 роки (а – за видом кібератак; б – за сферами господарювання)

Джерело: складено автором на основі база даних Європейського репозитарію кіберінцидентів

У межах даного дослідження також вирішено більш детальніше проаналізувати дати здійснення кібератак (рис. 1.8). Це обумовлено тим, що у багатьох дослідження (Prieto Curiel (2023), Bernasco et al (2017), Haberman & Ratcliffe (2013) вже емпірично доведено, що часова концентрація є стійкою ознакою різних видів злочинності.

Дані, 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.

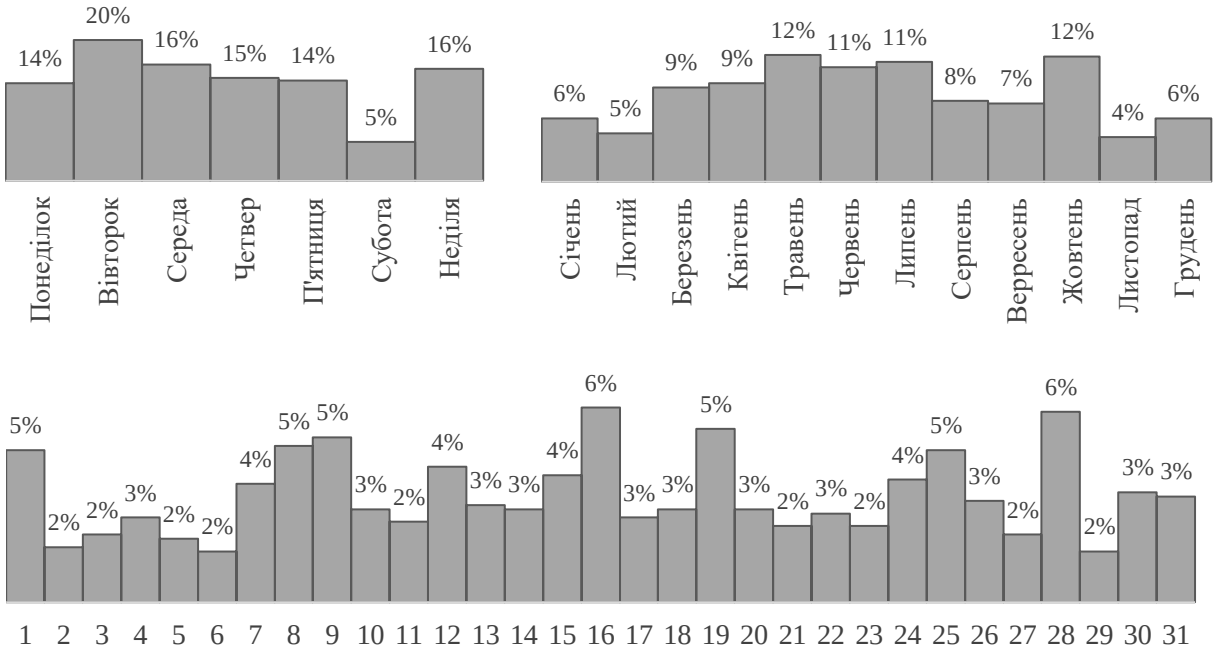


Рисунок 1.8 – Часова концентрація кіберзагроз у розрізі місяців, днів тижня та днів

Джерело: складено автором на основі база даних Європейського репозитарію кіберінцидентів

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 1.2 наведено найбільш поширені способи здійснення кібератак у світі у розрізі сфер господарювання.

Дані таблиці 1.2 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.

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) (Federal Bureau of Investigation).

Таблиця 1.2 – 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: складено авторами на основі даних IBM Security

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.

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.

1.2.2. Закономірності здійснення фінансових кібершахрайств з використанням криптовалюти

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.

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 криптоопераційї, 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.

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

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

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

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

– транзакції на децентралізованих біржах (анонімні ринки, представлені розподіленим реєстром програм, що дозволяють користувачам проводити

транзакції з використанням криптовалют без участі централізованих організацій-посередників при торгівлі чи зберіганні криптовалюти);

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

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

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

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

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 (Savchuk et al (2020), Horban et al (2021):

- 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:

$$supp(X \to Y) = P\,(X \cap Y) = \frac{n(\{X; Y\} \in d_i}{N} \qquad (1.1)$$

- 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:

$$conf(X \to Y) = P\ (X|Y) = \frac{n1(\{X;Y\} \in d_i}{n1(\{X\} \in d_i} \quad (1.2)$$

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

У межах даного дослідження застосовано алгоритми асоціативних правил для визначення ймовірних умов, які будуть вказувати на можливість проведення шахрайської операції з криптовалютою. Об'єктом дослідження обрано Ethereum. За даними BanklessTimes, Ethereum (ETH) зараз використовується для незаконної діяльності більше порівняно з Bitcoin. Згідно з аналізом, частка незаконних транзакцій у загальному відомому потоці Ethereum зросла до 0,33 відсотка проти 0,04 відсотка для Bitcoin. Експерти наголошують, що криптовалюта Ethereum є популярним фінансовим інструментом серед учасників на ринку даркнету, які використовуються для торгівлі незаконними товарами та послугами. Це повязано з цим, що Ethereum пропонує більшу конфіденційність, ніж Bitcoin. Ці ринки часто розміщені в «темній мережі», доступ до якої можливий лише за допомогою спеціального програмного забезпечення. Крім цього, зростання незаконної діяльності з викоритсанням Ethereum, ймовірно, пов'язано з його популярністю як платформи для смарт-контрактів. Розумні контракти дозволяють розробляти децентралізовані програми (dApps), які часто використовуються злочинцями для сприяння незаконній діяльності, такій як відмивання грошей і торгівля наркотиками. Крім того, збільшення частки незаконної діяльності Ethereum може бути пов'язане з його популярністю серед операторів програм-вимагачів та інших злочинців. Атаки програм-вимагачів останнім часом стали більш поширеними, і злочинці часто вимагають оплату в криптовалюті. 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, тоді як фрагмент сформованої статистичної бази подано в таблиці 1.3.

Таблиця 1.3 – 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

Джерело: власні розрахунки автора

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 1.4.

Таблиця 1.4 – Результати побудови асоціативних правил для визначення закономірностей зійснення незаконних операцій з Ефіріум

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

Джерело: власні розрахунки автора

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 1.4, 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 1.9).

	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)	1,000000	7662,000	77,85794
2	(-39,576163<URFA<=100,277515)	1,000000	9669,000	98,25221
3	(-574,848976<AVR<=776,291550)	1,000000	9456,000	96,08780
4	(-11,224277<AVS<=100,744593)	1,000000	9309,000	94,59405
5	(-73745,232761<TES<=94068,968712)	1,000000	9791,000	99,49192
6	(-73645,038405<TER<=96923,921976)	1,000000	9781,000	99,39031
7	(-35,997920<USTA<=87,555079)	1,000000	9634,000	97,89656
8	(FRAUD>0,902041)	1,000000	2179,000	22,14206
9	(-0,070274<FRAUD<=0,124189, -35,997920<USTA<=87,555079)	2,000000	7462,000	75,82563
10	(-0,070274<FRAUD<=0,124189, -73645,038405<TER<=96923,921976, -35,997920<USTA<=87,555079)	3,000000	7406,000	75,25658
11	(-0,070274<FRAUD<=0,124189, -73745,232761<TES<=94068,968712, -35,997920<USTA<=87,555079)	3,000000	7415,000	75,34803
12	(-0,070274<FRAUD<=0,124189, -11,224277<AVS<=100,744593, -35,997920<USTA<=87,555079)	3,000000	6961,000	70,73468
13	(-0,070274<FRAUD<=0,124189, -574,848976<AVR<=776,291550, -35,997920<USTA<=87,555079)	3,000000	7094,000	72,08617
14	(-0,070274<FRAUD<=0,124189, -39,576163<URFA<=100,277515, -35,997920<USTA<=87,555079)	3,000000	7382,000	75,01270
15	-73745,232761<TES<=94068,968712, -73645,038405<TER<=96923,921976, -35,997920<USTA<=87,555079)	4,000000	7399,000	75,18545
16	-73745,232761<TES<=94068,968712, -73645,038405<TER<=96923,921976, -35,997920<USTA<=87,555079)	5,000000	6926,000	70,37903
17	-73745,232761<TES<=94068,968712, -73645,038405<TER<=96923,921976, -35,997920<USTA<=87,555079)	5,000000	7043,000	71,56793
18	73745,232761<TES<=94068,968712, -73645,038405<TER<=96923,921976, -35,997920<USTA<=87,555079)	5,000000	7319,000	74,37252
19	73745,232761<TES<=94068,968712, -73645,038405<TER<=96923,921976, -35,997920<USTA<=87,555079)	6,000000	6919,000	70,30790

Рисунок 1.9 – Частота виявлених випадків здійснення фінансових кібершахрайств з використанням Ефіріум

Джерело: власні розрахунки автора

Аналіз рисунку 1.7 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.

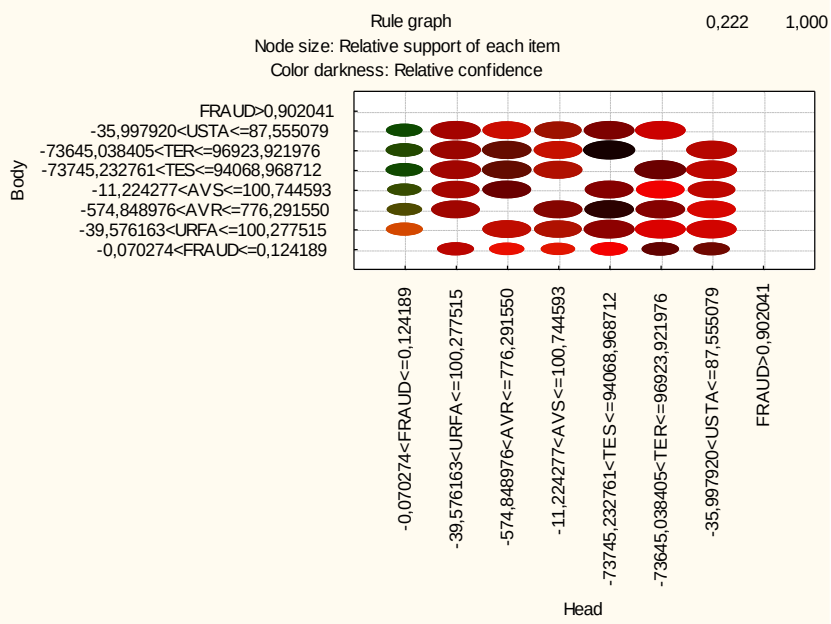


Рисунок 1.10 – Граф асоціативних правил

Джерело: власні розрахунки автора

В рамках даного етапу побудовано граф виявлених на другому етапі асоціативних правил, представлений на рисунку 1.10, 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 найбільшим даний показник є для низького рівня ризику, коли TER не перевищує 96923, AVR - 776, TES – 94.068 відповідно. Найменша частка випадків спостерігається для низького рівня ризику здійснення фінансових кібершахрайств з використанням Ефіріум в межах до 0,12 частки одиниці.

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.

1.3. Концептуальні засади дослідження фінансових злочинів в умовах цифрових перетворень

1.3.1. Визначення детермінант розвитку тіньових фінансово-економічних відносин в національній економіці

Розвиток фінансової та економічної злочинності в країні стримують процеси розширеного відтворення, посилюють диференціацію доходів населення і соціальну напруженість, послаблюють важелі державного управління і перешкоджають економічному розвитку. Попри багаторічну історію існування тіньової економіки в різних країнах світу, досі не знайдено ефективного механізму протидії даним деструктивним процесам, оскільки на практиці постійно відбувається удосконалення методів та інструментів здійснення даних протиправних діянь. У науковій літературі існують численні емпіричні дослідження, які аналізують різні змінні для пояснення тіньової економіки шляхом виявлення значущих детермінант. Проте в основі більшості емпіричних досліджень, спрямованих на визначення факторів поширення корупції, є використання панельних даних. Використання панельних даних дозволяють вставити загальні закономірності, проте не враховують специфіку розвитку саме національної економіки. Це обумовило необхідність збору статистичних даних у розрізі України та застосування математичного інструментарію, який буде адекватно оцінювати вплив різноманітних детермінант на рівень корупції .

У межах даного дослідження для визначення значимих демермінант впливу на тіньову економіку використано багатомірні адаптивні регресивні MAR-сплайни, в основі яких алгоритм складних задач нелінійної регресії. Алгоритм передбачає знаходження набору простих лінійних функцій, які в сукупності забезпечують найкращу ефективність використання.

Інструментарій MAR-сплайни використовувався для виявлення точок зростання корупційних ризиків в країні, спричинених зовнішніми економічними шоками. Багатовимірні адаптивні регресивні сплайни MAR є непараметричною процедурою формалізації в залежності від набору базисних функцій і коефіцієнтів, які повністю визначаються набором вхідних даних. Ця процедура базується на підході, згідно з яким набір значень вхідних змінних (регресорів) поділяється на області зі своїми специфічними рівняннями регресії та класифікації. Такий підхід передбачає побудову адаптивних моделей, які дозволяють отримувати надійні прогнози та використовуються у випадках переломних моментів і формалізації немонотонного характеру зв’язку між ефектами та відгуками, які важко апроксимуються параметричними моделями.

Основні функції багатовимірних адаптивних регресивних сплайнів MAR до та після точки перемикання регресії описані таким чином:

$$(x-t)_+ = \begin{cases} x-t, if\ x > t \\ 0, if\ x \le t \end{cases} \qquad (1.3)$$
$$(x-t)_- = \begin{cases} t-x, if\ x < t \\ 0, if\ x \ge t \end{cases}$$

де t – точка перегину кускової функції.

Основні функції MARSplines (багатовимірних сплайнів адаптивної регресії) у програмному забезпеченні STATISTICS формалізуються на основі наступних математичних співвідношень:

$$(x-t)_+ = max\ (0; x-t) \qquad (1.4)$$
$$(x-t)_- = max\ (0; t-x)$$

За умови формалізації багатовимірної залежності для кожної компоненти вектора регресора будуються базові функції (1.3) і (1.4), які визначають множину базових функцій, побудованих на основі набору вхідних даних:

$$B = \{(x_i - t)_+, (t - x_i)_-\}_{\substack{t \in \{x_{1i},\dots,x_{Ni}\} \\ i=1,\dots,n}} \qquad (1.5)$$

Загальне рівняння багатовимірних адаптивних регресивних сплайнів MAR для m ненульових складових членів записується як комбінація зваженої суми базисних функцій та їх добутків:

$$y = f(X) = \alpha_0 + \sum_{j=1}^{m} \alpha_j \cdot B_j(X) \qquad (1.6)$$

де α_0 – постійна величина, вільний термін;

α_j – константа, параметр багатовимірного рівняння адаптивної регресії;

m – загальна кількість основних функцій;

X – вектори вхідних регресорів;

$B_j(X)$ – j-на базисна функція з множини B або добуток двох або більше таких функцій .

Базовий принцип побудови багатовимірних адаптивних регресивних MAR-сплайнів передбачає визначення як базисних функцій, так і термінів, які визначають кількість різних комбінацій базових функцій, враховуючи запити до кожного з релевантних регресорних факторів.

Для характеристики рівня тіньової економіки в країні використано обсяг тіньової економіки у % до ВВП (SE), визначеного за методикою Ф. Шнайдера (2005). Детермінанти поширення тіньової економіки розглянемо у розрізі трьох ключових напрямків:

1. Економічні фактори: рівень податкового навантаження (TAX); рівень витрат державного управління на кінцеве споживання, % ВВП (GFCE); рівень

монетарної свободи (MON); рівень торгівельної свободи (TRD); кількість державних підприємств (SOE).

2. Інституційні фактори: кількість політичних партій в країні (PP); індекс свободи преси (PFI); рівень політичної стабільності і відсутності насильства/тероризму (PS); рівень регуляторної якості (RQ); рівень верховенства права (RL).

3. Соціальні фактори: частка доходу, що належить найменшим 10% населення (INC_L); частка доходу, що належить найбільшим 10% населення (INC); середньомісячна заробітна плата в сфері управлінні (WG_G); рівень безробіття (UNM); кількість зареєстрованих злочинів на 100 тис. населення (CRM).

Отже, для визначення факторів впливу на тіньову економіку в Україні обрано 15 індикаторів. Джерелом первинних даних слугували дані World Bank, Держаної служби статистики України. Періодом дослідження обрано 1998-2021 роки. Для надання загальної характеристики досліджуваних індикаторів визначено їх статистичні характеристики (середнє, модельне, медіанне, мінімальне та максимальне значення, коефіцієнт варіації та стандартне відхилення (рис. 1.11).

	Descriptive Statistics (Spreadsheet7.sta)							
Variable	Mean	Median	Mode	Frequency of Mode	Minimum	Maximum	Std.Dev.	Coef.Var.
CPI	26,00	26,00	26,00000	4	15,0000	33,00	4,054	15,592
SE	43,09	42,60	Multiple	2	34,9000	55,70	5,380	12,486
TAX	76,06	78,40	Multiple	2	62,3000	90,20	8,054	10,589
GFCE	18,87	18,84	Multiple	1	16,8908	24,61	1,621	8,592
MON	64,05	64,90	63,00000	2	38,3000	78,70	10,530	16,439
TRD	77,48	80,15	Multiple	2	53,0000	86,20	9,184	11,852
SOE	6660,00	6893,00	Multiple	1	0,0000	14158,00	3061,909	45,975
INC_L	4,17	4,15	4,400000	4	3,6000	5,30	0,398	9,551
INC	22,80	22,20	Multiple	2	20,6000	28,60	2,072	9,089
WG_G	4654,00	2656,00	Multiple	1	250,0000	18661,00	5514,701	118,494
UNM	8,86	8,95	Multiple	1	6,3500	11,86	1,576	17,795
CRM	1121,38	1107,00	Multiple	1	860,6205	1698,00	199,759	17,814
PP	13073,88	15421,00	Multiple	1	360,0000	19183,00	5630,811	43,069
PFI	35,59	34,99	Multiple	1	19,2500	51,00	7,498	21,068
PS	-0,70	-0,36	Multiple	1	-2,0208	0,17	0,743	-106,126
RQ	-0,50	-0,53	Multiple	1	-0,7574	-0,26	0,131	-25,953
RL	-0,80	-0,78	Multiple	1	-1,1088	-0,54	0,125	-15,694

Рисунок 1.11 – Описові статистики характеристики рівня тіньової економіки та економічних, соціальних, інституційних факторів

Джерело: власні розрахунки автора

Аналізуючи результативний показник – рівень тіньової економіки, відмітимо, що мінімальна та максимальна межі приймають значення 34,90 та 55,70 відповідно. Середньостатистичний рівень тіньової економіки становить 43,09, медіанне значення, тобто значення, яке ділить часовий ряд навпіл є 42,60. В той же час модельне значення, тобто найбільш поширене значення чітко не визначене і є мультиплікативним. Крім того, дана сукупність є однорідною, що пояснюється значенням коефіцієнта варіації в обсязі 12,49.

2 етап. Прогнозування значень рівня тіньової економіки з 2018 по 2021 рр. за допомогою методу експоненційного згладжування шляхом побудови лінійної моделі тренду з метою проведення обробки пропусків та формування повної статистичної бази дослідження. Ретроспективними даними для обчислення прогнозних рівнів тіньової економіки виступили статистичні дані за період з 1998 по 2017 рр. Так, узагальнююча модель експоненціального згладжування має наступний вигляд:

$$S_t = \alpha \cdot X_t + (1 - \alpha) \cdot S_{t-1} \quad (1.7)$$

де X_t – рівень часового ряду в момент часу t;

α – параметр згладжування, який приймає значення від нуля (коли ігноруються усі поточні спостереження) до одиниці (коли повністю ігноруються усі попередні спостереження);

S_t, S_{t-1} – експоненціально згладжене значення в момент часу t та (t-1) відповідно.

Прогнози на один крок вперед обчислюються наступним чином (для моделей без тренду, для лінійних та експоненційних моделей тренду до моделі додається компонент тренду):

- адитивна модель:

$$F_t = S_t + I_{t-p} \quad (1.8)$$

$$I_t = I_{t-p} + \delta \cdot (1 - \alpha) \cdot e_t$$

- мультиплікативна модель:

$$F_t = S_t \cdot I_{t-p} \quad (1.9)$$

$$I_t = I_{t-p} + \delta \cdot (1 - \alpha) \cdot e_t / S_t$$

де δ - сезонний параметр параметром згладжування, який зазначається лише для сезонних моделей;

S_t - просте експоненціально згладжене значення часового ряду в момент t;

I_{t-p} - згладжений сезонний фактор у момент часу t мінус p (довжина сезону);

e_t – залишки у момент часу t.

Для побудови прогнозів експоненціального згладжування на основі моделей часових рядів, які містять як експоненційну компоненту тренду, так і адитивну сезонну компоненту, виникає необхідність проведення додаткового обчислення згладжених значень для першого сезону на базі початкових

значень для сезонних компонент. За замовчуванням модуль часових рядів Для оцінювання цих значень використовується метод класичної сезонної декомпозиції. Для обчислення згладженого значення (прогноз) для першого спостереження, оцінки S0 (початкова сезонна компонента) і T0 (початковий тренд) використовуються наступні математичні співвідношення:

$$T_0 = exp\left(\frac{\big(log(M_k) - log(M_1)\big)}{p}\right) \tag{1.10}$$

$$S_0 = exp\big((log(M_1) - p \cdot log(T_0)/2)\big)$$

де k - кількість повних сезонних циклів;
M_k - середнє значення для останнього сезонного циклу;
M_1 - середнє значення для першого сезонного циклу;
p - тривалість сезонного циклу.

Для побудови прогнозів експоненціального згладжування на основі моделей часових рядів, які містять як експоненційну компоненту тренду, так і мультиплікативну сезонну компоненту, виникає необхідність проведення додаткового обчислення згладжених значень для першого сезону на базі початкових значень для сезонних компонент. За замовчуванням модуль часових рядів оцінюватиме ці значення із даних за допомогою класичної сезонної декомпозиції. Для обчислення згладженого значення (прогноз) для першого спостереження, оцінки S0 (початкова сезонна компонента) і T0 (початковий тренд) використовуються наступні математичні співвідношення:

$$T_0 = exp\left(\frac{\big(log(M_2) - log(M_1)\big)}{p}\right) \tag{1.11}$$

$$S_0 = exp\big((log(M_1) - p \cdot log(T_0)/2)\big)$$

де M_2 - середнє значення для другого сезонного циклу;
M_1 - середнє значення для першого сезонного циклу.

Для обчислення прогнозних рівнів статистичного показника тіньової економіки скористаємось програмним пакетом Statistica, застосувавши команду Statistics/Advanced linear/Nonlinear Models/Time Series/Forecasting/Exponential Smoothing and Forecasting.

Таким чином, прогнозна модель експоненціального згладжування за показником «рівень тіньової економіки» набуває вигляду:

$$SE_t = LT_t + 0.846 \cdot X_t + (1 - 0.846) \cdot S_{t-1} + I_{t-p}, I_t = I_{t-p}, \tag{1.12}$$

S0=-56.05, T0=-0.705

де SE_t - модель тренду;
LT_t – лінійний тренд (значення в момент часу t).

Візуалізація співвідношення теоретичних рівнів, обчислених за формулами (1.12), фактичних даних та залишків моделі представимо на рисунку 1.12.

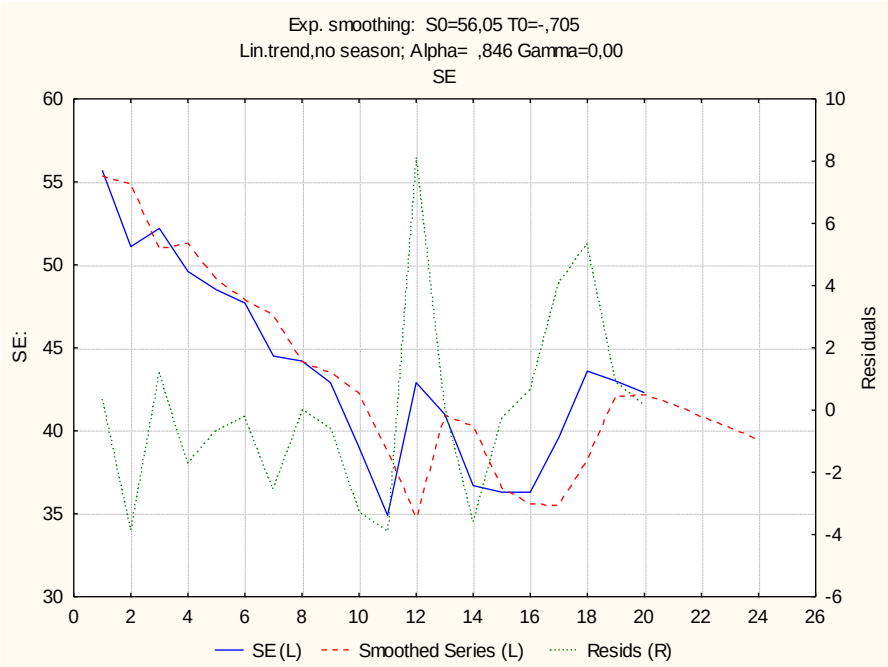


Рисунок 1.12 – Скріншот фрагменту прграми Statistica співвідношення теоретичних рівнів, фактичних даних та залишків моделі експоненційного згладжування рівнів тіньової економіки

Джерело: власні розрахунки автора

3 етап. Застосування багатомірних адаптивних регресивних MAR-сплайнів до визначення релевантності впливу окремо розглянутих груп економічних, соціальних, інституційних факторів на рівень тіньової економіки. Так, безпосереднє проведення сплайн-моделювання (за допомогою команди Data Mining/MARSplines (Multivariate Adaptive Regression Splines)) дозволяє отримаємо наступні параметри, які розмежимо в розрізі результативних показників.

Визначення релевантності впливу груп економічних, соціальних, інституційних факторів на рівень тіньової економіки (таблиця 1.5).

Отже, кількість незалежних змінних – 5, кількість залежних змінних – 1, кількість термів – 3, 4 і 3 в розрізі економічних, соціальних, інституційних факторів; кількість базисних функцій – 2, 3, 2 відповідно; порядок взаємодії (кількість складових добутку базисних функцій) – 1, а також кількість звернень до факторів-регресорів: економічні – 1 до TAX, TRD, соціальні – 1 до INC, WG_G, UNM, інституційні –1 до PP, PFI.

Таблиця 1.5 – Параметри проведення сплайн-моделювання впливу груп економічних, соціальних, інституційних факторів на рівень тіньової економіки

Model specifications	Економічні фактори на SE	Соціальні фактори на SE	Інституційні фактори на SE
Independents	5	5	5
Dependents	1	1	1
Number of terms	3	4	3
Number of basis functions	2	3	2
Order of interactions	1	1	1
Penalty	2,000000	2,000000	2,000000
Threshold	0,000500	0,000500	0,000500
GCV error	11,45123	7,645729	4,449249
Prune	Yes	Yes	Yes

Джерело: власні розрахунки автора

Розглянемо побудовані моделі впливу економічних, соціальних та інституційних факторів на рівень тіньової економіки у вигляді багатомірних адаптивних регресивних MAR-сплайнів (рис. 1.13):

А

Model coefficients (Spreadsheet7.sta)
NOTE: Highlighted cells indicate basis functions of type max(0, independent-knot), otherwise max(0, knot-independent)

Coefficients, knots and basis functions	Coefficients SE	Knots TAX	Knots GFCE	Knots MON	Knots TRD	Knots SOE
Intercept	54,64627					
Term 1	-0,32680				53,00000	
Term 2	-0,25871	62,30000				

Б

Model coefficients (Spreadsheet7.sta)
NOTE: Highlighted cells indicate basis functions of type max(0, independent-knot), otherwise max(0, knot-independent)

Coefficients, knots and basis functions	Coefficients SE	Knots INC_L	Knots INC	Knots WG_G	Knots UNM	Knots CRM
Intercept	37,26822					
Term 1	1,07452		20,60000			
Term 2	1,79228				6,350000	
Term 3	-0,00024			250,0000		

В

Model coefficients (Spreadsheet7.sta)
NOTE: Highlighted cells indicate basis functions of type max(0, independent-knot), otherwise max(0, knot-independent)

Coefficients, knots and basis functions	Coefficients SE	Knots PP	Knots PFI	Knots PS	Knots RQ	Knots RL
Intercept	51,10068					
Term 1	-0,00081	360,0000				
Term 2	0,14019		19,25000			

Рисунок 1.13 – Коефіцієнти моделі та терми моделі впливу факторів на рівень тіньової економіки у вигляді багатомірних адаптивних регресивних MAR-сплайнів (А- економічні фактори; Б- соціальні фактори; В-інституційні фактори)

Джерело: власні розрахунки автора

На основі даних рисунку 1.14, багатомірний адаптивний регресивний MAR-сплайн впливу економічних факторів на рівень тіньової економіки набуває вигляду:

SE = 5,46462734897707e+001 - 3,26803688902672e-001*max(0; TRD-5,30000000000000e+001) - 2,58705503226437e-001*max(0; TAX-6,23000000000000e+001) (1.13)

SE = 3,72682189375652e+001 + 1,07451898413057e+000*max(0; INC-2,06000000000000e+001) + 1,79227748551907e+000*max(0; UNM-6,34999990463257e+000) - 2,35399929677021e-004*max(0; WG_G-2,50000000000000e+002) (1.14)

SE = 5,11006780742204e+001 - 8,10605746111352e-004*max(0; PP-3,60000000000000e+002) + 1,40192396027726e-001*max(0; PFI-1,92500000000000e+001) (1.15)

Таким чином, серед розглянутих 5 економічних факторів релевантними при дослідження впливу на рівень тіньової економіки виявлено 2 фактори: рівень торгівельної свободи (TRD) та рівень податкового навантаження (TAX).

Переходячи до аналізу залежності рівня тіньової економіки від значущих економічних факторів, зазначимо, що обидва показники TRD та TAX будуть мати від'ємний вплив у випадку набуття значення більше 53,00 та 62,30 відповідно. При прийнятті показниками TRD та TAX значень не більше 53,00 та 62,30 відповідно, вони не будуть впливати на рівень тіньової економіки. При цьому, показники TRD та TAX будуть впливати на зменшення результуючої ознаки на 0,327 та 0,259 при збільшенні зазначених факторних на 1 одиницю.

З поміж соціальних факторів впливу на рівень тіньової економіки значущими є два фактори: частка доходу, що належить найменшим 10% населення (INC) та рівень безробіття (UNM). Переходячи до аналізу залежності рівня тіньової економіки від значущих соціальних факторів, зазначимо, що показники INC та UNM будуть мати додатній вплив у випадку набуття значення більше 20,60 та 6,35 відповідно. В свою чергу, показник WG_G є дестимулятором результативної ознаки у випадку набуття значення більше 250,00. Так, при зростанні зазначених трьох факторних ознак на одиницю, рівень тіньової економіки буде зростати на 1,075 1, 792 та зменшуватись на 2,354 одиниць. При прийнятті показниками INC, UNM та WG_G значень не більше 20,60, 6,35 та 250,30 відповідно, вони не будуть впливати на рівень тіньової економіки.

Стосовно впливу інституційних факторів на динаміку зміну рівня тіньової економіки виявлено, що значущими є 2 індикатори: кількість політичних партій (PP) та індекс свободи преси (PFI). Зокрема, показники PP та PFI мають протилежний характер впливу на рівень тіньової економіки:

обернений та прямий відповідно у випадку набуття значення більше 360,0 та 19,25. При прийнятті показниками PP та PFI значень не більше зазначених рівнів, вони не будуть впливати на рівень тіньової економіки. При цьому, показники PP та PFI будуть впливати на зменшення та збільшення результуючої ознаки на 0,00081 та 14,02 при збільшенні зазначених факторних на 1 одиницю.

Для доведення адекватності представлених вище моделей (1.13)-(1.15) розглянемо наведені в таблиці 1.6 індикатори.

Таблиця 1.6 – Регресійні статистики моделей MAR-сплайнів залежності рівня тіньової економіки від груп економічних, соціальних та інституційних факторів

Regression statistics	Економічні фактори на SE	Соціальні фактори на SE	Інституційні фактори на SE
Mean (observed)	43,08567	43,08567	43,08567
Standard deviation (observed)	5,37980	5,37980	5,37980
Mean (predicted)	43,08567	43,08567	43,08567
Standard deviation (predicted)	4,63177	4,99392	5,10220
Mean (residual)	-0,00000	-0,00000	-0,00000
Standard deviation (residual)	2,73659	2,00073	1,70580
R-square	0,74125	0,86169	0,89946
R-square adjusted	0,70243	0,83258	0,88438

Джерело: власні розрахунки автора

Аналіз таблиці 1.6 дозволяє стверджувати, що варіація рівня тіньової економіки на 74,13% пояснюється варіацію економічних факторів, на 86,17% пояснюється варіацією соціальних факторів і на 89,95% - зміною інституційних факторів. Крім того, підтвердженням достовірності та точності моделей виступають: мінімальне значення загального критерію якості моделі – узагальнена ковзна середня помилка (GCV error), яке приймає значення від 4,45 до 11,45; несуттєве відхилення фактичних та прогнозних значень.

Таким чином, посилення принципів ділової доброчесності дозволить зменшити прояв корупційних діянь та злочинів у сфері службової діяльності у процесі прийняття рішень органами державної влади та їх посадовими особами, а також розбудувати етичну культуру ведення підприємницької діяльності.

1.3.2. Вплив фінансових злочинів на стан фінансової стабільності країни в умовах діджиталізації

На сьогодні близько чверті світового ВВП перебуває у тіні. У доковідний період загальна частка тіньової діяльності у світовій економіці мала стійку тенденцію до зменшення завдяки інноваційним цифровим рішенням для моніторингу руху грошових коштів на транснаціональному рівні та обміну інформацією про фінансові транзакції у рамках співпраці національних регуляторів та міжнародних організацій. Проте пандемія короновірусу спровокувала різке падіння ВВП і значне зростання рівня безробіття, наслідком чого у 2020 році став рекордний темп зростання тіньової економіки по країнам ЄС, а саме на 9,8 більше порівняно з 2019 роком (Schneider, (2022).

На сьогодні питання протидії тінізації національної економіки досі залишається одним із ключових викликів для стабільного розвитку країни, оскільки провокує зниження податкових надходжень у державні фонди, деформує ринкові конкурентні відносини між економічними агентами, сприяє розвитку неформальної трудової зайнятості, й загалом призводить до неефективного функціонування бюджетної системи на всіх рівнях, що спричинює недофінансування суспільно важливих бюджетних витрат та зростання соціальної напруги в суспільстві. Попри декларування багатьма урядами заходів з детінізації національної економіки, протягом десятиріччя (2008-2017рр.) у 39 з поміж 144 аналізованих країнах світу зафіксовано збільшення обсягів тіньової економіки, тоді як протягом пятиріччя (2013-2017 р.) – вже налічувалося 62 країни з позитивним приростом тіньової економіки. Таким чином, тіньові процеси інтенсивно укорінюються в систему економічних відносин країн, що передбачає необхідність розробки комплексу фінансово-економічних заходів, удосконалення роботи правоохоронних та судових органів, а також кардинальної зміни колективної свідомості у суспільстві щодо толерування проявів протиправної діяльності в країні. Надійні інституції забезпечують необхідний захист від корупції та конфіскації приватної власності (Berdiev & Saunoris, 2016).

Надмірний рівень тіньової економіки робить вразливою фінансову систему країни. Албулеску та ін. (2016) стверджують, що високий рівень фінансової стабільності означає кращий доступ до різних форм фінансування, залучення приватних інвестиційних ресурсів та коштів міжнародних організацій. З іншого боку, зниження рівня фінансової стабільності може спровокувати скорочення загального обсягу доходу та ускладнення доступу до фінансових ресурсів. У підсумку, економічні агенти будуть схильні розвивати неформальні види діяльності, ухилятися від сплати податків та функціонувати в тіньовому секторі економіки. Крім цього, наслідки протиправної економічної діяльності прослідковується в зростанні неочікуваних кредитних збитків, волатильності валютного курсу, виділенні коштів центральним банком для підтримки окремих фінансових установ тощо. Крім цього, фінансовий сектор можна розглядати як механізм стримування темпів та зменшення обсягів нелегальних фінансових операцій в країні за

рахунок встановлення лімітів використання готівки та обмеження для її використання за певними транзакціями, вимог до кредитоспроможності позичальника для отримання нового або пролонгації існуючого кредиту, граничних меж для здійснення безготівкових розрахунків як громадянами, так і суб'єктами господарювання тощо. Уряд разом з центральним банком може реалізовувати фінансову політику для моніторингу від ухилення сплати податків (Blackburn et al, 2012).

Розвиток цифрових фінансових технологій підвищує швидкість фінансових операцій і створює умови для стабільних і безпечних транзакцій. Розширення цифрових фінансових послуг також збільшує частку населення, що не користується банківськими послугами, у офіційних банківських послугах, і таким чином диверсифікує ринкові ризики та сприяє стабільності фінансового сектора (Pazarbasioglu & Mora, 2020). Водночас акумулювання значного масиву даних про фінансові транзакції та використання технологій штучного інтелекту для їх аналізу дозволяють якісно проводити моніторинг джерел походження коштів та напрямків використання. Таким чином, цифрові фінансові технології створюють базис для формування нових концепцій до вивчення передумов виникнення тіньової економіки, пошуку механізмів протидії неформальним економічним відносинам, а також для забезпечення фінансової стабільності в країні.

Для визначення ландшафту наукових публікацій з даної проблематики проведено бібліографічний аналіз. Джерелом бібліографічних даних для даного дослідження обрано міжнародну наукометричну базу даних Scopus від Elsevier (таблиця 1.7).

Таблиця 1.7 – Результати пошуку наукових публікацій за визначеними напрямками, проіндексованих БД Scopus

Пошуковий запит	2003-2007	2008-2012	2013-2017	2018-2022	Всього
"shadow economy" OR "illegal economy" OR "informal economy" OR "underground economy" OR "parallel economy"	402	862	1430	1985	4379
"finan* stab*" AND digit* OR tech* OR electron* OR cyber*	51	96	202	618	967
"shadow economy" OR "illegal economy" OR "informal economy" OR "underground economy" OR "parallel economy" AND digit* OR tech* OR electron* OR cyber*	19	74	160	369	626

Джерело: власні розрахунки автора

Для аналізу наукових публікацій, присвячених питанням тіньової економіки та фінансової стабільності в контексті цифрових фінансових трансформацій, обрано двадцятирічний період з розбивкою на менші періоди: 1) І період - 2003-2007 рр. (вплив цифровізації на сферу фінансових відносин

є мінімальним); II період - 2008-2012 рр. (початок розвитку fintech, поява перших криптовалют та нових технологій, таких як P2P, електронні гаманці); III період - 2013-2017 рр. (експоненціальне зростання платіжного сегменту Fintech, розвиток венчурного інвестування); IV період - 2018-2022 рр. (зростання нових технологій BaaS, PaaS, IaaS, розвиток хмарних технологій, розвиток альткоїнів). В англомовній науковій літературі для характеристики тіньової економіки використовуються різні терміни (illegal economy, underground economy, parallel economy, informal economy), які нами було враховано при пошуку наукових публікацій з даної тематики.

Дані таблиці 1.7 вказують, що протягом останніх двох десятиріч опубліковано 4379 наукових публікацій, які стосуються питань тіньової економіки. Попри багаторічні наукові напрацювання з даної тематики, дослідження питань тіньової економіки у кожний з аналізований пятирічний період постійно зростає. Зокрема, протягом 2018-2022 років опубліковано 1985 публікацій, проіндексованих наукометричною базою даних Scopus, що на 38,8% та 130,3% більше порівняно з 2013-2017 рр. та 2008-2012 роками відповідно. Питаннями тіньової економіки найбільше у світі займаються дослідники зі США (897 публікацій або 20,5 % від загального обсягу) та Великобританії (753 публікацій або 17,2%). При цьому, основними науковими центрами, дослідники яких вивичають питання тіньової економіки, є Sheffield University Management School (178 публікацій), The University of Sheffield (101 публікацій), Johannes Kepler University Linz (89 публікацій), University of Johannesburg (57 публікацій), London School of Economics and Political Science (45 публікацій). Найбільш видатними науковцями, які досліджують тіньову економіку є Williams C.C. (Sheffield University Management School, UK), яким опубліковано 215 публікацій, проіндексоданих базою даних Scopus, та Schneider F. (Johannes Kepler University Linz, Austria) - 81 публікацію.

Тіньова економіка має значний негативний вплив у короткостроковій перспективі, що відображається у збільшенні податкового тягаря на економічних суб'єктів, які функціонують у правовому полі. Проте тіньова економіка також має позитивний вплив на економічне зростання в довгостроковій перспективі, фактично коли вона є заходом для виживання для малозабезпеченого населення (Medina & Schneider, 2021).

Другий пошуковий запит спрямований на визначення публікацій, присвячених питанням фінансової стабільності в контексті цифрових змін. Протягом 2003-2022 років опубліковано 967 наукових праць у виданнях, що включені до наукометричної бази даних Scopus, при цьому 64% з них було надруковано протягом останніх п'яти років. Це дозволяє стверджувати, що розвиток цифрових інформаційних технологій загострив питання забезпечення фінансової стабільності країни. Стрімкий розвиток інформаційних технологій та нарощення масштабів венчурного інвестування трансформував традиційні моделі комерційних банків і змусив фінансові установи оптимізувати їх витрати, шукати нетрадиційні джерела доходів та

співпрацювати з фінтех компаніясм для розробки інноваційних фінансових продуктів або удосконалення бізнес-процесів.

На думку Khattak et al. цифрова трансформація зумовить зміни у внутрішньому та зовнішньому середовищі функціонування комерційних банків. Зміни у зовнішньому середовищі пов'язані з появою нових небанківських учасників на ринку фінансових послуг, що призводить до посилення конкурентної боротьби та залучення банківськими установами технологій фінтех-компаній. Цифрова трансформація відьувається й всередині банку – впровадження банками передових сучасних технологій (штучний інтелект, блокчейн, великі дані, технології хмарних обчислень тощо). Проте технологізація фінансового сектору не лише позитивно впливає на розвиток фінансового сектору та економічне зростання, але й спричинює негативні наслідки. Полегшення доступу до кредитних ресурсів призводить до збільшенню обсягу непрацюючих кредитів, тоді як надмірне використання фінтех-технологій збільшує цифрові ризики, такі як крадіжка даних, збої в платіжних системах тощо (Vives, 2019).

Третій пошуковий запит орієнтований на дослідження впливу діджиталізації на темпи розвитку тіньової економіки. Кількість публікацій з даного напрямку з кожним періодом екпоненційно зростає. Протягом останнього десятиріччя (2013-2017 та 2018-2022) опубліковано 85% наукових праць за цією тематикою. У низці наукових робіт (Haruna & Alhassa, 2022; Boitan & Ștefoni, 2023; Silalahi, 2022) емпірично доведено, що діджиталізація сприяє зменшенню темпів поширення тіньової економіки незалежно від рівня економічного розвитку країни. Практика багатьох краї світу засвідчує, що зменшення обсягу готівкових операцій та збільшення безготівкоих розрахунків призводить до пропорційного скорочення розміру тіньової економіки. Фахівцями консалтингової компанії ATKearney&VISA визначено, що за умови зростання безготівкових розрахунків щорічно на 10% протягом 5 років це дозволило б додатково акумулювати 1,2 трлн дол США, що співрозмірно розмірам економіки Канади (ATKearney &VISA, 2017).

У роботі оцінено довгостроковий взаємозв’язок між розвитком цифрових фінансів, тіньової економіки та фінансової стабільності на прикладі країн Південної Азії на основі використання коінтеграційних регресійних моделей. Встановлено, що фінансова цифровізація сприяє зменшенню частки тіньової економіки у ВВП. Проте надмірне здійснення грошових транзакій з використання мобільного пристрою та банкоматів у країнах, що розвиваються, сприяє нестабільності фінансового сектора через збільшення відсотка проблемних кредитів і співвідношення банківських кредитів до депозитів (Syed et al, 2021).

Метою даного дослідження - оцінити характер та ступінь взаємозв’язків між тіньовою економікою, стабільністю фінансової системи та фінансовою цифровізацією. Для досягнення поставленої мети запропоновано використовувати когнітивне моделювання. Когнітивний підхід представляє собою процес моделювання поведінкових патернів складних систем у

відповідь на зміни середовища на основі аналізу факторів, які кількісно й якісно характеризують стан цієї системи. Специфіка застосування методів когнітивного моделювання полягає в тому, що відбувається визначення сили та напрямку впливу факторів на об’єкта управління із урахуванням схожості та відмінності у впливі різних факторів на об’єкт управління (Lebid, 2015). Об'єктом управління обрано обсяг тіньової економіки до ВВП, тоді як пояснювальними факторами запропоновано три групи індикаторів: 1 група – індикатори, які характеризують опосередковану участь фінансових установ в протиправній діяльності; 2 група - індикатори, що відображають стан діджиталізації фінансових послуг; 3 група - індикатори для характеристики фінансової стабільності країни (таблиця 1.8).

Таблиця 1.8 – Вхідні змінні

Ідикатор		Пояснення	Джерело
Тіньова економіка	SE	Обсяг тіньової економіки до ВВП, %	Schneider
Участь фінансових установ в обслуговуванні тіньової економіки	CASH	Співвідношення готівки (M0) до ВВП	НБУ
	CLP	Співвідношення безготівкових карткових операцій до загальної кількості трансакцій	НБУ
	DOL	Рівень доларизації економіки*	НБУ
	F_FDI	Рівень фіктивних прямих інвестицій, % ВВП*	НБУ
Діджиталі-зація фінансових послуг	ATM	Кількість банкоматів на 100 000 дорослого населення	НБУ
	TER	Кількість платіжних терміналів на 100 000 дорослого населення	НБУ
	BRN_C	Кількість відділень комерційних банків на 100 000 дорослого населення	НБУ
	PMT	Обсяг приватних грошових переказів через коррахунки банків та міжнародні платіжні системи, % ВВП	НБУ
	DEP_A	Кількість депозитних рахунків на 1000 осіб дорослого населення	НБУ
	LOAN_A	Кількість кредитних рахунків у всіх мікрофінансових організаціях на 1000 осіб дорослих	IMF
	DBT_C	Кількість дебетових карток на 1000 осіб дорослих	IMF
	ONL_B	Частка громадян, що користовуються онлайн банкінгом	IMF
	NVT	Співвідношення вартості мережі Bitcoin до транзакцій	Blockchain
Фінансова стабільність	ROA	Рентабельність активів, % *(ризик прибутковості)*	НБУ
	RCA	Норматив достатності (адекватності) регулятивного капіталу *(ризик ліквідності)*	НБУ
	NPL	Частка непрацюючих кредитів, % *(кредитний ризик)*	НБУ
	GDP	Зміна реального ВВП, % до попереднього року *(макроекономічний ризик)*	НБУ
	LIQ	Норматив короткострокової ліквідності *(ризик капіталу)*	НБУ
	EXR	Середньорічна волатильність обмінного курсу* *(валютний ризик)*	НБУ

* розрахункові показники

У таблиці 1.8 містяться декілька відносних показників, які були попередньо визначені на основі первинних даних: рівень доларизації економіки (відношення обсягу депозитів резидентів та нерезидентів в іноземній валюті до грошової маси (грошовий агрегат М3)), середньорічна волатильність обмінного курсу (відношення стандартного відхилення вартості національної валюти в дол США за заданий проміжок часу до аналізованого періоду); рівень фіктивних прямих інвестицій (відношення обсягу вхідного та вихідного потоку прямих іноземних інвестицій, ініціатором або отримувачем яких є країна з офшоної зони, до ВВП країни,%) (Lieonov et al., 2019). Для характеристики рівня фінансової стабільності країни використано розроблену Національним банком України карту ризиків, охоплює макроекономічний ризик, .ризик прибутковості, ризик ліквідності, кредитний ризик, ризик капіталу та валютний ризик.

Запропонований науково-методичний підхід до оцінювання системи взаємозв'язків у ланцюзі відносин «тіньова економіка-фінансова діджиталізація -фінансова стабільність» передбачає реалізацію наступних етапів:

– визначення сукупності факторів (індикаторів), які впливають на об'єкт управління - тіньова економіка;

– визначення факторів, які мають статистично значимий зв'язок з об'єктом управління;

– побудова когнітивної карти для ідентифікація характеру впливу між факторами та об'єктом управління;

– кількісне визначення ступеня впливу факторів на тіньову економіку на основі лінійних та нелінійних рівнянь;

– побудова оптимізаційної моделі для визначення ймовірного зменшення обсягу тіньової економіки за умови поточного стану розвитку цифрових фінансів та рівня фінансової стабільності в країні;

– аналіз та інтерпретація отриманих результатів.

Апробація запропонованого науково-методичного підходу проведена на основі статистичних даних про Україну, тоді як періодом для дослідження обрано 2005-2021 роки.

На початковому етапі для пояснення динаміки зміни тіньової економіки обрано 21 індикатор. Для виявлення найбільш суттєвих чинників, що впливають на досліджувану об'єкт - тіньову економіку - використано кореляційний аналіз. Для оцінювання тісноти статистичного зв'язку між досліджуваними змінними та обсягом тіньової економіки розраховано коефіцієнт кореляції, результати чого подано в таблиці 1.9. Для подальших розрахунків відібрано показники, для яких коефіцієнт кореляції більше за 0,5.

За результати кореляційного аналізу, 9 з поміж 21 показника мали середній та високий ступінь зв'язку з результатним показником. Виходячи з цього, дані індикатори й будуть слугувати основою для побудови когнітивної карти.

Таблиця 1.9 – Результати кореляційного аналізу

Участь фінансових установ в обслуговуванні тіньової економіки		Діджиталізація фінансових послуг	
CASH	0,319	ATM	-0,697*
CLP	-0,501*	TER	-0,527*
DOL	-0,154	BRN_C	0,568*
F_FDI	0,532*	PMT	0,441
Фінансова стабільність		DEP_A	0,004
ROA	-0,290	LOAN_A	0,447
RCA	-0,600	DBT_C	-0,330
NPL	-0,568*	ONL_B	-0,665*
GDP	0,596*	NVT	-0,057
LIQ	-0,278		
EXR	0,006		

* - статистично значимі індикатори

Джерело: власні розрахунки автора

Основним інструментом когнітивного моделювання є когнітивна карта – це зручна і ефективна техніка візуалізації причинно-наслідкових зв'язків факторів з об'єктом управління. Когнітивна карта складається з вершин (системно значущі фактори впливу на систему) та дуг (причинно-наслідкові зв'язки між факторами).

Згідно з концепцією когнітивного консонансу, об'єктом управління формується під дією низки факторів, які відповідають таким критеріям (Мокін, 2018):

Критерій 1. Чинник має вплив на вершину системи (об'єктом управління);

Критерій 2. Чинник є кількісно вимірюваним;

Критерій 3. На чинник впливають інші чинники.

Критерій 4. Кожному чиннику відповідає окремий інструмент управління.

Результат побудови когнітивної карти для попередньо відібраних 9 чинників впливу на об'єкт управління – тіньову економіку подано на рисунку 1.14.

Підґрунтям для побудови когнітивної карти є врахування принципів системної динаміки, при цьому зв'язки між об'єктами визначалися як на основі результатів кореляційного аналізу, так і суб'єктивних припущень. Інформаційно-статистична база для проведення розрахунків подана в таблиці 1.10.

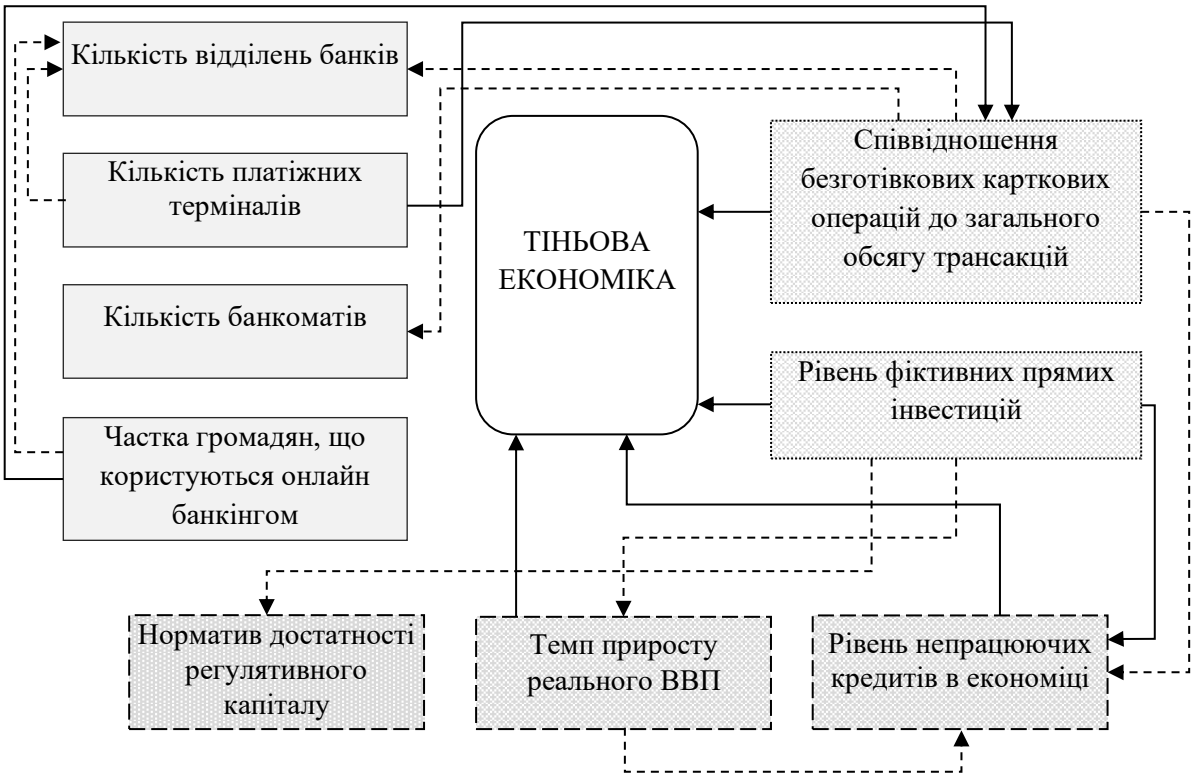


Рисунок 1.14 – Когнітивна карта моделювання впливу факторів на тіньову економіку

Джерело: власна розробка автора

Таблиця 1.10 – Динаміка рівня тіньової економіки та визначальних факторів її розвитку за період з 2005 по 2021 рр.

	SE	CLP	ATM	TER	BRN_C	RCA	NPL	GDP	ONL_B	F_FDI
2005	37	3,2044	28,16	830,772	3,86	14,65	5,8	27,9073	19,7	14,8
2006	33,5	3,3077	36,72	1056,76	3,87	13,98	6,2	23,5485	22,1	14,2
2007	34,5	3,6061	52,42	1553,92	3,86	13,92	4,3	32,9349	27,68	14,6
2008	35,5	4,5594	70,37	2373,3	3,74	13,08	3,1	31,9147	30,76	14
2009	30	5,2029	73,14	2950,88	3,22	18,28	4,5	-4,41826	33,71	13,4542
2010	33	6,5379	76,57	2616,41	2,33	20,34	14,1	13,9702	37,11	12,8946
2011	32	8,0465	84,3	2762,7	1,6	18,51	17	20,4425	39,18	12,7786
2012	30	12,351	92,8	3171,3	1,07	18,09	17,6	8,05221	40,88	14,2873
2013	30	17,373	104,06	4196,43	0,92	17,55	19,3	4,30913	42,91	15,1654
2014	36	25,043	95,09	5748,31	0,77	14,03	16,3	8,3072	45,33	16,3909
2015	35	31,213	87,12	5326,73	0,56	8,92	22	25,3088	47,08	22,8069
2016	33	35,477	88,77	5110	0,5	13,34	31,7	19,9555	49,03	21,5614
2017	32	39,298	97,83	5796,27	0,45	15,35	49,4	24,9798	51,9	17,3052
2018	29	45,104	97,39	6699,59	0,43	15,52	52,1	19,424	54,37	14,0283
2019	27	50,277	96,3	7967,21	0,42	18,72	48,9	11,7096	57,5	13,864
2020	30	55,814	93,74	9446,04	0,41	21,63	45,7	6,15579	60,78	12,5071
2021	32	60,807	91,24	11793,3	0,39	21,44	37,8	29,1051	60,62	12,2246

Джерело: власні розрахунки автора

Для врахування лагової затримки між зміною результативного показника та факторними змінними були взяті перші різниці. Проміжні результати розрахунку досліджуваних змінних з урахуванням лагової затримки в 1 рік подано в таблиці 1.11.

Таблиця 1.11 – Динаміка рівня корупції та визначальних факторів його формування за період з 2005 по 2021 рр. з урахуванням лагової затримки в 1 рік

	SE (t-1)	CLP(t-1)	ATM(t-1)	TER(t-1)	BRN_C(t-1)	RCA(t-1)	NPL (t-1)	GDP(t-1)	ONL_B(t-1)	F_FDI(t-1)
2005	39	5,36	20,09	655,23	3,71	13,50	5,30	28,91	17,73	15,45
2006	37	3,20	28,16	830,77	3,86	14,65	5,80	27,91	19,70	14,80
2007	33,5	3,31	36,72	1056,76	3,87	13,98	6,20	23,55	22,10	14,20
2008	34,5	3,61	52,42	1553,92	3,86	13,92	4,30	32,93	27,68	14,60
2009	35,5	4,56	70,37	2373,30	3,74	13,08	3,10	31,91	30,76	14,00
2010	30	5,20	73,14	2950,88	3,22	18,28	4,50	-4,42	33,71	13,45
2011	33	6,54	76,57	2616,41	2,33	20,34	14,10	13,97	37,11	12,89
2012	32	8,05	84,30	2762,70	1,60	18,51	17,00	20,44	39,18	12,78
2013	30	12,35	92,80	3171,30	1,07	18,09	17,60	8,05	40,88	14,29
2014	30	17,37	104,06	4196,43	0,92	17,55	19,30	4,31	42,91	15,17
2015	36	25,04	95,09	5748,31	0,77	14,03	16,30	8,31	45,33	16,39
2016	35	31,21	87,12	5326,73	0,56	8,92	22,00	25,31	47,08	22,81
2017	33	35,48	88,77	5110,00	0,50	13,34	31,70	19,96	49,03	21,56
2018	32	39,30	97,83	5796,27	0,45	15,35	49,40	24,98	51,90	17,31
2019	29	45,10	97,39	6699,59	0,43	15,52	52,10	19,42	54,37	14,03
2020	27	50,28	96,30	7967,21	0,42	18,72	48,90	11,71	57,50	13,86
2021	30	55,81	93,74	9446,04	0,41	21,63	45,70	6,16	60,78	12,51

Джерело: власні розрахунки автора

Наступним етапом розробленого науково-методичного підходу є формалізація форми взаємозв'язку між досліджуваними показниками за допомогою лінійних або нелінійних (поліноміальної, логарифмічної, гіперболічної та ступеневої функцій) економетричних залежностей, яку візуально представлені на когнітивній карті. Розрахунки проведені з використанням програмного статистичного пакету Statistica. У подальшому будуть наведені результати формалізації взаємозалежності між показниками з найвищими показниками адекватності побудових економетричних моделей.

1. Індикатори тіньової економіки та фінансової стабільності.

Зв'язок тіньової економіки (SE) з попередньо визначеними значущими показниками - частки безготівкових карткових операцій (CLP), частки

непрацюючих кредитів (NPL), зміни реального ВВП (GDP) та рівня фіктивних прямих інвестицій (F_FDI) у лінійній комбінації наведено на рисунку 1.15.

N=17	Regression Summary for Dependent Variable: SE (Spreadsheet1.sta) R= ,73456072 R?= ,53957945 Adjusted R?= ,38610593 F(4,12)=3,5158 p<,04037 Std.Error of estimate: 2,1544					
	Beta	Std.Err. of Beta	B	Std.Err. of B	t(12)	p-level
Intercept			33,50814	3,182008	10,53050	0,000000
CLP(t-1)	0,98443	0,675174	0,14633	0,100359	1,45804	0,170499
NPL (t-1)	-1,57747	0,641961	-0,24676	0,100421	-2,45726	0,030189
GDP(t-1)	-0,07932	0,221607	-0,02024	0,056557	-0,35791	0,726624
F_FDI(t-1)	0,09729	0,233466	0,09295	0,223072	0,41670	0,684253

Рисунок 1.15 – Результати побудови регресійної моделі для оцінювання зв'язку між тіньовою економікою та фінансовою стабільністю

Джерело: власні розрахунки автора

На основі рисунку 1.15 можна стверджувати, що статистично значущим (p-рівень не менше 0,05 частки одиниці) є виключно показник "частка непрацюючих кредитів" з лагом в 1 рік, тоді як всі інші показники є значимими на рівні значимості 90%. Регресійне рівняння матиме наступний вигляд:

$$SE_t = 33.508 + 0.146 \cdot CLP_{t-1} - 0.247 \cdot NLP_{t-1} - 0.020 \cdot GDP_{t-1} + 0.093 \cdot F\_FDI_{t-1} \quad (1.16)$$

Вплив фіктивних прямих інвестицій (F_FDI) на рівень макроекономічного ризику в країні, що описується як зміна реального ВВП по відношенню до попереднього періоду (GDP), представлено на рисунку 1.16.

N=17	Regression Summary for Dependent Variable: GDP (Spreadsheet1.sta) R= ,21484417 R?= ,04615802 Adjusted R?= ----- F(1,15)=,72588 p<,40762 Std.Error of estimate: 10,880					
	Beta	Std.Err. of Beta	B	Std.Err. of B	t(15)	p-level
Intercept			5,538777	14,69970	0,376795	0,711603
F_FDI(t-1)	0,214844	0,252170	0,805277	0,94518	0,851983	0,407621

Рисунок 1.16 – Результати побудови регресійної моделі для оцінювання зв'язку між фіктивними прямими інвестиціями та зміною реального ВВП

Джерело: власні розрахунки автора

Рівень зв'язку між аналізованими індикаторами є значущим на рівні 90% та описується наступним рівнянням:

$$GDP_t = 5.539 + 0.805 \cdot F\_FDI_{t-1} \quad (1.17)$$

Між кредитним ризиком (NPL), макроекономічним ризиком (GDP) та рівнем безготівкових розрахунків в економіці (CLP) формалізовано нелінійну залежність (рис. 1.18).

N=16	Regression Summary for Dependent Variable: NPL (Spreadsheet1.sta) R= ,97325296 R?= ,94722132 Adjusted R?= ,92083198 F(5,10)=35,894 p<,00000 Std.Error of estimate: 5,0352					
	Beta	Std.Err. of Beta	B	Std.Err. of B	t(10)	p-level
Intercept			-119,347	67,0053	-1,78116	0,105228
SQRV12	0,465164	0,496197	4,001	4,2677	0,93746	0,370611
1/V18	0,529675	0,535230	165,211	166,9442	0,98962	0,345700
LN-V12	0,482124	0,519847	8,095	8,7279	0,92743	0,375543
V18**2	-0,738693	0,349545	-0,037	0,0177	-2,11330	0,060705
LN-V18	1,385141	0,791031	39,194	22,3831	1,75106	0,110491

Рисунок 1.18 – Результати побудови регресійної моделі для оцінювання зв'язку між рівнем безготівкових розрахунків та індикаторами фінансової стабільності

Джерело: власні розрахунки автора

Безготівкові розрахунки в економіці України на 94,7% пояснюються зміною частки непрацюючих кредитів та реального валового внутрішнього продукту. Нелінійна залежність між змінними описується наступним рівнянням:

$$NPL_t = -119.347 + 4.001 \cdot \sqrt{CLP_{t-1}} + 165.244 \cdot \frac{1}{GDP_{t-1}} + 8.095 \cdot ln\ ln\ (CLP_{t-1}) - 0.037 \cdot GDP_{t-1}^2 + 39.194 \cdot ln\ (GDP_{t-1}) \quad (1.18)$$

Динаміка розвитку прямих інвестицій, джерелом походження або кінцевим споживачем яких є резиденти з країни, що входить до офшоної зони, (F_FDI) подано на рисунку 1.19.

N=17	Regression Summary for Dependent Variable: F_FDI (Spreadsheet1.sta) R= ,72532871 R?= ,52610173 Adjusted R?= ,49450852 F(1,15)=16,652 p<,00098 Std.Error of estimate: 2,1131					
	Beta	Std.Err. of Beta	B	Std.Err. of B	t(15)	p-level
Intercept			29,423	3,54477	8,30045	0,000001
1/V20	-0,725329	0,177745	-213,239	52,25518	-4,08073	0,000984

Рисунок 1.19 – Результати побудови регресійної моделі для оцінювання динаміки розвитку фіктивних прямих інвестицій

Джерело: власні розрахунки автора

Модель залежності фіктивних прямих інвестицій від власних попередніх значень має вигляд:

$$F\_FDI_t = 29.423 - 213.239 \cdot \frac{1}{F\_FDI_{t-1}} \quad (1.19)$$

1. Індикатори тіньової економіки та діджиталізації фінансових послуг.

Вплив фіктивних прямих інвестицій (F_FDI) на рівень прибутковості на ринку фінансових послуг (RCA) представлено на рисунку 1.20.

Regression Summary for Dependent Variable: RCA (Spreadsheet1.sta)
R= ,73394365 R?= ,53867328 Adjusted R?= ,47276947
F(2,14)=8,1736 p<,00445 Std.Error of estimate: 2,4664

N=17	Beta	Std.Err. of Beta	B	Std.Err. of B	t(14)	p-level
Intercept			-198,672	82,6831	-2,40281	0,030703
1/V20	3,886030	1,363091	1305,698	457,9957	2,85090	0,012827
SQRV20	3,330981	1,363091	32,677	13,3721	2,44370	0,028386

Рисунок 1.20 – Результати побудови регресійної моделі для оцінювання зв'язку між фіктивними прямими інвестиціями та рентабельністю активів

Джерело: власні розрахунки автора

Враховуючи представлені на рисунку 1.20 результати, можна стверджувати про статистично значущий нелінійний зв'язок між рівнем фіктивних прямих інвестицій та рентабельністю активів, про що свідчать статистика Стьюдента (фактичне значення за абсолютним рівнем перевищує критично допустимий рівень). Формалізація взаємозвязку між цими змінними подано в наступній формулі:

$$RCA_t = -198.672 + 1305.698 \cdot \frac{1}{F\_FDI_{t-1}} + 32.677 \cdot \sqrt{F\_FDI_{t-1}} \qquad (1.20)$$

На рисунку 1.21 представлено результати нелінійного оцінювання зв'язку частки безготівкових карткових операцій (CLP) з кількістю платіжних терміналів (TER).

Regression Summary for Dependent Variable: CLP (Spreadsheet1.sta)
R= ,98610919 R?= ,97241134 Adjusted R?= ,96321512
F(4,12)=105,74 p<,00000 Std.Error of estimate: 3,9155

N=17	Beta	Std.Err. of Beta	B	Std.Err. of B	t(12)	p-level
Intercept			578,6	349,67	1,65460	0,123906
TER(t-1)	5,48764	1,994259	0,0	0,02	2,75172	0,017546
1/V14	-0,83168	0,723498	-41349,3	35970,79	-1,14952	0,272735
V14**2	-2,21931	0,872724	-0,0	0,00	-2,54296	0,025797
LN-V14	-3,23068	1,837162	-83,3	47,36	-1,75852	0,104110

Рисунок 1.21 – Результати побудови регресійної моделі для оцінювання зв'язку між часткою безготівкових карткових операцій та кількістю платіжних терміналів

Джерело: власні розрахунки автора

$$CLP_t = 578.6 - 41349.3 \cdot \frac{1}{TER_{t-1}} - 83.3 \cdot ln\,(TER_{t-1}) \qquad (1.21)$$

Зв'язок між кількістю відділень комерційних банків (BRN_C), часткою громадян, що користовуються онлайн банкінгом (ONL_B), рівнем безготівкових розрахунків (CLP) та кількістю платіжних терміналів (TER) описується нелінійною функцією (рисунок 1.22).

N=17	Regression Summary for Dependent Variable: BRN_C (Spreadsheet1.sta) R= ,98488341 R?= ,96999533 Adjusted R?= ,96307117 F(3,13)=140,09 p<,00000 Std.Error of estimate: ,27893					
	Beta	Std.Err. of Beta	B	Std.Err. of B	t(13)	p-level
Intercept			-7,28572	4,24984	-1,71435	0,110190
1/V12	0,698520	0,106497	9,49863	1,44816	6,55909	0,000018
1/V19	0,689691	0,205441	83,48733	24,86871	3,35712	0,005150
LN-V14	0,365946	0,238108	0,67078	0,43645	1,53689	0,148297

Рисунок 1.22 – Результати побудови регресійної моделі для оцінювання зв'язку між індикаторами діджиталізації фінансового сектора та рівнем безготівкових розрахунків

Джерело: власні розрахунки автора

Побудована нелінійна регресійна модель є статистичною значущою, оскільки коефіцієнт детермінації становить 0,97. При цьому рівняння, що описує нелінінй залежність між показниками, має наступний вигляд:

$$BRN\_C_t = -7.286 + 9.499 \cdot \frac{1}{CLP_{t-1}} + 83.487 \cdot \frac{1}{ONL\_B_{t-1}} + 0.671 \cdot ln\,(TER_{t-1})\,(TER_{t-1}) \quad (1.22)$$

Для визначення динамічних закономірностей у використанні платіжних терміналів (TER) враховано не лише поточні, а й попередні значення даного показника (рисунок 1.23).

N=17	Regression Summary for Dependent Variable: TER (Spreadsheet1.sta) R= ,98519496 R?= ,97060910 Adjusted R?= ,96382659 F(3,13)=143,10 p<,00000 Std.Error of estimate: 577,78					
	Beta	Std.Err. of Beta	B	Std.Err. of B	t(13)	p-level
Intercept			-8168,33	7758,464	-1,05283	0,311596
TER(t-1)	-0,093451	0,682417	-0,11	0,806	-0,13694	0,893175
V14**2	0,761861	0,413896	0,00	0,000	1,84071	0,088597
LN-V14	0,362575	0,318942	1391,00	1223,603	1,13681	0,276140

Рисунок 1.23 – Результати побудови регресійної моделі для оцінювання закономірностей у розвитку платіжних терміналів

Джерело: власні розрахунки автора

$$TER_t = -8168.33 - 0.11 \cdot TER_{t-1} + 1391.00 \cdot ln\,(TER_{t-1}) \quad (1.23)$$

Результати оцінювання зв'язку між кількістю банкоматів (ATM) та рівнем безготівкових розрахунків (CLP) представлено на рисунку 1.24.

N=17	Regression Summary for Dependent Variable: ATM (Spreadsheet1.sta) R= ,78764708 R?= ,62038792 Adjusted R?= ,59508045 F(1,15)=24,514 p<,00017 Std.Error of estimate: 14,039					
	Beta	Std.Err. of Beta	B	Std.Err. of B	t(15)	p-level
Intercept			100,380	5,28716	18,98566	0,000000
1/V12	-0,787647	0,159083	-162,805	32,88217	-4,95116	0,000174

Рисунок 1.24 – Результати побудови регресійної моделі для оцінювання зв'язку між кількістю банкоматів та рівнем безготівкових розрахунків

Джерело: власні розрахунки автора

Дані рисунку 1.24 наочно демонструють, що рівень безготівкових розрахунків з урахуванням лагової затримки в один рік є статистично значущим для поясненння зміни кількості банкоматів у країні. Гіперболічна залежність між кількістю банкоматів та рівнем безготівкових розрахунків описується наступним рівнняням:

$$ATM_t = 100.380 - 162.805 \cdot \frac{1}{CLP_{t-1}} \qquad (1.24)$$

Зміна частки громадян, що користовуються онлайн банкінгом (ONL_B), описується не лише поточними, а й власними попередніми значеннями (рисунок 1.25).

N=17	Regression Summary for Dependent Variable: ONL_B (Spreadsheet1.sta) R= ,99652850 R?= ,99306904 Adjusted R?= ,99260698 F(1,15)=2149,2 p<,00000 Std.Error of estimate: 1,0964					
	Beta	Std.Err. of Beta	B	Std.Err. of B	t(15)	p-level
Intercept			3,882465	0,872171	4,45150	0,000466
ONL_B(t-1)	0,996528	0,021496	0,965899	0,020835	46,35951	0,000000

Рисунок 1.25 – Результати побудови регресійної моделі для оцінювання закономірностей у розвитку онлайн банкінгу

Джерело: власні розрахунки автора

Дані рисунку 1.25 вказують, що дана залежність є статистично значимою, оскільки коефіцієнт детермінації майже 1, а p-рівень - менше 0,05 частки одиниці. Рівняння, що описує даний зв'язок, має наступний вигляд:

$$ONL\_B_t = 3.882 + 0.966 \cdot ONL\_B_{t-1} \qquad (1.25)$$

Наступним етапом запропонованого науково-методичного підходу є постановка та вирішення оптимізаційної задачі оцінювання впливу діджиталізації фінансових послуг на тіньову економіку в умовах забезпечення фінансової стабільності на основі формалізованої когнітивної моделі.

Враховуючи ідентиковані вище взаємозв'язки в ланцюзі "тіньова економіка - цифрові фінанси - фінансова стабільність, а також загальний напрям мінімізації цільової функції (тіньової економіки) побудуємо оптимізаційну задачу:

$$SE_t(TER_{t-1}, ONL\_B_{t-1}, F\_FDI_{t-1} = 33.508 + 0.146 \cdot CLP_{t-1} - 0.247 \cdot NLP_{t-1} - 0.020 \cdot GDP_{t-1} + 0.093 \cdot F\_FDI_{t-1} \to min \quad (1.26)$$

$$CLP_t = 578.6 - 41349.3 \cdot \frac{1}{TER_{t-1}} - 83.3 \cdot ln\,(TER_{t-1}) \geq \frac{\sum_{t=1}^{T} CLP_t}{T}$$

$$RCA_t = -198.672 + 1305.698 \cdot \frac{1}{F\_FDA_{t-1}} + 32.677 \cdot \sqrt{F\_FDA_{t-1}} \geq \frac{\sum_{t=1}^{T} RCA_t}{T}$$

$$F\_FDI_t = 29.423 - 213.239 \cdot \frac{1}{F\_FDA_{t-1}} \leq \frac{\sum_{t=1}^{T} F\_FDI_t}{T}$$

$$GDP_t = 5.539 + 0.805 \cdot F\_FDI_{t-1} \geq \frac{\sum_{t=1}^{T} GDP_t}{T}$$

$$NPL_t = -119.347 + 4.001 \cdot \sqrt{CLP_{t-1}} + 165.244 \cdot \frac{1}{GDP_{t-1}} + 8.095 \cdot ln\,ln\,(CLP_{t-1}) - 0.037 \cdot GDP_{t-1}^2 + 39.194 \cdot ln\,(GDP_{t-1}) \leq \frac{\sum_{t=1}^{T} NPL_t}{T}$$

$$BRN\_C_t = -7.286 + 9.499 \cdot \frac{1}{CLP_{t-1}} + 83.487 \cdot \frac{1}{ONL\_B_{t-1}} + 0.671 \cdot ln\,(TER_{t-1}) \geq \frac{\sum_{t=1}^{T} BRN\_C_t}{T}$$

$$TER_t = -8168.33 - 0.11 \cdot TER_{t-1} + 1391.00 \cdot ln\,(TER_{t-1}) \geq \frac{\sum_{t=1}^{T} TER_t}{T}$$

$$ATM_t = 100.380 - 162.805 \cdot \frac{1}{CLP_{t-1}} \geq \frac{\sum_{t=1}^{T} ATM_t}{T}$$

$$ONL\_B_t = 3.882 + 0.966 \cdot ONL\_B_{t-1} \geq \frac{\sum_{t=1}^{T} ONL\_B_t}{T}$$

Для вирішення побудованої оптимізаційної задачі формалізації когнітивної моделі оцінювання впливу цифрових фінансів на динаміку поширення тіньових відносин в економіці використаємо інструментарій «Пошук рішення» MS Excel, зокрема вирішення задачі нелінійного програмування методом узагальненого градієнта. Отримані результати

представимо в таблиці 1.12 (стовпець 5) та порівняємо їх з фактичними (стовпці 3 та 4) та середніми (стовпець 2) значеннями.

Таблиця 1.12 – Результати когнітивного моделювання

Індикатор		Середнє фактичне значення	Мінімальне фактичне значення	Максимальне фактичне значення	Оптимальне значення
1		2	3	4	5
Рівень тіньової економіки		32,69	27,00	39,00	14,43
Участь фінустанов в обслуговуванні тіньової економіки	Співвідношення безготівкових карткових операцій до загальної кількості трансакцій	22,92	3,20	60,81	75,36
	Рівень фіктивних прямих інвестицій, % ВВП	15,13	12,23	22,81	10,48
Діджиталізація фінансових послуг	Кількість банкоматів	77,01	20,09	104,06	82,00
	Кількість платіжних терміналів	4447,51	655,23	11793,31	12288,91
	Кількість відділень комерційних банків	1,78	0,39	3,87	0,28
	Частка громадян, що користуються онлайн банкінгом	41,02	17,73	60,78	65,00
фінансова стабільність	Норматив достатності регулятивного капіталу	16,16	8,92	21,63	22,46
	Частка непрацюючих кредитів	22,28	3,10	52,10	15,30
	Зміна реального ВВП	18,47	-4,42	32,94	28,46

Джерело: власні розрахунки автора

За результатами вирішення оптимізаційної задачі встановлено, що рівень тіньової економіки в України з урахуванням поточного стану розвитку цифрових фінансів та рівня фінансової стабільності можна знизити до рівня 14,43% від ВВП, що на 55,8% менше порівняно зі середньорічним значенням. Проведені розрахунки засвідчують, що поточний рівень розвитку цифрових фінансів та фінансової міцності в Україні є достатнім для суттєвого скорочення тіньових операцій в економіці. Для досягнення оптимального значення тіньової економіки за умов поточної кон'юнктури фінансового ринку доцільно реалізувати комплекс заходів, спрямованих на:

– збільшення обсягу cashless економіки на чверть порівняно з 2021 роком;

– зменшення обсягу непрацюючих кредитів на 59,5%;

– оптимізацію банківської інфраструктури (зменшення кількості банкоматів на 10,1%, скорочення кількості відділень комерційних банків на 28,2%, збільшення платіжних терміналів на 4,2%);

– стимулювання громадян до користування онлайн банкінгом;

– скорочення рівня фіктивних прямих інвестицій на 14,3%.

Отже, запропонований науково-методичний підхід до визначення потенційного скорочення обсягу тіньової економіки на основі врахування когнітивного консонансу між керованими та спостережуваними факторами, Практична апробація розробленого підходу засвідчила, що побудована когнітивна карта виявилась стійкою, тобто її можна використовувати для задач когнітивного моделювання. Аналіз отриманих розрахунків дозволив сформувати комплекс рекомендацій щодо протидії тіньовій економіці в Україні за рахунок оптимізації основних пов'язаних показників. Підсумовуючи, зауважимо, що боротьба з тіньовою економікою є довгостроковими узгодженими комплексними заходами багатьох державних інституцій, для реалізації якого всі галузеві міністерства мають продовжувати конструктивний діалог з підприємствами й неурядовими організаціями. При цьому вагома роль в успішній реалізації дорожньої карти з детінізації національної економіки є удосконалення роботи контролюючих та судових органів, які мають справедливо гарантувати захист прав та свобод як людини, так прав і законних інтересів суб'єктів підприємницької діяльності.

1.3.3. Дослідження місця та значення діджиталізації в системі протидії фінансовим шахрайствам

Цифровізація фінансово-економічних відносин відкрила нові можливості для злочинців у сфері легалізації доходів, отриманих незаконним шляхом. З одного боку, цифровий слід грошей стало простіше відслідковувати, саме тому одним із напрямків протидії легалізації доходів є контроль та орієнтування на поступову відмову від готівки. З іншого боку, зловмисники можуть створювати десятки акаунтів у платіжних системах та робити сотні транзакцій не виходячи з дому. Генерація великих масивів даних в такому випадку логічно веде до застосування сучасних методів аналізу даних, заснованих на глибокому та машинному навчанні.

Переходячи до аналізу наукового доробку в сфері протидії легалізації доходів, отриманих незаконним шляхом варто зазначити, що дана тема є популярною як серед науковців-економістів, так і серед науковців у галузі юриспруденції.

Вплив легалізації доходів, отриманих незаконним шляхом на сталий розвиток досліджували Z. Dobrowolski та L. Sulkowski (2020) та запропонували стійку модель боротьби з легалізацією доходів, отриманих незаконним шляхом через посилення аудиторського потенціалу органів фінансового

контролю, і як наслідок покращення слідчих функцій парламентських наглядових органів. Визначення ризику легалізації доходів, отриманих незаконним шляхом для бізнес-сектору стало основою для дослідження J. Ferwerda та E.R. Kleemans (2019), автори довели, що ризик легалізації доходів, отриманих незаконним шляхом відрізняється для різних секторів бізнес-діяльності та встановили, що для європейського простору найвищий ризик мають компанії, діяльність яких пов'язана з казино, готельним бізнесом та реалізацією об'єктів мистецтва.

Застосування методів data mining для протидії легалізації доходів, отриманих незаконним шляхом досліджували A. Salehi, M. Ghazanfari та M. Fathian (2017). Автори провели порівняльну характеристику побудованих моделей: багатонейронної мережі персептрона, імовірнісної нейронної мережі, радіально-базисної функції та лінійної нейронної моделі в якості класифікації транзакцій банку та обрали найкращу. Отримана модель дозволяє пришвидшити процес виявлення транзакцій, які мають ризик легалізації доходів, отриманих незаконним шляхом. Натомість A.I. Canhoto (2021) досліджувала можливості використання методів машинного навчання для протидії легалізації доходів, отриманих незаконним шляхом. У дослідженні автор справедливо зауважує, що основна проблема застосування методів математичного моделювання для протидії легалізації незаконних доходів це відсутність якісних наборів даних. У доступі до науковців є дані, які дозволяють виявити нетипову фінансову поведінку особи. Але дані, які напряму пов'язують транзакції, здійснені фінансовими інституціями та факти легалізації грошей відсутні. Оскільки фактичні дані про легалізацію знаходяться у органів слідства різних країн, які є конфіденційними.

Переходячи до дослідження наукових робіт присвячених впливу цифровізації на роботу суб'єктів системи протидії легалізації кримінальним доходам, зазначимо, що безумовно діджиталізація підвищує якість фінансового моніторингу в банках та сприяє ефективнішому впровадженню рекомендацій FATF у сфері протидії легалізації. Автори Vovk et al (2020) запропонували схему вдосконалення процесу фінансового моніторингу в банку, а також сформували пропозиції щодо проведення фізичних заходів для підвищення рівня дотримання законодавства у сфері протидії легалізації доходів, отриманих незаконним шляхом. До схожого висновку дійшли і K. Said та D.Karimi (2022), зазначаючи що автоматизація банківських процесів підвищує фінансову безпеку банку та покращує фінансовий моніторинг. Особливо вагомий вплив діджиталізації на легалізацію незаконних доходів прослідковується через зменшення кількості готівки в обігу. Автори Kobushko et al (2021) доходять висновку, що готівка залишається основним інструментом прискорення легалізації незаконних доходів, а впровадження технологій безготівкового розрахунку не дає поки що очікуваного ефекту у вигляді зниження обсягів легалізації незаконних доходів використовуючи готівкові потоки. Автори встановили пряму залежність попиту на готівку та тіньової економіки.

Останні дослідження свідчать що фінтех широко впроваджується в банках в країнах що розвиваються, що дозволяє набагато швидше приєднатись фінансовим установам даних країн до глобальної системи протидії легалізації кримінальним доходам. Значна група науковців дійшла висновку про те, що впровадження цифрових технологій в комплексі покращує можливості банківського середовища та безумовно впливає на можливість оперативного виявлення незаконних операцій. Окрім зазначеного, не можна нехтувати тим, що цифровізація пришвидшує роботу співробітника відповідного органу системи протидії легілації: інтерактивний пошук замінює довге перелистування папірців, тобто економляться людино-години роботи.

A. Addo та PK. Senyo (2020) у своїх дослідженнях зупиняються на вивченні впливу цифровізації на правоохоронну діяльність, а саме боротьбу з корупцією. Так, вони визначають, що цифровізація є потужним антикорупційним інструментом. Приклади застосування цифрових технологій у прокурорській діяльності досліджував Denis de Castro Halis (2019), автор зазначає, що засоби цифровізації одночасно з підвищенням швидкості обробки документів формують й засади до їх безпосереднього контролю, забезпечуючи незалежність слідства та відповідність його законам. Окремо варто розглянути застосування сучасних технологій у судовій діяльності. Автор Yu. Mulyana (2021) зазначає, що цифровізація судів починається з електронного документообігу, але не обмежується ним: всі процеси пов’язані зі справами можуть обслуговуватись в електронному суді, або наприклад суди можуть проводитись у онлайн-форматі, що пришвидшує процес.

Легалізацію доходів, отриманих незаконним шляхом за допомогою криптовалюти досліджував C. Wronka (2022), зосереджуючись не тільки на аналізі сутності легалізації, а й можливих превентивних заходів їй протидії. Автор визначив, що віртуальні активи становлять значну загрозу легалізації незаконних доходів. А як заходи протидії легалізації пропонується введення на законодавчому рівні ліцензування діяльності з видачі криптогаманців, цим самим покладаючи відповідальність за легалізацію незаконних доходів на постачальника криптогаманців. За такого підходу з’явиться можливість регулювати створення та використання криптогаманців. А з іншого боку, постачальники криптогаманців будуть прискіпливіше ставитись до процесу ідентифікації та аутентифікації клієнтів, що однозначно позитивно вплине на протидію легалізації незаконних доходів за допомогою криптовалюти. D. Dupuis та K. Gleason (2020) займались питанням необхідності регулювання обігу криптовалюти, в контексті протидії легалізації незаконних доходів, визначаючи наявні шляхи обміну криптовалюти на фіатні кошти, що надає змогу злочинцям легалізувати кошти, отримані незаконним шляхом.

Отже, справедливо зробити висновок, що в сучасному науковому середовищі протидії легалізації доходів отриманих незаконним шляхом в умовах діджиталізації суспільства відводиться значна роль та розглядають в своїй більшості як комплекс заходів з попередження, виявлення та подальшого покарання злочинних дій, спрямованих на приховання чи маскування

незаконного походження коштів або іншого майна чи володіння ними, прав на такі кошти або майно, джерела їх походження, місцезнаходження, переміщення, а так само набуття, володіння або використання коштів чи іншого майна з метою надання правомірного вигляду володінню, їх використанню або розпорядженню ними чи дій, спрямованих на приховання джерел їх походження, а також вчинення з такими коштами або іншим майном фінансової операції чи укладення щодо них угоди за умови усвідомлення особою того, що вони були одержані злочинним шляхом.

Методи легалізації незаконних доходів можуть бути різні: застосування недосконалості платіжних систем, створення та використання фіктивних підприємств, контрабанда, використання банківських переказів, укладання договорів псевдострахування, використання ломбардів та кредитних спілок, використання криптовалюти.

Проте, з огляду нашого дослідження, їх доцільно поділити на дві групи: ті які не зазнали значних змін від цифровізації відносин, та ті, які виникли внаслідок цифровізації або ж зазнали значної модернізації внаслідок неї.

До першої групи можна віднести:

1. Використання контрабандного способу легалізації доходів, отриманих незаконним шляхом полягає у махінаціях при декларуванні готівки, дорогоцінних банківських металів. Вчиняючи злочинні дії, порушуючи митні правила, шляхом декларування у іншій країні готівки в іноземній валюті як особистих заощаджень та ухилення від декларування їх при проходженні митниці в Україні реалізується розшарування доходів. Заплутаність митних правил в різних країнах, помилки, халатність чи злочинний умисел під час проходження особою митного контролю, використання «обхідних шляхів» на державному кордоні підвищує ризик легалізації доходів, отриманих незаконним шляхом. Безумовно митні органи значно збільшили власні інструменти контролю з розвитком цифровізації, так зараз сформовані значні бази даних перевірки митної вартості та інші системи контролю за товарами, проте в межах схеми легалізації ці зміни не здійснюють суттєвий вплив.

2. Окремим прикладом легалізації доходів, отриманих незаконним шляхом є використання страхових компаній. Зловмисниками здійснюється підробка страхових випадків, оформлення договорів псевдострахування, ухилення від оподаткування. З точки зору діджиталізаційних процесів, які хоч і впливають на страхову сферу, проте сутнісно схеми легалізації не зазнали змін.

3. Використання ломбардів для обміну предметів розкоші та інших цінних активів на готівку та навпаки. Відповідно суттю схем є готівковий обіг, якого майже не стосується цифровізація.

До другої групи варто віднести:

1. Платіжні системи. За допомогою платіжних систем зловмисники здійснюють перерахунок коштів з рахунків на інші рахунки, в тому числі закордон, реалізуючи розшарування незаконних доходів. Використання

мережі підставних осіб дозволяє зменшити розміри транзакції, уникаючи їх підозрілості, що ускладнює контроль та можливості виявлення фактів легалізації. Розвиток цифровізації спричинив зростання кількості платіжних систем та поширення доступу до них з будь-якої країни. Реєстрація гаманців у платіжних системах здійснюється за простішою ніж у банках процедурою.

2. Конвертаційні центри. Створення та використання конвертаційних центрів дозволяє зловмисникам перетворювати безготівкові кошти в готівкові, що спричиняє втрату їх цифрового сліду. Афілійовані з підприємствами особи, які мають право прийняття рішень, в разі їх залучення до процесів легалізації доходів, отриманих незаконним шляхом допомагають заплутувати походження коштів шляхом переуступки права вимоги по боргам, надання чи отримання благодійної допомоги. Цим самим замінюючи реальне походження коштів. Іншим способом використання конвертаційного центру – фіктивна господарська діяльність. Шляхом оформлення фіктивних платіжних доручень, отримання кредитів на діяльність, отримання коштів за державними цільовими програмами підтримки бізнесу здійснюється як розміщення, так і розшарування і інтеграція незаконних доходів.

Наразі, зареєструвати підприємницьку діяльність в Україні можна в режимі онлайн. Додатково до цього, цифровізація зумовила виникнення цілого ряду видів економічної діяльності, пов’язаної з інформаційними технологіями. Наприклад, розробка програмного забезпечення є по суті видом інтелектуальної діяльності, для підтримки якої не потрібно значного статутного капіталу чи основних фондів. Підприємства з орієнтацією на розробку програмного забезпечення підходять для легалізації незаконних доходів, оскільки легко імітувати факт надання послуг чи виконання робіт.

3. Банки. Банківські перекази мають бути під пильним контролем з точки зору протидії легалізації. Через банківські перекази найчастіше відбувається заплутування джерел походження коштів. Значна кількість транзакцій між фізичними особами з подальшим їх переказом чи виведення у готівку, перерахунок за роботи чи послуги фіктивного підприємства, придбання цінних паперів через банки є шляхами легалізації незаконних доходів через банківські установи. Розвиток мобільного банкінгу та фінтех прискорили процес розшарювання доходів, отриманих незаконним шляхом.

4. Віртуальні активи. Останнім часом серед злочинців часто стала використовуватись криптовалюта. Електронні кошти слугують засобом розшарування, оскільки можливість створення багатьох криптогаманців за короткий період часу з мінімальною, на відміну від банку, індентифікацією особи. Здійснення тисяч транзакцій за допомогою сотень криптогаманців розмиває походження коштів і стає складно пов’язати кошти з первинним злочином.

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.

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.

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 1.26. На основі даних рисунку 1.26 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.

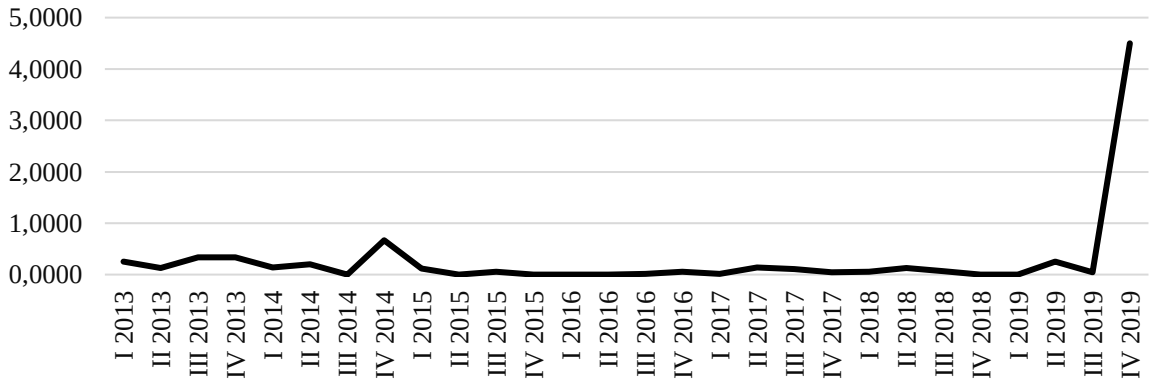


Рисунок 1.26 – Частка направлених до суду обвинувальних актів у загальній кількості кримінальних правопорушень, за якими проводилось досудове розслідування у відповідний період

Джерело: розроблено автором на основі даних Генеральної прокуратури України

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 1.27). 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.

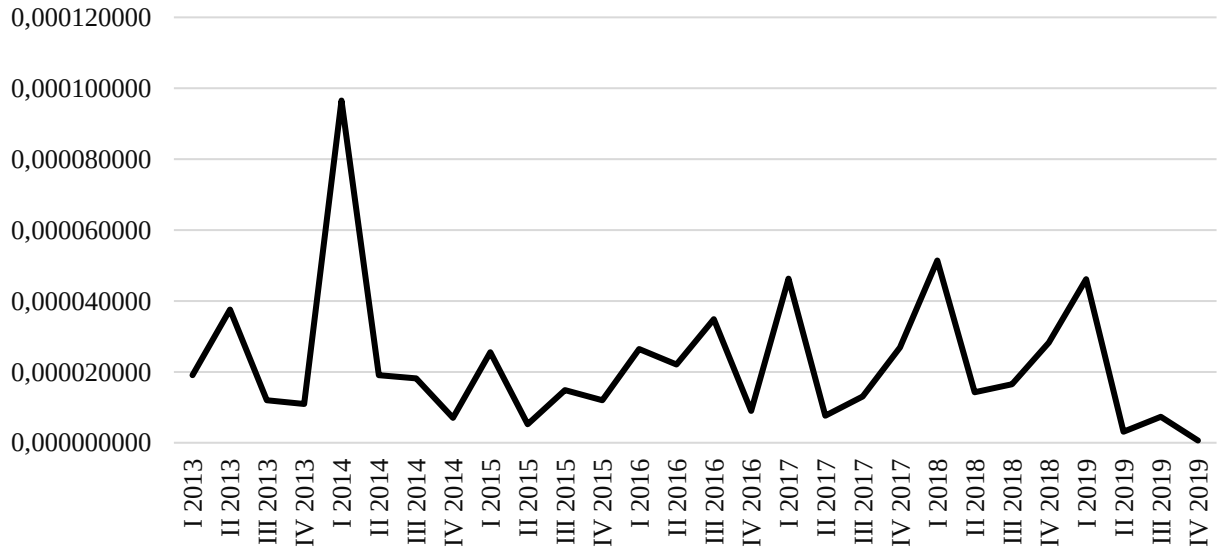


Рисунок 1.27 – Частка кримінальних правопорушень по яких проводилось досудове розслідування, яка припадає на одне повідомлення про операцію, що було передане до Державної служби фінансового моніторингу

Джерело: розроблено автором на основі даних Державної служби статистики України, Державної служби фінансового моніторингу України

Характеристикою другої альтернативи є показник діджиталізації економіки, який є відношенням кількості абонентів мережі інтернет до чисельності населення (рисунок 1.28). 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.

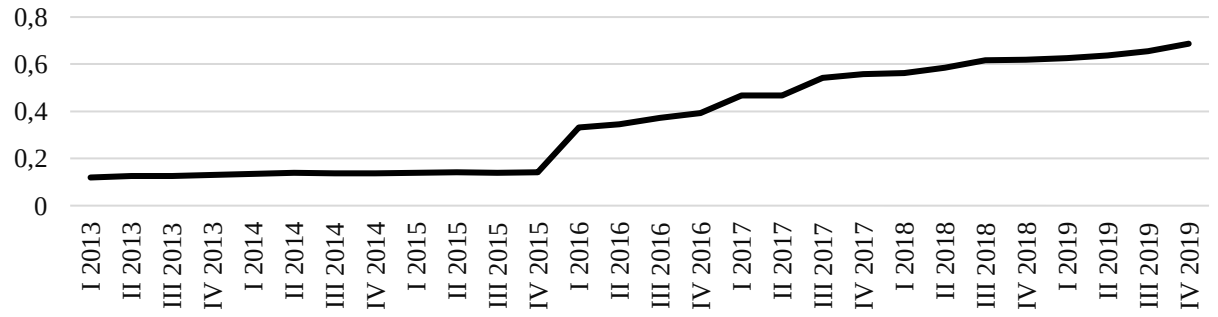


Рисунок 1.28 – Динаміка діджиталізації економіки

Джерело: розроблено автором на основі даних Державної служби статистики України

Для специфікації функції залежності результативної ознаки від факторних, побудуємо корелограму нульових різниць (рисунок 1.29) та таблицю автокореляційної функції (рисунок 1.30).

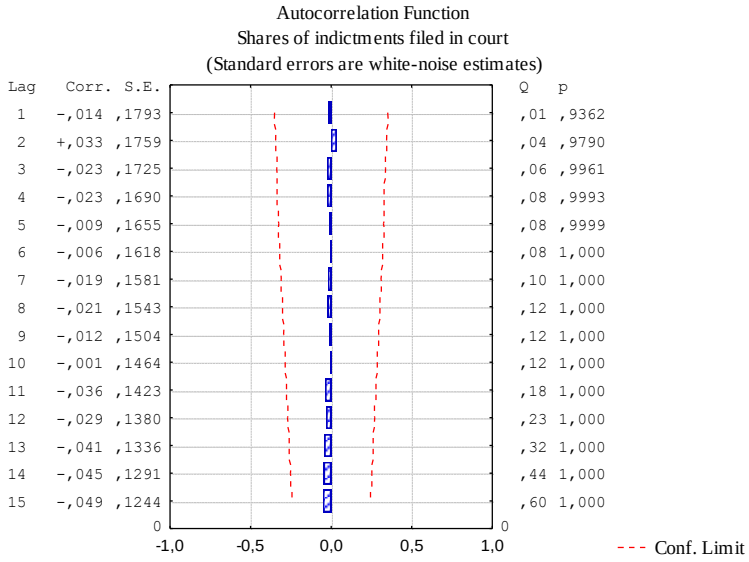


Рисунок 1.29 – Корелограма нульових різниць Частки направлених до суду обвинувальних актів

Джерело: розроблено автором

Autocorrelation Function
Shares of indictments filed in court
(Standard errors are white-noise estimates)

Lag	Auto-Corr.	Std.Err.	Box & Ljung Q	p
1	-0,0143	0,1793	0,0064	0,936242
2	0,0334	0,1759	0,0425	0,978969
3	-0,0231	0,1725	0,0604	0,996121
4	-0,0226	0,1690	0,0783	0,999254
5	-0,0086	0,1655	0,0810	0,999904
6	-0,0060	0,1618	0,0824	0,999989
7	-0,0191	0,1581	0,0969	0,999998
8	-0,0208	0,1543	0,1151	1,000000
9	-0,0122	0,1504	0,1216	1,000000
10	-0,0015	0,1464	0,1217	1,000000
11	-0,0356	0,1423	0,1843	1,000000
12	-0,0290	0,1380	0,2283	1,000000
13	-0,0408	0,1336	0,3215	1,000000
14	-0,0453	0,1291	0,4448	1,000000

Рисунок 1.30 – Значення автокореляційної функції та статистична значущість коефіцієнтів автокореляції нульових різниць Частки направлених до суду обвинувальних актів

Джерело: розроблено автором

Як видно з рисунків 1.29 та 1.30, немає чіткої залежності значень коефіцієнтів автокореляції різних порядків від часового лагу, крім того коефіцієнти актокореляції є статистично незначущими (p-value близьке до 1). Це свідчить про відхилення гіпотези про лінійну залежність частки направлених до суду обвинувальних актів у загальній кількості кримінальних правопорушень, за якими проводилось досудове розслідування, від двох альтернатив: частка кримінальних правопорушень, по яким проводилось досудове розслідування, яка припадає на одне повідомлення про операцію, що було передане до Державної служби фінансового моніторингу; діджиталізація

економіки. Саме тому доцільно обрати у якості функції підгонки – нелінійну функцію впливу факторних ознак на результативну.

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

$$u(x_1, x_2, x_3, \dots, x_n) = \prod_{j=1}^{n} \left(x_j - \varphi_j\right)^{\beta_j} \tag{1.27}$$

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 (1.27) набуває вигляду функції Кобба-Дугласа (формула 1.28).

$$u(x_1, x_2) = \prod_{j=1}^{2} \left(x_j\right)^{\beta_j}, \sum_{j=1}^{2} \beta_j = 1 \tag{1.28}$$

Враховуючи обмеження $\sum_{j=1}^{2} \beta_j = 1$ формули (1.28), для формалізації ефективності системи протидії легалізації кримінальних доходів в умовах діджиталізації банківської діяльності за допомогою побудови функції корисності, пропонується розглянути задачу пошуку значень коефіцієнтів еластичності двох розглянутих альтернатив як задачу нелінійного програмування:

$$\sum_{t=1}^{T}\left(u_t - \prod_{j=1}^{2}(x_{jt})^{\beta_j}\right)^2 \rightarrow min \qquad (1.29)$$

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

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

Т – довжина досліджуваного часового ряду.

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

Таким чином, вирішення нелінійної оптимізаційної задачі (1.29) оцінювання ефективності системи протидії легалізації кримінальних доходів за допомогою функції корисності дозволяє отримати наступні результати при мінімальному значенні суми квадратів відхилень фактичних значень частка направлених до суду обвинувальних актів від їх теоретичних рівнів на рівні 18,28 од.

$$u(x_1, x_2) = {x_1}^{0,0019} \cdot {x_2}^{0,9981} \qquad (1.30)$$

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.

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. Тепер це електронні листи з підробленими посиланнями на пакети державної фінансової допомоги, банків, що розподіляють допомогу тощо.

Отже, на рис. 1.31 представлено дорожню карту реформування системи протидії легалізації доходів, отриманих незаконним шляхом, в умовах діджиталізації економіки та появи нових викликів сучасних світогосподарських відносин.

.

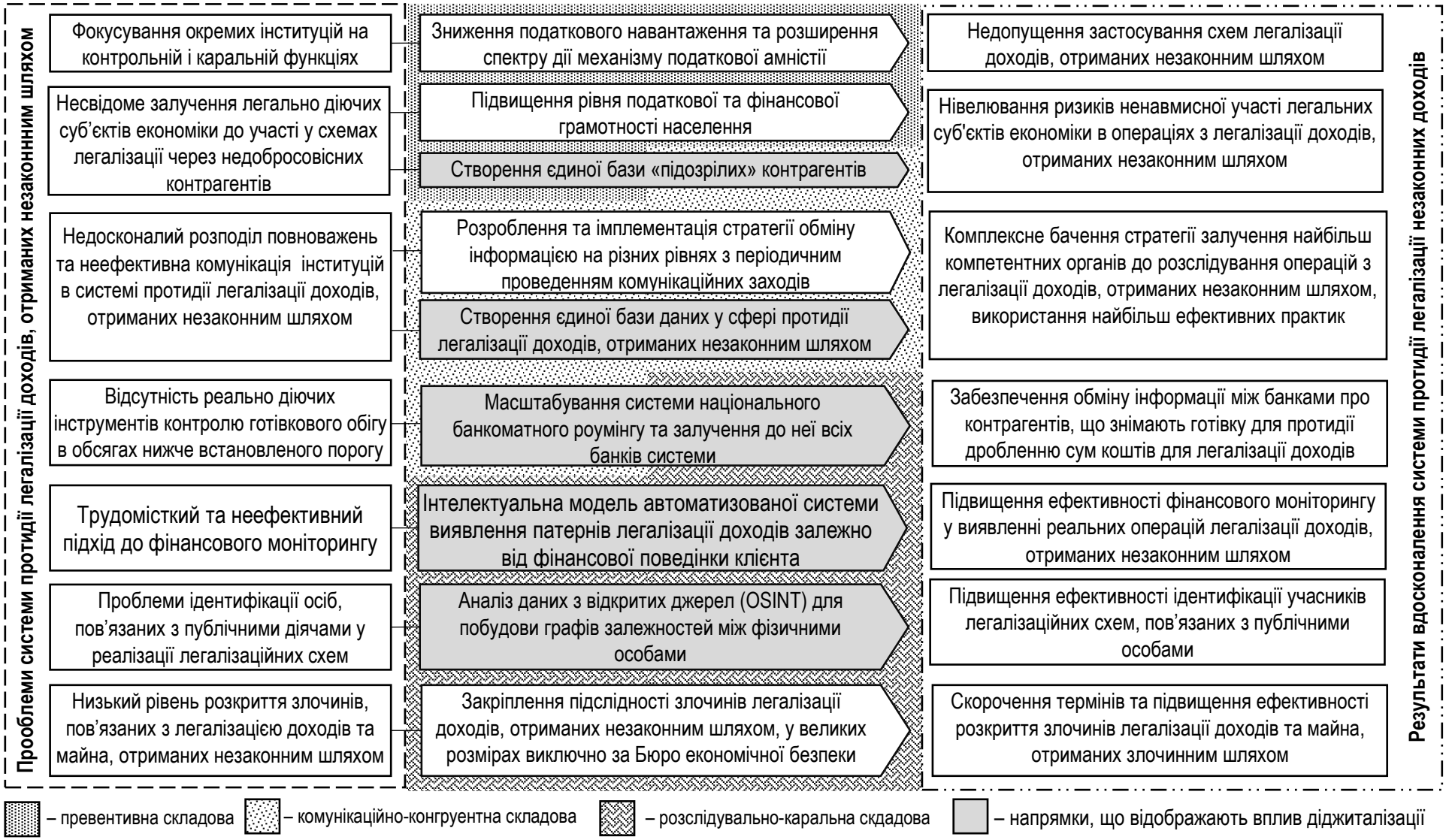


Рисунок 1.31 – Напрямки реформування системи протидії легалізації доходів, отриманих незаконним шляхом, в умовах діджиталізації економіки

Джерело: розроблено автором

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.

1.4. Практика використання due diligence для посилення кіберзахисту

Для фінансово-економічної безпеки та стабільності сучасних суб’єктів господарювання значним ризиком є шахрайства, що можуть статися через відсутність чіткої ясності функціонування організації, неналежну діяльність установи, недоліки інформаційного та технічного забезпечення, фінансові питання. Злочинцям більш доступними стають технічні навички та прогрес технології. Тому стає важче боротися традиційними методиками із тактикою вчинення сучасних кримінальних злочинів. Для перешкоджання шахрайствам, підвищення ефективності господарської діяльності, з метою забезпечення безпечного безперебійного функціонування підприємств, збереження активів, необхідно запроваджувати систему надійного захисту суб’єктів, що основується на застосування різних механізмів та інструментів. При чому, виходячи із специфіки функціонування підприємств, для запобігання шахрайствам на підприємствах, потрібно проводити їх перевірку, таку як: є аудит, оцінка, податкові перевірки, процедура due diligence (Dotsenko & Berezhna, 2023) .

Надійність суб’єктів господарювання в першу чергу визначається його фінансовою безпекою. А в умовах цифровізації економіки, що зростає швидкими темпами, визначальною у діяльності підприємств протягом останніх років, постає система фінансового кіберзахисту. І для протидії фінансовим кібершахрайствам, як однієї з новітніх методик, пропонується застосування інструменту Due diligence. Це сприятиме підвищенню фінансового кіберзахисту підприємства, що забезпечить полегшення досягнення стратегічних цілей, підвищення вартості бізнесу, розширення конкурентних переваг.

Так, в сучасних цифровізованих умовах функціонування суб'єктів господарювання, особливої актуальності набуває удосконалення системи фінансового захисту, в тому числі через застосування такої процедури перевірки як Due diligence, що є особливо ефективною в аспекті протидії фінансовим кібершахрайствам.

Метою дослідження є вивчення та поглиблення теоретичних аспектів Due diligence суб'єктів господарювання в аспекті протидії фінансовому кібершахрайству, виявлення основних чинників та розробка структурно-логічної економіко-математичної моделі Due diligence суб'єктів господарювання в аспекті протидії фінансовому кібершахрайств.

Поняття due diligence є відносно новою категорією, що набуває активного використання серед сучасних науковців світу. Дискусії навколо теоретичне та практичне вивчення цього питання приведені у роботах таких вчених, як: Elbel et al. (2023) щодо впливу та наслідків Закону Європейського Союзу про Due diligence на діяльність дрібних підприємств; Deva S. (2023), Villiers (2022), Liesa C. R. F. (2022), Sedano T. G. (2022) стосовно дискусій законодавчо-правових питань Due diligence; Litwin D. (2023) стосовно Due diligence економічної нерівності, впливу бізнесу на нерівність; Guanipa H. J., Chimá J. T. (2023), Camoletto,S., Corazza L., Pizzi S., Santini E. (2022) про корпоративну due diligence, в тому числі корпоративну відповідальність; та ін.

Проаналізувавши літературні надбання з досліджуваного питання, було сформульовано поняття Due Diligence (належна перевірка, експертиза) – як наукової категорії, що передбачає проведення сукупності дій: різновекторне дослідження та оцінка роботи суб'єкта, з глибоким вивченням фінансового стану, оцінкою ризиків (в тому числі фінансових, інвестиційних), аналіз місця об'єкта на ринку, з особливим акцентом на питання, пов'язані з безпекою, правами людини та навколишнього середовища – для формування комплексного висновку щодо фінансового, юридичного, інвестиційного стану суб'єкта дослідження, наявних ризиків. Due Diligence включає наступні етапи: пошук та збір даних, вивчення, консолідація та аналіз даних, формування висновку щодо стану підприємства з досліджуваного питання, прийняття відповідного рішення (Dotsenko et al., 2023).

Нормативною основою Due diligence є Пропозиція для Директиви Європейського Парламенту та Ради щодо належної перевірки корпоративного сталого розвитку від 23.02.2022р. Законодавчий акт Європейського Союзу про Due diligence направлений на досягнення цілей сталого розвитку ООН, зокрема напрямків, пов'язаних з правами людини та навколишнього середовища, безпекою, пом'якшення негативних впливів на них. Це дозволить формувати ефективні бізнес-рішення для захисту організацій, забезпечення довгострокової стійкості підприємств.

Due Diligence переважно містить перевірку відповідності, під час якої всебічно розглядаються операційна діяльність, взаємини з контрагентами й державними органами, можливі несприятливі чинники діяльності підприємства

тощо.Залежно від потреб процедури Due Diligence виділяють його наступні види (таблиця 1.13).

Таблиця 1.13 – Види Due Diligence

№	Назва	Опис
1	Загальний Due Diligence	всеосяжна перевірка основних аспектів діяльності компанії, зокрема фінансовий стан, оподаткування, юридичні аспекти, менеджмент, частка компанії на ринку тощо
2	Фінансовий Due Diligence	перевірка фінансового стану компанії, зокрема активів і зобов'язань з погляду їхньої оцінки (наявність позабалансових зобов'язань, знецінення запасів тощо)
3	Податковий Due Diligence	виявлення податкових ризиків і об'єктивна оцінка всіх податкових аспектів ведення бізнесу.
4	Правовий Due Diligence	аналіз юридичних аспектів роботи компанії, наприклад, реєстрація інтелектуальних прав власності, судові справи тощо.
5	Vendor Due Diligence	замовником якого є сама компанія або її поточний власник.
6	Операційний Due Diligence	перевірка операційної діяльності, зокрема, рівень завантаження виробничих потужностей, можливість зміни асортименту й збільшення виробництва.
7	Технологічний Due Diligence	вивчення технології виробництва, стану устаткування.

Due Diligence в тому числі дозволяє визначити та сформувати розуміння стану фінансової захисту досліджуваного суб'єкта, зокрема його фінансової кібербезпеки, для забезпечення заходів протидії фінансовим злочинам, фінансовим кібершахрайствам. Для реалізації Due diligence підприємств в аспекті протидії фінансовим кібершахрайствам доцільно визначити ряд етапів і особливостей щодо його реалізації. На рисунок 1.32 зображено побудовану в ході дослідження структурно-логічну схему етапів і особливостей реалізації Due diligence підприємств. Схема побудована за допомогою ПЗ Bizagi Modeler.

Впровадження комплексної методики Due diligence в аспекті протидії фінансовим кібершахрайствам сприятиме забезпеченню наступних переваг для підприємств: удосконалення корпоративного управління; покращення нормативної бази корпоративного менеджменту; формування ефективних бізнес-рішень; забезпечення довгострокової стійкості та стабільності; формування стійкості у ланцюгах безперервної діяльності до раптових загроз; отримання конкурентних переваг; уникнення небажаних репутаційних ризиків; зменшення ризиків створення вартості; пом'якшення ризиків; скорочення збитків від бізнес-діяльності; посилення корпоративної відповідальності за несприятливі наслідки ведення бізнесу; формування узгодженості серед підприємств щодо зобов'язань по нормам діяльності підприємств; забезпечення кращого правового захисту для постраждалих від функціонування підприємств; покращення політики безпеки підприємств.

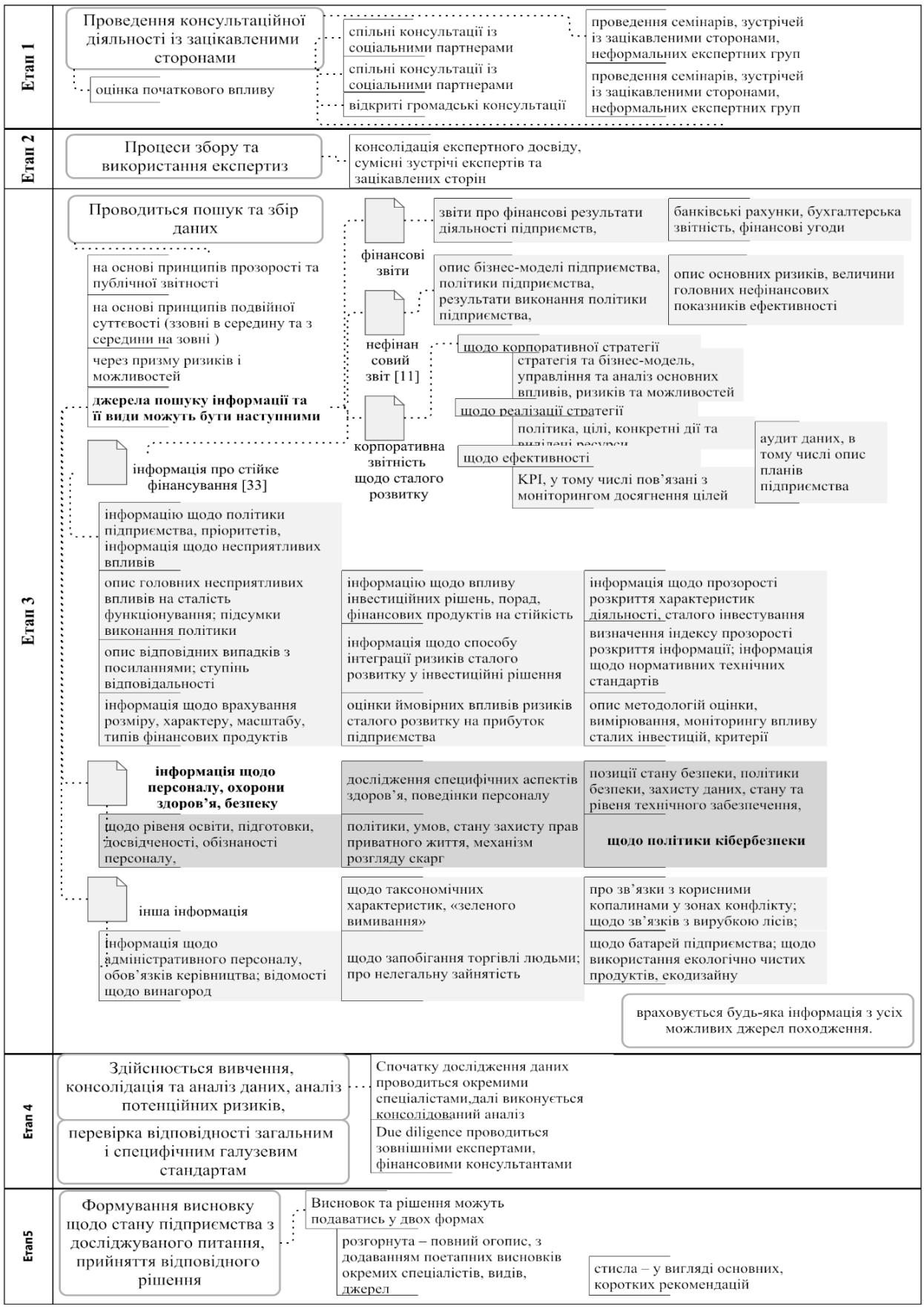


Рисунок 1.32 – Структурно-логічна схему етапів і особливостей реалізації Due diligence суб'єктів господарювання

У межах даного дослідження запропоновано оцінити рівень протидії фінансовим кібершахрайствам на основі аналізу релевантних показників у розрізі різних країн світу. Для дослідження даного питання використано комплекс методів економетричного моделювання, а саме кластерний аналіз, дисперсійний аналіз та регресійний аналіз. Реалізація даного завдання здійснено у межах чотирьох етапів.

На першому етапі дослідження відбувається збір статистичної бази дослідження, що характеризує стан протидії фінансовим кібершахрайствам; відбір по країнах Світу факторів, що впливають на стан кібербезпеки. Інформаційна база дослідження побудована на основі показників The World Bank, Global Digital Convergence, Digital Development Dashboard, NCSI. Індикатори оцінювання було обрано за 2021 рік for 68 країнам Світу.

До факторних показників, що визначають стан протидії фінансовим кібершахрайствам віднесено наступні 32 показника: Digital Development Level (C1), Basel AML Index(C2), Assessment of the ease of doing business(C3), Assessment of the ease of obtaining electricity(C4), Human Development Index(C5), Index Distribution of human rights(C6), Secure Internet servers (C7), Business extent of disclosure index (0=less disclosure to 10=more disclosure) (C8), Research and development expenditure (% of GDP) (C9), Firms competing against unregistered firms (% of firms) (C10), Firms using banks to finance working capital (% of firms) (C11) , Firms that spend on R&D (% of firms) (C12), Losses due to theft and vandalism (% of annual sales of affected firms) (C13), Firms offering formal training (% of firms) (C14), Firms experiencing losses due to theft and vandalism (% of firms) (C15), Informal payments to public officials (% of firms) (C16), Firms using banks to finance investment (% of firms) (C17), Value lost due to electrical outages (% of sales for affected firms) (C18), Fixed broadband subscriptions: >10 Mbit/s, Individuals using the Internet, total (%) (C19), Active mobile-broadband subscriptions per 100 inhabitants (C20), Fixed broadband basket as a % of GNI p.c. (C21), Fixed broadband subscriptions per 100 inhabitants (C22), Fixed-telephone subscriptions per 100 inhabitants (C23), Mobile broadband basket as a % of GNI p.c. (C24), Mobile cellular basket as a % of GNI p.c. (C25), Mobile data and voice basket (high consumption) as a % of GNI p.c. (C26), Mobile data and voice basket (low consumption) as a % of GNI p.c. (C27), Mobile-cellular subscriptions per 100 inhabitants (C28), Population covered by a mobile-cellular network (%) (C29), Population covered by at least a 3G mobile network (%) (C30), Total fixed broadband subscriptions(C31). Результативним показником рівень кібербезпеки взято National Cyber Security Index. Фрагмент сформованих вхідних даних подано у таблиці 1.14.

На другому етапі було проведено кластерний аналіз – групування країн Світу на кластери з використання інструментарію програми Statistica 10 та Statistica Portable. Кластеризація країн ґрунтується на застосуванні ітеративного дівізівного методу k-середніх (k-means clustering).

Таблиця 1.14 – Фрагмент кількісної формалізації статистичної бази дослідження

Country	C0	C1	C2	…	C30	C31	C32
Albania	62,3400	48,7400	5,7200	…	99,8600	99,2000	559394,0000
Austria	68,8300	75,7600	4,4200	…	99,0000	98,0000	2592000,0000
Belarus	53,2500	62,3300	5,0400	…	99,9000	99,9000	3238881,0000
Belgium	94,8100	74,0700	3,9400	…	100,0000	100,0000	4920679,0000
Botswana	29,8700	41,9600	4,8700	…	98,0000	98,0000	203020,0000
…	…	…	…	…	…	…	…
Thailand	64,9400	56,6300	6,1500	…	98,8000	98,8000	12420940,0000
Trinidad and Tobago	33,7700	52,6000	4,8500	…	100,0000	100,0000	370887,0000
Tunisia	53,2500	46,2600	5,2000	…	99,0000	99,0000	1496897,0000
Türkiye	54,5500	58,2900	5,7000	…	99,7500	98,8100	18135736,0000
Ukraine	75,3200	55,9600	5,2100	…	99,9000	91,6000	7566286,0000
Uruguay	59,7400	63,8600	3,9800	…	92,7000	92,7000	1105458,0000
Uzbekistan	36,3600	49,0000	5,2000	…	99,4000	95,0000	7497459,0000
Zambia	55,8400	29,6600	6,0300	…	97,1000	95,5000	80592,0000
Zimbabwe	15,5800	28,9700	6,7900	…	93,5400	84,3100	205333,0000

Джерело: розроблено авторами

На основі сформованої вхідної бази з 32 показників за 2021 рік по 68 країнам світу, з урахуванням дисперсійного аналізу, було виконано групування країн світу на 2 – 12 кластерів; доведено доцільність групування країн світу на 9 кластерів.

Так, було визначено 9 окремі кластери (рисунок 1.32), що містять групування країн світу згідно обраних ключових показників у графічному вигляді, із зазначенням кількості країн-членів кожного кластеру, евклідових відстаней від центру групування як визначальний показник даного типу групування країн світу.

Members of Cluster Number 3 (SpreadsheeBerezhna_clast_t.sta) and Distances from Respective Cluster Center
Cluster contains 7 cases

	Distance
Colombia	441835,9
Egypt	432249,6
Indonesia	494527,2
Netherlands	547481,5
Poland	354955,5
Thailand	742940,1
Ukraine	434756,8

Рисунок 1.32 – Склад та характеристика 3-го із 9 умовних кластерів країн світу в розрізі рівня кібербезпеки та стану протидії фінансовому кібершахрайству згідно показника евклідових відстаней

Джерело: розроблено авторами

Аналіз сформованих кластерів країн Світу дозволяє стверджувати, що групування цілком відповідає загальному рівня кібербезпеки та стану протидії фінансовому кібершахрайству в країнах з одного кластеру. Так, виокремлено для подальшого аналізу кластер країн, що містить Україну, який обрано для дослідження у роботі. Тобто, цей кластер включає Colombia, Egypt, Indonesia, Netherlands, Poland, Thailand, Ukraine – країни для яких характерні спільні риси кібербезпеки та стану протидії фінансовому кібершахрайству.

Більш комплексно описати результати кластерного аналізу дозволяє аналіз показників за допомогою стандартизованих середніх значень (рисунок 1.33) та евклідових відстаней (рисунок 1.34).

	Cluster Means (SpreadsheeBerezhna_clast_t.sta)								
Variable	Cluster No. 1	Cluster No. 2	Cluster No. 3	Cluster No. 4	Cluster No. 5	Cluster No. 6	Cluster No. 7	Cluster No. 8	Cluster No. 9
C0	65	52	66	78	65	55	47,7	42,4	28,1
C1	63	62	58	66	61	53	51,0	53,1	28,7
C2	5	7	5	4	5	5	5,5	5,7	6,6
C3	85	95	81	85	79	82	74,9	72,3	51,3
C4	85	95	81	85	79	82	74,9	72,3	51,3
C5	1	1	1	1	1	1	0,8	0,8	0,5
C6	1	0	1	1	1	1	0,7	0,8	0,7
C7	2476546	1962997	758071	352332	471909	21965	22386,0	14255,4	1930,6
C8	7	10	9	7	7	6	5,6	5,6	6,2
C9	1	3	1	2	2	1	0,6	0,4	0,2
C10	28	58	43	29	37	52	43,3	50,2	65,2
C11	37	22	32	33	35	34	26,2	39,2	25,5
C12	15	39	11	16	18	15	6,9	12,8	10,7
C13	3	1	3	3	4	4	3,6	4,6	6,8
C14	29	79	27	38	36	34	24,7	41,9	28,9
C15	16	4	11	19	13	16	9,7	19,6	26,7
C16	21	11	13	6	12	3	15,7	16,4	38,1
C17	36	15	30	31	33	28	23,2	30,3	25,4
C18	2	1	1	1	5	1	1,5	2,5	10,6
C19	21033710	531874700	8754531	3851565	1863386	1033674	543886,9	281473,3	15436,5
C20	82	73	78	86	80	78	72,7	75,9	35,1
C21	92	102	112	103	103	97	81,5	85,1	44,8
C22	2	1	3	2	3	5	5,4	6,1	43,9
C23	29	38	19	33	23	20	15,4	20,8	1,3
C24	26	13	12	26	17	17	15,1	20,9	0,9
C25	1	1	1	1	1	1	1,9	2,4	10,6
C26	1	0	1	1	1	1	1,1	1,9	7,4
C27	1	1	2	1	2	2	2,8	5,3	15,8
C28	1	1	1	1	1	1	1,8	3,1	8,7
C29	120	122	134	119	127	132	108,5	120,3	89,4
C30	99	100	99	100	98	98	98,8	96,9	92,6
C31	99	100	98	98	96	98	98,2	90,9	83,4
C32	22323550	535786600	9710106	4529849	2376303	987899	756578,0	375129,1	101240,5

Рисунок 1.33 – Середні значення показників рівня кібербезпеки та стану протидії фінансовому кібершахрайству в межах 9 кластерів

Джерело: розроблено авторами

Чим менше значення евклідової відстані, тим країни в даному кластері більш схожі за рівенем кібербезпеки та станом протидії фінансовому кібершахрайству.

Cluster Number	Euclidean Distances between Clusters (SpreadsheeBerezhna_clast_t.sta) Distances below diagonal Squared distances above diagonal								
	No. 1	No. 2	No. 3	No. 4	No. 5	No. 6	No. 7	No. 8	No. 9
No. 1	0	1,589706E+16	9,479705E+12	1,867740E+13	2,331553E+13	2,609807E+13	2,699969E+13	2,783185E+13	2,853704E+13
No. 2	126083600	0,000000E-01	1,667917E+16	1,700136E+16	1,713457E+16	1,720623E+16	1,722950E+16	1,725032E+16	1,726779E+16
No. 3	3078913	1,291479E+08	0,000000E-01	1,546629E+12	3,071346E+12	4,128194E+12	4,488533E+12	4,832963E+12	5,129510E+12
No. 4	4321735	1,303892E+08	1,243636E+06	0,000000E-01	2,607549E+11	6,240928E+11	7,662778E+11	9,127741E+11	1,043977E+12
No. 5	4828616	1,308991E+08	1,752526E+06	5,106417E+05	0,000000E-01	8,541027E+10	1,383836E+11	2,035331E+11	2,670214E+11
No. 6	5108627	1,311725E+08	2,031796E+06	7,899954E+05	2,922503E+05	0,000000E-01	8,890928E+09	2,852581E+10	5,525368E+10
No. 7	5196123	1,312612E+08	2,118616E+06	8,753730E+05	3,719994E+05	9,429172E+04	0,000000E-01	6,497887E+09	2,148926E+10
No. 8	5275591	1,313405E+08	2,198400E+06	9,553921E+05	4,511464E+05	1,688958E+05	8,060947E+04	0,000000E-01	4,422498E+09
No. 9	5342008	1,314070E+08	2,264842E+06	1,021752E+06	5,167411E+05	2,350610E+05	1,465921E+05	6,650187E+04	0,000000E-01

Рисунок 1.34 – Евклідові відстані між 9 кластерами

Джерело: розроблено авторами

Адекватність моделі перевірено на етапі 2 (кластерний аналіз) за допомогою дисперсійного аналізу. Доведено доцільність групування країн Світу за станом протидії фінансовому кібершахрайству та рінем кібербезпеки на 9 кластерів з урахуванням значення внутрішньогрупової та міжгрупової дисперсій ознак, параметрів F (критерій Фішера), параметрів p (імовірність відхилення гіпотези про недоцільність проведення певного групування). Так, були розглянуті послідовно результати групування від 2 до 12 кластерів.

За результатами дисперсійного аналізу спостерігаємо покращення показників адекватності при переході до 9 груп з подальшим їх погіршенням при кластеризації від 10 груп. Це пояснюється тим, що при виділенні від 2 до 8 кластерів в розрізі більшості вхідних показників спостерігаються наступні значення показників адекватності: відмінне від нульового значення міжгрупової дисперсії (що суперечить вимозі мінімізації даної дисперсії); в розрізі міжгрупової дисперсії спостерігаються в більшості випадків близькі до нульового значення; низькі значення критерію Фішера; значення p більші за 0,05 в розрізі ряду показників. Це свідчить про недоцільність проведення групування на 2 – 8 кластерів.

Ситуація значно покращується при переході на 9 кластерів (рисунок 1.35). Значення міжгрупової дисперсії в цілому збільшуються, внутрішньогрупової зменшуються, а статистично значущими виступають більшість вхідних показників (23 із 33 показників – значення p для яких прямують до допустимого рівня менше 0,05, а 10 статистично не значущі: C1, C8, C11, C12, C13, C14, C15, C16, C17, C31).

	Analysis of Variance (SpreadsheeBerezhna_clast_t.sta)					
Variable	Between SS	df	Within SS	df	F	signif. p
C0	1,524654E+04	8	2,269475E+04	59	4,955	0,000102
C1	7,809341E+03	8	9,885562E+03	59	5,826	0,000018
C2	3,094147E+01	8	5,735105E+01	59	3,979	0,000801
C3	7,134303E+03	8	7,775247E+03	59	6,767	0,000003
C4	7,134303E+03	8	7,775247E+03	59	6,767	0,000003
C5	5,845594E-01	8	6,596292E-01	59	6,536	0,000004
C6	6,455577E-01	8	2,742421E+00	59	1,736	0,108903
C7	3,373626E+13	8	9,425740E+13	59	2,640	0,015221
C8	7,848264E+01	8	3,136927E+02	59	1,845	0,086502
C9	2,279906E+01	8	5,870506E+01	59	2,864	0,009246
C10	8,750300E+03	8	2,226524E+04	59	2,898	0,008570
C11	1,506828E+03	8	1,244834E+04	59	0,893	0,528412
C12	1,398658E+03	8	6,815490E+03	59	1,513	0,172106
C13	1,089695E+02	8	7,119233E+02	59	1,129	0,357762
C14	4,195098E+03	8	1,850678E+04	59	1,672	0,124527
C15	1,853194E+03	8	6,759950E+03	59	2,022	0,059213
C16	6,100735E+03	8	2,286789E+04	59	1,968	0,066574
C17	1,148288E+03	8	1,595149E+04	59	0,531	0,828533
C18	6,337980E+02	8	2,081157E+03	59	2,246	0,036319
C19	2,770574E+17	8	2,909506E+14	59	7022,837	0,000000
C20	1,458598E+04	8	1,449012E+04	59	7,424	0,000001
C21	2,466829E+04	8	4,567978E+04	59	3,983	0,000794
C22	1,158186E+04	8	1,963262E+04	59	4,351	0,000361
C23	5,251958E+03	8	8,636795E+03	59	4,485	0,000272
C24	3,765020E+03	8	1,154849E+04	59	2,404	0,025625
C25	6,424162E+02	8	6,297721E+02	59	7,523	0,000001
C26	2,968103E+02	8	3,259851E+02	59	6,715	0,000003
C27	1,401115E+03	8	1,248847E+03	59	8,274	0,000000
C28	4,109352E+02	8	2,922943E+02	59	10,368	0,000000
C29	1,114735E+04	8	3,332745E+04	59	2,467	0,022323
C30	2,985987E+02	8	9,115524E+02	59	2,416	0,024985
C31	1,658097E+03	8	6,534629E+03	59	1,871	0,081812
C32	2,809651E+17	8	3,303997E+14	59	6271,549	0,000000

Рисунок 1.35 – Аналіз адекватності кластеризації країн світу на 9 груп станом на 2021 рік

Джерело: розроблено авторами

При здійсненні переходу з 10, а далі 11 – 12 кластерів, показники адекватності групування за результатами дисперсійного аналізу знову погіршуються. Спостерігаємо, що імовірність відхилення гіпотези про недоцільність даного групування більше допустимогг рівня 0,05 по більшості вхідних показників. Так, можна зробити висновок про доцільність проведення групування країн країн світу за станом протидії фінансовому кібершахрайству та рінем кібербезпеки на 9 кластерів.

Третій етап передбачає визначення релевантних факторів, що визначають стан протидії фінансовому кібершахрайству, що впливають на рівень кібербезпеки, на основі методик Sigma-restricted parameterization та кореляційного аналізу.

Перший кроком третього етапу – виконання Univariate Tests of Significance факторів, що визначають стан протидії фінансовому кібершахрайству на рівень кібербезпеки (рисунок 1.36).

Effect	Univariate Tests of Significance for C0 (SpreadsheetBerezhna_fact_.sta) Sigma-restricted parameterization Effective hypothesis decomposition				
	SS	Degr. of Freedom	MS	F	p
Intercept		0			
"C1"	56,336	1	56,336	0,376945	0,543104
"C2"	1139,066	1	1139,066	7,621539	0,009018
"C3"		0			
"C4"		0			
"C5"	214,445	1	214,445	1,434861	0,238800
"C6"	71,479	1	71,479	0,478266	0,493645
"C7"	491,995	1	491,995	3,291958	0,077961
"C8"	490,038	1	490,038	3,278863	0,078530
"C9"	0,243	1	0,243	0,001628	0,968042
"C10"	1,893	1	1,893	0,012668	0,911011
"C11"	87,536	1	87,536	0,585705	0,449073
"C12"	92,548	1	92,548	0,619241	0,436480
"C13"	63,793	1	63,793	0,426841	0,517694
"C14"	17,607	1	17,607	0,117809	0,733420
"C15"	258,234	1	258,234	1,727855	0,196999
"C16"	525,043	1	525,043	3,513086	0,069019
"C17"	34,895	1	34,895	0,233487	0,631876
"C18"	532,797	1	532,797	3,564967	0,067091
"C19"	745,291	1	745,291	4,986770	0,031849
"C20"	108,768	1	108,768	0,727770	0,399248
"C21"	198,042	1	198,042	1,325109	0,257266
"C22"	76,573	1	76,573	0,512354	0,478739
"C23"	377,211	1	377,211	2,523933	0,120876
"C24"	57,480	1	57,480	0,384603	0,539056
"C25"	220,967	1	220,967	1,478502	0,231922
"C26"	87,723	1	87,723	0,586959	0,448592
"C27"	217,141	1	217,141	1,452902	0,235926
"C28"	30,972	1	30,972	0,207237	0,651676
"C29"	270,966	1	270,966	1,813043	0,186561
"C30"	2,950	1	2,950	0,019741	0,889045
"C31"	212,796	1	212,796	1,423827	0,240579
"C32"	743,323	1	743,323	4,973603	0,032062
Error	5380,330	36	149,454		

Рисунок 1.36 – Univariate Tests of Significance впливу факторів стану протидії фінансовому кібершахрайству на рівня кібербезпеки для країн світу

Джерело: розроблено авторами

За даними рисунку 1.36, що відображують результати Univariate Tests of Significance впливу факторів, що визначають стан протидії фінансовому кібершахрайству на рівень кібербезпеки, виділено 3 статистично значущих фактори: C2, C19, C32. Так як по цим факторам розрахункові рівні значущості критерія Фішера відповідає вимозі – менше критично допустимого p=0,05 (для C2 – p=0,00901, C19 – p=0,03184, C32 – p=0,03206); найбільші рівні сум квадратів відхилень (SS): для C2 - SS=1139,06, C19 - SS=745,29, C32 - SS=743,32. Для інших показників вклад факторів є статистично незначущими.

Другий крок третього етапу (також підтвердження статистичної значущості 3 показників, що визначають стан протидії фінансовому кібершахрайству, що впливають на рівень кібербезпеки) – побудова Pareto Chart of t-Values значущості впливу факторів, що визначають стан протидії фінансовому кібершахрайству на рівень кібербезпеки (рисунок 1.37). Діаграма Парето наглядно допомагає графічно візуалізувати 80% впливових факторів і 20% невпливових факторів.

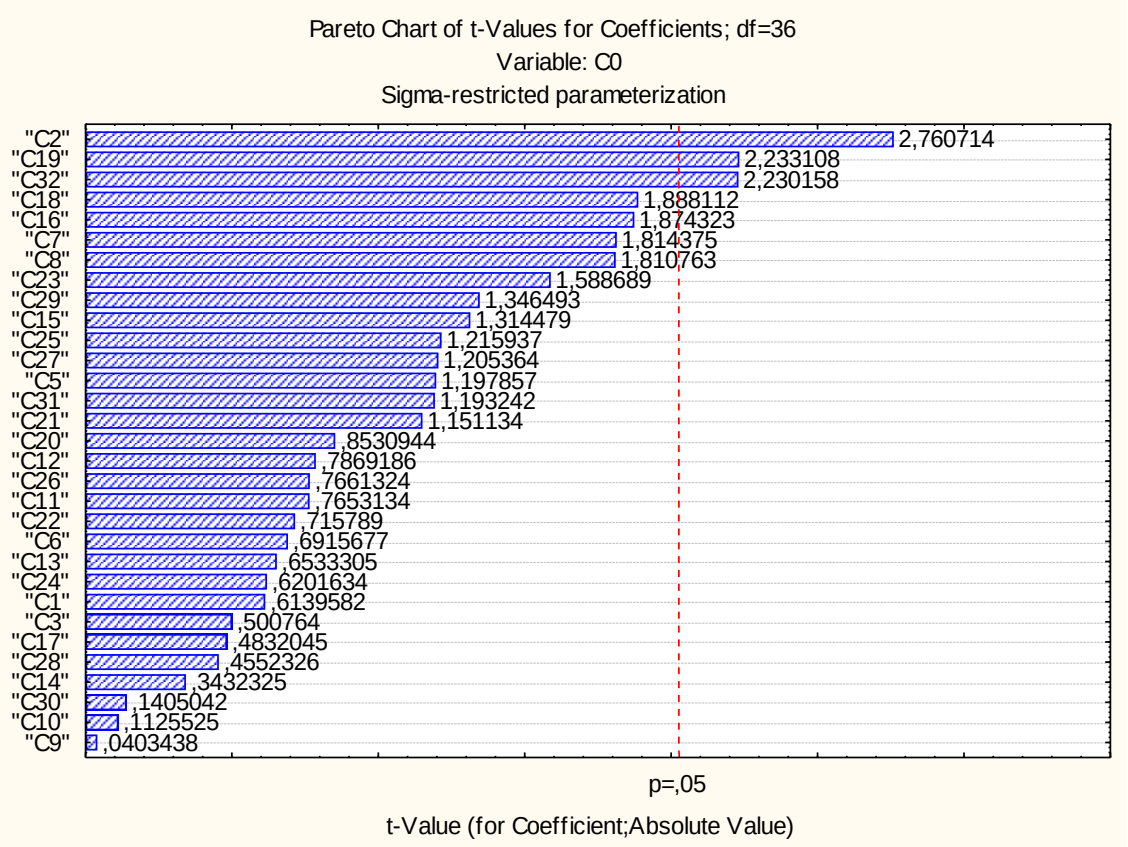


Рисунок 1.37 – Pareto Chart of t-Values значущості впливу факторів, що визначають стан протидії фінансовому кібершахрайству на рівень кібербезпеки для країн світу

Джерело: розроблено авторами

На рисунку 1.37 видно 3 смуги показників С2, С19, С32, що перетинають червону лінію (межу критично допустимого рівня критерія Фішера (р) 0,05 і означає їх статистичну значущість. Тобто показники С2, С19, С32 оказують 80% впливу, тому є релевантними факторами, що визначають стан протидії фінансовому кібершахрайству, що пропонується використовувати в подальшому дослідженні. Додатково, Діаграма Парето допомагає ранжуватм показники від найвпливовішого до показника з найменш впливового.

Третій крок етапу 3 – проведення кореляційного аналізу. Побудовано кореляційну матрицю взаємозалежності релевантних факторів, що визначають стан протидії фінансовому кібершахрайству та рівня кібербезпеки (рисунок 1.38).

	Correlations (SpreadsheetBerezhna_fact_.sta) Marked correlations are significant at p < ,05000 N=68 (Casew ise deletion of missing data)																
Variable	Means	Std.Dev.	C0	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11	C12	C13	C1
C0	56	24	1,000000	0,801126	-0,771716	0,585713	0,585713	0,796090	0,467135	0,340057	0,147929	0,604925	-0,517743	0,195612	0,191042	-0,341661	0,28
C1	55	16	0,801126	1,000000	-0,783286	0,709013	0,709013	0,957958	0,450732	0,380607	0,023103	0,714319	-0,666174	0,297407	0,350532	-0,579170	0,39
C2	5	1	-0,771716	-0,783286	1,000000	-0,553360	-0,553360	-0,804005	-0,584857	-0,235624	-0,010836	-0,564402	0,437779	-0,383877	-0,321935	0,409463	-0,36
C3	76	15	0,585713	0,709013	-0,553360	1,000000	1,000000	0,701095	0,111944	0,304040	0,114276	0,436701	-0,444307	0,153868	0,230781	-0,318907	0,21
C4	76	15	0,585713	0,709013	-0,553360	1,000000	1,000000	0,701095	0,111944	0,304040	0,114276	0,436701	-0,444307	0,153868	0,230781	-0,318907	0,21
C5	1	0	0,796090	0,957958	-0,804005	0,701095	0,701095	1,000000	0,461170	0,313220	0,051363	0,620939	-0,643240	0,321879	0,283080	-0,566853	0,36
C6	1	0	0,467135	0,450732	-0,584857	0,111944	0,111944	0,461170	1,000000	0,149355	-0,219884	0,267783	-0,160844	0,391259	0,240935	-0,168503	0,32
C7	469049	1382155	0,340057	0,380607	-0,235624	0,304040	0,304040	0,313220	0,149355	1,000000	-0,065597	0,415155	-0,272508	0,042103	0,227533	-0,189624	0,14
C8	7	2	0,147929	0,023103	-0,010836	0,114276	0,114276	0,051363	-0,219884	-0,065597	1,000000	0,003516	-0,012038	-0,031038	-0,061017	0,105408	-0,07
C9	1	1	0,604925	0,714319	-0,564402	0,436701	0,436701	0,620939	0,267783	0,415155	0,003516	1,000000	-0,548625	0,086136	0,279031	-0,418915	0,23
C10	44	22	-0,517743	-0,666174	0,437779	-0,444307	-0,444307	-0,643240	-0,160844	-0,272508	-0,012038	-0,548625	1,000000	0,022680	-0,085296	0,335618	-0,02
C11	33	14	0,195612	0,297407	-0,383877	0,153868	0,153868	0,321879	0,391259	0,042103	-0,031038	0,086136	0,022680	1,000000	0,302410	-0,220883	0,35
C12	14	11	0,191042	0,350532	-0,321935	0,230781	0,230781	0,283080	0,240935	0,227533	-0,061017	0,279031	-0,085296	0,302410	1,000000	-0,263424	0,58
C13	4	4	-0,341661	-0,579170	0,409463	-0,318907	-0,318907	-0,566853	-0,168503	-0,189624	0,105408	-0,418915	0,335618	-0,220883	-0,263424	1,000000	-0,36
C14	34	18	0,288074	0,394845	-0,366817	0,210776	0,210776	0,360489	0,324393	0,142942	-0,072323	0,230034	-0,024800	0,353010	0,584606	-0,365012	1,00
C15	16	11	-0,161776	-0,122572	-0,086275	-0,230426	-0,230426	-0,122920	0,235785	-0,010317	-0,098497	-0,095692	0,209401	0,146696	0,387948	-0,025594	0,31
C16	16	21	-0,314831	-0,563724	0,534749	-0,398680	-0,398680	-0,568055	-0,338481	-0,143863	-0,050451	-0,350248	0,405019	-0,245619	-0,171199	0,382081	-0,21
C17	30	16	0,080848	0,123396	-0,251891	0,027794	0,027794	0,142161	0,292111	0,007551	0,045493	0,035248	0,061284	0,757754	0,070062	-0,116709	0,17
C18	3	6	-0,304555	-0,564376	0,407795	-0,453002	-0,453002	-0,599534	-0,281121	-0,141692	-0,026202	-0,300498	0,326499	-0,304778	-0,039237	0,453818	-0,08
C19	11639349	64339166	0,007697	0,085831	0,137326	0,190596	0,190596	0,025452	-0,309716	0,198477	0,176047	0,197753	0,049629	-0,086605	0,280226	-0,136733	0,29
C20	74	21	0,680418	0,861398	-0,683670	0,676702	0,676702	0,876839	0,376811	0,224853	0,099032	0,485513	-0,567403	0,407923	0,224402	-0,429258	0,32
C21	90	32	0,519099	0,674968	-0,510579	0,535613	0,535613	0,648297	0,215338	0,215163	0,146242	0,470368	-0,550327	0,152286	0,188202	-0,371030	0,16
C22	8	22	-0,446470	-0,531000	0,436094	-0,632789	-0,632789	-0,557064	-0,082320	-0,111285	-0,084871	-0,248875	0,373312	-0,219039	-0,102087	0,245942	-0,22
C23	21	14	0,749203	0,914765	-0,702630	0,608859	0,608859	0,880689	0,411651	0,373869	-0,003335	0,637845	-0,589606	0,289422	0,335075	-0,601710	0,40
C24	17	15	0,521124	0,691072	-0,529283	0,465391	0,465391	0,688370	0,341029	0,270537	-0,077208	0,438214	-0,495006	0,258588	0,096004	-0,356166	0,19
C25	2	4	-0,531820	-0,585685	0,467256	-0,575130	-0,575130	-0,585603	-0,198654	-0,144931	-0,095416	-0,308799	0,450374	-0,226379	-0,142786	0,242131	-0,18
C26	2	3	-0,565474	-0,635738	0,533144	-0,486116	-0,486116	-0,710807	-0,149611	-0,147532	-0,147211	-0,313398	0,464582	-0,156915	-0,149780	0,331639	-0,19

Рисунок 1.38 – Кореляційна матриця взаємозалежності релевантних факторів, що визначають стан протидії фінансовому кібершахрайству та рівня кібербезпеки для країн світу

Джерело: розроблено авторами

На рисунку 1.38 видно, що розрахункові коефіцієнти кореляції між результативним показником С0 та факторними показниками мають наступний зв'язок: сильний зв'язок – коефіцієнт кореляції між С0 та С1 дорівнює 0,80, С2 – 0,77, С5 – 0,79, С23 – 0,74; середній зв'язок – коефіцієнт кореляції між С0 і С3 дорівнює 0,58,С4 – 0,58, С6 – 0,46, С9 – 0,60, С10 – 0,51, С20 – 0,68, С21 – 0,51, С22 – 0,44, С24 – 052, С25 – 053, С26 – 0,56, С27 – 0,61; слабкий зв'язок - коефіцієнт кореляції між С0 і С7 дорівнює 0,34, С13 – 0,34, С14 – 0,28, С16 – 031, С18 – 0,30, С29 – 0,30. Але далі, при дослідженні впливу факторів, що визначають стан протидії фінансовому кібершахрайству, на рівень кібербезпеки, варто приймати до уваги ознаки з сильним і середнім зв'язком.

Таким чином, для країн Світу результати проведених перевірок релевантності впливу факторів, що визначають стан протидії фінансовому кібершахрайству на рівень кібербезпеки, що виконано методом Univariate Tests of Significance, побудовою Pareto Chart of t-Values значущості впливу факторів, побудови кореляційної матриці взаємозалежності релевантних факторів, встановлено найвпливовіші фактори: С1, С2, С5, С23; С3, С4, С6, С9, С10, С20, С21, С22, С24, С25, С26, С27.

Аналогічно для кластеру 7 країн з Україною побудовано кореляційну матрицю взаємозалежності релевантних факторів, що визначають стан протидії фінансовому кібершахрайству впливу на рівень кібербезпеки (рисунок 1.39).

	Correlations (SpreadsheetBerezhna_fact_cl3.sta) Marked correlations are significant at p < ,05000 N=7 (Casew ise deletion of missing data)															
Variable	Means	Std.Dev.	C0	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11	C12	C13
C0	66	17	1,000000	0,788225	-0,236449	-0,192997	-0,192997	0,864923	0,440806	0,599470	-0,464515	0,689146	-0,732314	0,060861	0,183833	-0,585464
C1	58	12	0,788225	1,000000	-0,503624	0,066603	0,066603	0,975383	0,652369	0,925734	-0,777973	0,851776	-0,677522	0,302353	0,521911	-0,513255
C2	5	1	-0,236449	-0,503624	1,000000	0,294999	0,294999	-0,439601	-0,727955	-0,669148	0,661092	-0,275072	-0,060984	-0,528874	-0,538629	-0,164628
C3	81	11	-0,192997	0,066603	0,294999	1,000000	1,000000	0,117184	-0,244242	0,056591	-0,265781	0,350083	-0,357849	0,122499	-0,308231	-0,031810
C4	81	11	-0,192997	0,066603	0,294999	1,000000	1,000000	0,117184	-0,244242	0,056591	-0,265781	0,350083	-0,357849	0,122499	-0,308231	-0,031810
C5	1	0	0,864923	0,975383	-0,439601	0,117184	0,117184	1,000000	0,569390	0,856384	-0,783722	0,885371	-0,758440	0,285371	0,403017	-0,571087
C6	1	0	0,440806	0,652369	-0,727955	-0,244242	-0,244242	0,569390	1,000000	0,723726	-0,369709	0,221141	-0,027763	0,664165	0,491834	0,124810
C7	758071	991266	0,599470	0,925734	-0,669148	0,056591	0,056591	0,856384	0,723726	1,000000	-0,794087	0,786189	-0,569965	0,266110	0,459102	-0,194273
C8	9	3	-0,464515	-0,777973	0,661092	-0,265781	-0,265781	-0,783722	-0,369709	-0,794087	1,000000	-0,842111	0,549961	-0,303457	-0,450845	0,378273
C9	1	1	0,689146	0,851776	-0,275072	0,350083	0,350083	0,885371	0,221141	0,786189	-0,842111	1,000000	-0,901759	-0,039148	0,199174	-0,553049
C10	43	22	-0,732314	-0,677522	-0,060984	-0,357849	-0,357849	-0,758440	-0,027763	-0,569965	0,549961	-0,901759	1,000000	0,296977	0,159730	0,508549
C11	32	16	0,060861	0,302353	-0,528874	0,122499	0,122499	0,285371	0,664165	0,266110	-0,303457	-0,039148	0,296977	1,000000	0,495408	0,030908
C12	11	13	0,183833	0,521911	-0,538629	-0,308231	-0,308231	0,403017	0,491834	0,459102	-0,450845	0,199174	0,159730	0,495408	1,000000	-0,453428
C13	3	3	-0,585464	-0,513255	-0,164628	-0,031810	-0,031810	-0,571087	0,124810	-0,194273	0,378273	-0,553049	0,508549	0,030908	-0,453428	1,000000
C14	27	23	0,205429	0,487158	-0,493005	-0,210547	-0,210547	0,411882	0,469682	0,361935	-0,444115	0,165758	0,181692	0,648788	0,961249	-0,509970
C15	11	10	0,381725	0,573852	-0,550518	-0,531131	-0,531131	0,459445	0,691529	0,503007	-0,294463	0,131963	0,134316	0,487692	0,915088	-0,367518
C16	13	8	-0,362766	-0,486957	0,461760	-0,058995	-0,058995	-0,532968	0,056251	-0,439884	0,841863	-0,684862	0,443669	0,008431	-0,393445	0,541314
C17	30	19	-0,226580	-0,151729	-0,469215	0,010927	0,010927	-0,126338	0,398111	-0,111447	-0,050908	-0,384627	0,567093	0,845616	0,163461	0,363683
C18	1	1	-0,395795	-0,317055	0,699709	0,655816	0,655816	-0,297995	-0,333522	-0,449579	0,407693	-0,258709	0,134001	0,155594	-0,226441	-0,055037
C19	8754531	2067614	-0,399001	-0,403441	0,759278	0,622507	0,622507	-0,367131	-0,773810	-0,384571	0,270176	0,030101	-0,257060	-0,648266	-0,635385	0,052488
C20	78	10	0,898822	0,858771	-0,072819	0,116388	0,116388	0,914020	0,316588	0,623627	-0,557089	0,819975	-0,814488	0,087906	0,303684	-0,784338
C21	112	50	0,587451	0,587317	-0,416381	0,339957	0,339957	0,677103	0,570689	0,582316	-0,532357	0,546084	-0,534337	0,462615	-0,150269	0,035140
C22	3	2	-0,939426	-0,643065	0,122559	0,335232	0,335232	-0,728980	-0,193211	-0,421045	0,383548	-0,616566	0,677328	0,151995	-0,198683	0,708074
C23	19	12	0,777253	0,976116	-0,462297	-0,030277	-0,030277	0,943348	0,570986	0,863667	-0,754214	0,822073	-0,628644	0,250406	0,638455	-0,645290
C24	12	9	0,548409	0,843051	-0,658008	-0,020783	-0,020783	0,808218	0,450762	0,793100	-0,910004	0,764361	-0,441666	0,314908	0,738257	-0,574043
C25	1	1	-0,419408	-0,565110	0,542881	-0,245623	-0,245623	-0,582933	-0,421658	-0,743338	0,663326	-0,676443	0,615819	-0,014049	0,176813	-0,208511

Рисунок 1.39 – Кореляційна матриця взаємозалежності релевантних факторів, що визначають стан протидії фінансовому кібершахрайству та рівня кібербезпеки для кластеру 7 країн з Україною

Джерело: розроблено авторами

На рисунку 1.33 видно, що розрахункові коефіцієнти кореляції між результативним показником C0 та факторними показниками мають наступний зв'язок: сильний зв'язок – коефіцієнт кореляції між C0 та C1 дорівнює 0,78, C5 – 0,86, C20 – 0,89, C22 – 0,93, C23 – 0,77. Таким чином, для кластеру 7 країн з Україною встановлено найвпливовіші фактори: C1, C5, C20, C22, C23.

Адекватність моделі перевірено на етапі 3 (визначення релевантних факторів, що визначають стан протидії фінансовому кібершахрайству, при проведенні Univariate Tests of Significance. Адекватність перевірено за допомогою показників дсперсійного аналізу як і в 2-му етапі; а також шляхом побудови Pareto Chart of t-Values значущості впливу факторів, що визначають стан протидії фінансовому кібершахрайству на рівень кібербезпеки.

Етап 4 передбачає визначення сили та напрямку впливу релевантних факторів, що визначають стан протидії фінансовому кібершахрайству, на рівень кібербезпеки; побудова множинної лінійної регресії з використанням методу найменших квадратів (OLS-метод).

Першим кроком 4 етапу – визначення сили впливу, а також напрямку впливу виявлених для країн Світу релевантних факторів, що визначають стан протидії фінансовому кібершахрайству, на рівень кібербезпеки, для побудови множинної лінійної регресії. Для побудови множинної лінійної регресії використовуємо спочатку усі 32 фактори, що визначають стан протидії фінансовому кібершахрайству, впливають на результативний фактор C0 (рівень кібербезпеки). На рисунку 1.40 відображено розрахункові показники регресійного аналізу залежності між рівнем кібербезпеки та факторами, що визначають стан протидії фінансовому кібершахрайству.

Regression Summary for Dependent Variable: C0 (SpreadsheetBerezhna_fact_
R= ,90561669 R?= ,82014159 Adjusted R?= ,78089975
F(12,55)=20,900 p<,00000 Std.Error of estimate: 11,139

N=68	Beta	Std.Err. of Beta	B	Std.Err. of B	t(55)	p-level
Intercept			39,23216	23,18071	1,69245	0,096219
C1	0,599399	0,127163	0,87770	0,18621	4,71363	0,000017
C2	-0,395630	0,110917	-8,20131	2,29929	-3,56689	0,000757
C16	0,235390	0,079429	0,26939	0,09090	2,96355	0,004487
C15	-0,117170	0,070397	-0,24592	0,14775	-1,66441	0,101719
C8	0,188830	0,062220	1,85732	0,61199	3,03487	0,003671
C6	0,190875	0,080134	20,19924	8,48016	2,38194	0,020708
C11	-0,065245	0,067962	-0,10758	0,11206	-0,96002	0,341245
C29	-0,107269	0,073769	-0,09908	0,06814	-1,45413	0,151592
C22	-0,096476	0,077872	-0,10636	0,08585	-1,23890	0,220642
C18	0,113988	0,082458	0,42612	0,30825	1,38237	0,172445
C7	0,072721	0,063477	0,00000	0,00000	1,14563	0,256911
C12	-0,079040	0,073304	-0,16987	0,15755	-1,07825	0,285631

Рисунок 1.40 – Розрахункові показники регресійного аналізу залежності між рівнем кібербезпеки та факторами, що визначають стан протидії фінансовому кібершахрайству країн світу (32 показника)

Джерело: розроблено авторами

З рисунку 1.40 видно, що не усі фактори, що визначають стан протидії фінансовому кібершахрайству є статистично значущими. Тобто статично значущими є фактори: C1, C2, C16, C8, C6. Що також було частково визначено на другому етапі дослідження. Так як побудована модель є не достатньо адекватною згідно розрахункових показників регресійного аналізу, то модель лінійної множинної регресійної залежності між рівнем кібербезпеки та факторами, що визначають стан протидії фінансовому кібершахрайству, будувати за цими даними не доцільно.

Тому здійснено повторно аналогічний регресійний аналіз, але для залежності між рівнем кібербезпеки та 5 релевантними факторами (рисунок 1.41) відображено розрахункові показники регресійного аналізу залежності між рівнем кібербезпекита релевантними факторами, що визначають стан протидії фінансовому кібершахрайству.

Regression Summary for Dependent Variable: C0 (SpreadsheetBerezhna_
R= ,87543336 R?= ,76638357 Adjusted R?= ,74754354
F(5,62)=40,678 p<,00000 Std.Error of estimate: 11,957

N=68	Beta	Std.Err. of Beta	B	Std.Err. of B	t(62)	p-level
Intercept			24,89091	22,22575	1,11991	0,267071
C1	0,607221	0,102760	0,88916	0,15047	5,90911	0,000000
C2	-0,383360	0,110436	-7,94696	2,28931	-3,47134	0,000949
C6	0,098330	0,078945	10,40567	8,35427	1,24555	0,217616
C8	0,165196	0,064064	1,62485	0,63013	2,57860	0,012308
C16	0,274093	0,075794	0,31368	0,08674	3,61629	0,000601

Рисунок 1.41 – Розрахункові показники регресійного аналізу залежності між рівнем кібербезпеки та 5 факторами, що визначають стан протидії фінансовому кібершахрайству країн Світу (5 показників)

Джерело: розроблено авторами

Модель є достатньо адекватною (описано далі). Далі, згідно показників рисунку 11, формулюємо модель лінійної множинної регресійної залежності між рівнем кібербезпеки та факторами, що визначають стан протидії фінансовому кібершахрайству країн Світу (хоча один фактор є не релевантним) (формула 1.31):

$$C0 = 24{,}8909 + 0{,}8891 \cdot C1 - 7{,}9769 \cdot C2 + 10{,}4056 \cdot C6 + 1{,}6248 \cdot C8 + 0{,}3136 \cdot C16 \quad (1.31)$$

Далі, так як один фактор не є релевантним, здійснено ще один регресійний аналіз, але для залежності між рівнем кібербезпеки та 4 релевантними факторами (рисунок 1.42).

Regression Summary for Dependent Variable: C0 (SpreadsheetBerezhna_fact_
R= ,87208824 R?= ,76053789 Adjusted R?= ,74533395
F(4,63)=50,022 p<,00000 Std.Error of estimate: 12,009

N=68	Beta	Std.Err. of Beta	B	Std.Err. of B	t(63)	p-level
Intercept			40,79095	18,27359	2,23223	0,029163
C1	0,604101	0,103178	0,88459	0,15108	5,85492	0,000000
C2	-0,440572	0,100869	-9,13295	2,09099	-4,36777	0,000048
C8	0,142745	0,061745	1,40403	0,60732	2,31186	0,024067
C16	0,268513	0,075992	0,30730	0,08697	3,53344	0,000774

Рисунок 1.42 – Розрахункові показники регресійного аналізу залежності між рівнем кібербезпеки та 4 релевантними факторами, що визначають стан протидії фінансовому кібершахрайству країн Світу (4 показника)

Джерело: розроблено авторами

Згідно показників рисунку 1.42 формулюємо модель лінійної множинної регресійної залежності між рівнем кібербезпеки та 4 релевантними факторами, що визначають стан протидії фінансовому кібершахрайству країн Світу (формула 1.32):

$$C0 = 40.7909 + 0{,}8845 \cdot C1 - 9{,}1329 \cdot C2 + 1{,}4040 \cdot C8 + 0{,}3073 \cdot C16 \quad (1.32)$$

Отримана модель є адекватною та точною, що описано нижче для етапу 4. Усі обрані у модель фактори є статистично значущими, про що свідчать критерії Стьюдента та p-рівні (що є не вище допустимого критичнго рівня 0,05). Наступний аналіз показників моделі лінійної множинної регресійної залежності між рівнем кібербезпеки та релевантними факторами, що визначають стан протидії фінансовому кібершахрайству для країн Світу (формула 1.32): дозволяє сформулювати такі висновки:

– стимулятор рівня кібербезпеки є показник C1,C8,C16 (збільшення цього фактору спричиняє зростання як результативного фактору рівня кібербезпеки); так збільшення C1 на 1 одиницю спричиняє зростання рівня кібербезпеки на

0,8845 одиниці;. збільшення C8 на 1 одиницю спричиняє зростання рівня кібербезпеки на 1,4040 одиниці; збільшення C16 на 1 одиницю спричиняє зростання рівня кібербезпеки на 0,3073 одиниці;

– дестимулятор рівня кібербезпеки є показник C2 (збільшення цього фактору спричиняє зменшення як результативного фактору рівня кібербезпеки), так збільшення C2 на 1 одиницю спричиняє зменшення рівня кібербезпеки на 9,1329 одиниці;

– не здійснюють на рівень кібербезпеки статистично значущого впливу фактори інші фактори.

Другим кроком 4 етапу – визначення сили впливу, а також напрямку впливу виявлених для країн кластеру з Україною релевантних факторів, що визначають стан протидії фінансовому кібершахрайству, на рівень кібербезпеки, для побудови множинної лінійної регресії. Проводяться дії аналогічно попередньому регресійному аналізу для 68 країн Світу. Визначено сили впливу, а також напрямки впливу виявлених для кластеру 7 країн з Україною релевантних факторів та побудовано множинну лінійну регресію з використанням методу найменших квадратів (OLS-метод).

Для побудови множинної лінійної регресії використовуємо спочатку усі 32 фактори, що визначають стан протидії фінансовому кібершахрайству, впливають на рівень кібербезпеки та результативний фактор C0. На рисунку 1.43 відображено розрахункові показники регресійного аналізу залежності між рівнем кібербезпекита факторами, що визначають стан протидії фінансовому кібершахрайству. Де ми спостерігаємо відсутність залежностей при такому наборі факторів.

	Regression Summary for Dependent Variable: C0 (SpreadsheetBerezhna_fa R=1,00000000 R?=1,00000000 Adjusted R?=1,00000000 F(6,0)= -- p< -- Std.Error of estimate: ----					
N=7	Beta	Std.Err. of Beta	B	Std.Err. of B	t(0)	p-level
Intercept			65,66175			
C22	-0,889388		-6,89166			
C21	0,215393		0,07512			
C6	0,258138		17,35637			
C27	0,179880		3,34721			
C10	-0,082039		-0,06544			
C25	0,003874		0,13124			

Рисунок 1.43 – Розрахункові показники регресійного аналізу залежності між рівнем кібербезпеки та факторами, що визначають стан протидії фінансовому кібершахрайству для кластеру 7 країн з Україною (32 показника)

Джерело: розроблено авторами

Тому для визначеного кластеру країн здійснено повторно регресійний аналіз, але для залежності між рівнем кібербезпеки та факторами, що визначають стан протидії фінансовому кібершахрайству (що було визначено при кореляційному аналізі). На рисунку 1.44 відображено розрахункові показники регресійного аналізу залежності між рівнем кібербезпекита релевантними факторами, що визначають стан протидії фінансовому кібершахрайству.

N=7	Regression Summary for Dependent Variable: C0 (SpreadsheetBerezhna_fact_cl3.s R= ,99327194 R?= ,98658915 Adjusted R?= ,91953493 F(5,1)=14,713 p<,19528 Std.Error of estimate: 4,9050 Beta	Std.Err. of Beta	B	Std.Err. of B	t(1)	p-level
Intercept			12,7802	67,3085	0,18987	0,880544
C1	1,50058	1,305931	2,1251	1,8494	1,14905	0,455917
C5	-0,24016	0,966822	-49,3960	198,8562	-0,24840	0,845001
C20	0,16138	0,390962	0,2750	0,6663	0,41277	0,750786
C22	-0,83656	0,258958	-6,4823	2,0066	-3,23048	0,191111
C23	-1,18291	0,770545	-1,6556	1,0784	-1,53515	0,367558

Рисунок 1.44 – Розрахункові показники регресійного аналізу залежності між рівнем кібербезпеки та факторами, що визначають стан протидії фінансовому кібершахрайству для кластеру 7 країн з Україною (5 показників)

Джерело: розроблено авторами

Згідно отриманих даних рисунку 1.38 бачимо, що фактори не є статистично значущими, але залежність існує. Далі, згідно показників рисунку 1.38, формулюємо модель лінійної множинної регресійної залежності між рівнем кібербезпеки та факторами, що визначають стан протидії фінансовому кібершахрайству (формула 1.33):

$$C0 = 12{,}7802 + 2{,}1251 \cdot C1 - 49{,}3960 \cdot C5 + 0{,}2750 \cdot C20 - 6{,}4823 \cdot C22 - 1{,}6556 \cdot C23 \quad (1.33)$$

Наступний аналіз показників моделі лінійної множинної регресійної залежності для обраного кластеру з Україною між рівнем кібербезпеки та релевантними факторами, що визначають стан протидії фінансовому кібершахрайству (формула 1.33) дозволяє сформулювати такі висновки:

- стимулятор рівня кібербезпеки є показник C1,C20 (збільшення цього фактору спричиняє зростання як результативного фактору рівня кібербезпеки); так збільшення C1 на 1 одиницю спричиняє зростання рівня кібербезпеки на 2,1251 одиниці; збільшення C20 на 1 одиницю спричиняє зростання рівня кібербезпеки на 0,2750 одиниці;

- дестимулятори рівня кібербезпеки є показники C5, C22, C23 (збільшення цих факторів спричиняє зменшення як результативного фактору рівня кібербезпеки), так збільшення C5 на 1 одиницю спричиняє зменшення рівня кібербезпеки на 49,3960 одиниці; збільшення C22 на 1 одиницю спричиняє зменшення рівня кібербезпеки на 6,4823 одиниці; збільшення C23 на 1 одиницю спричиняє зменшення рівня кібербезпеки на 1,6556 одиниці;

- не здійснюють на рівень кібербезпеки статистично значущого впливу фактори інші фактори.

Адекватність моделі регресійного аналізу перевірено за допомогою показників адекватності (коефіцієнта детермінації та значення критерію Фішера) по 68 країнам світу для 32 факторів, по 68 країнам світу для 5 факторів, по 68 країнам світу для 4 факторів (рисунок 1.39). Також точність і адекватність моделі підтверджується шляхом побудови графіку відповідності нормальному закону

розподілу залишків лінійної регресійної моделі залежності між рівнем кібербезпеки релевантних факторів, що визначають стан протидії фінансовому кібершахрайству (рисунок 1.45).

	Summary Statistics; DV: C0 (SpreadsheetBerezhna_fact_.
Statistic	Value
Multiple R	0,87209
Multiple R?	0,76054
Adjusted R?	0,74533
F(4,63)	50,02241
p	0,00000
Std.Err. of Estimate	12,00893

Рисунок 1.45 – Показники адекватності регресійного аналізу залежності між рівнем кібербезпеки та факторами, що визначають стан протидії фінансовому кібершахрайству для 68 країн сСвіту (4 фактори)

Джерело: розроблено авторами

Модель по 68 країнам Світу для 32 факторів – є не достатньо адекватною та точною з огляду на відповідний рівень коефіцієнта детермінації 0,9056 (відповідає нормі) та значення критерію Фішера 20,89 (не відповідає критичному значення), що є менше за критично допустимий рівень); модель по 68 країнам Світу для 5 факторів – є достатньо адекватною та точною з огляду на відповідний рівень коефіцієнта детермінації 0,8754 (відповідає нормі) та значення критерію Фішера 40,6784 (відповідає критичному значенню), що є більше за критично допустимий рівень ; по 68 країнам Світу для 4 факторів – є повністю адекватною та точною з огляду на відповідний рівень коефіцієнта детермінації 0,8720 (відповідає нормі) та значення критерію Фішера 50,0224 (відповідає критичному значенню), що є більше за критично допустимий рівень.

Аналогічно перевірено адекватність і точність регресійного аналізу залежності між рівнем кібербезпеки та факторами, що визначають стан протидії фінансовому кібершахрайству для кластеру з Україною для 32 факторів (рисунок А.10) – модель є повністю не адекватною, та 5 факторів – модель є адекватною та точною з огляду на відповідний рівень коефіцієнта детермінації 0,9932 (відповідає нормі) та значення критерію Фішера 14,7133 (відповідає критичному значенню), що є більше за критично допустимий рівень.

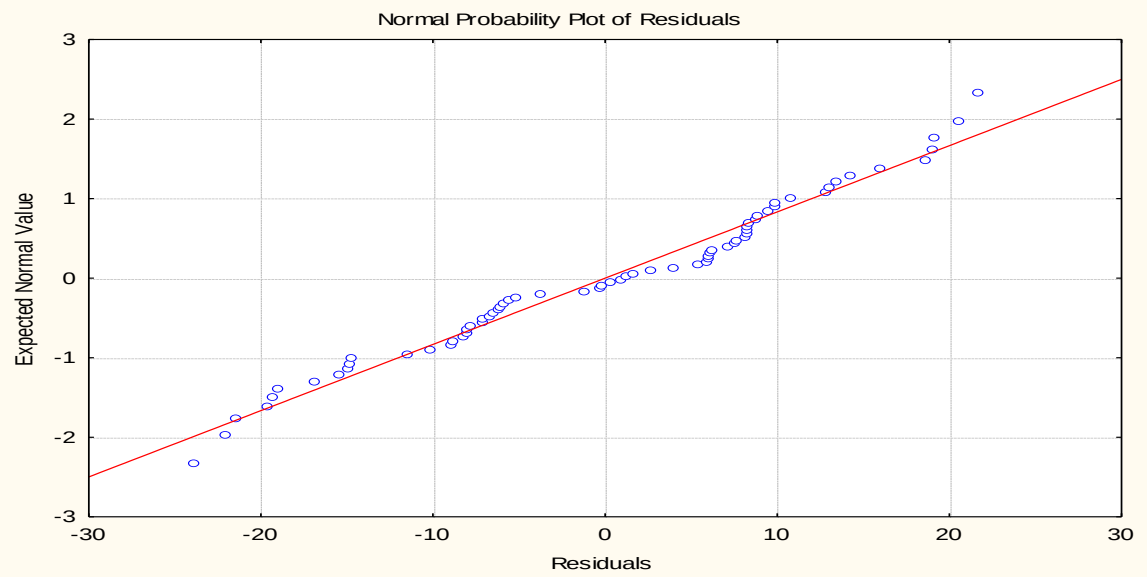


Рисунок 1.46 – Графічне зображення відповідності нормальному закону розподілу залишків лінійної регресійної моделі залежності між рівнем кібербезпеки і релевантних факторів, що визначають стан протидії фінансовому кібершахрайству для 68 країн світу (4 фактори)

Джерело: розроблено авторами

Таким чином, використання суб'єктами господарювання методик і моделей due diligence, дозволить сформувати керівні принципи та політику фінансової безпеки підприємств, що в свою чергу допоможе знизити рівень негативних наслідків в тому числі і фінансових кіберзагроз, фінансових кіберризиків, що можуть бути присутні у бізнес процесах; максимізувати можливі позитивні ефекти від прийняття сформованих з урахуванням ряду факторів, управлінських рішень.

РОЗДІЛ 2

НАПРЯМИ РОЗВИТКУ СИСТЕМИ ЗАПОБІГАННЯ ТА ПРОТИДІЇ ФІНАНСОВИМ КІБЕРШАХРАЙСТВАМ: КОНВЕРГЕНЦІЯ, ІНСТРУМЕНТАРІЙ ТА УПРАВЛІННЯ

2.1. Обґрунтування концепції конвергенції системи фінансового моніторингу та кібершахрайств

2.1.1. Концепція конвергенції систем фінансового моніторингу і кібербезпеки

Швидкий розвиток і накопичення новітніх технологій та цифрових даних створюють умови для використання інформаційних технологій у різних галузях та сферах діяльності. В Україні та світі створено сприятливі умови для зручного використання новітніх технологій у фінансовому секторі в онлайн режимі. Це дозволяє як фізичним особам, так і бізнесам віддалено користуватися фінансовими послугами, підключатися до онлайн банкінгу, валютних бірж, фондового ринку та інших фінансових установ. Проте цей процес супроводжується загрозами, оскільки в інформаційному просторі з'являються нові можливості для злочинців і легальних користувачів. Однак застосування цих нових можливостей в економічній сфері створює потребу в забезпеченні ефективної економічної безпеки для фінансових операцій, які проводяться через ці системи. За останні 10 років в Україні була встановлена система для протидії відмиванню незаконних коштів, фінансуванню тероризму, поширенню зброї масового знищення, включаючи кіберзагрози. Ця система включає в себе комплекс заходів з фінансового моніторингу та кібербезпеки, які передбачають перевірку клієнтів та їх фінансових транзакцій з метою забезпечення економічної чистоти та прозорості фінансових операцій. Але сьогодні розглядати окремо системи фінансового моніторингу та кібербезпеки є не актуальним, оскільки їх комплексне функціонування є більш дієвим та ефективним, тобто виникає необхідність забезпечення їх конвергенції.

Термін "конвергенція систем" вказує на процес зближення або об'єднання різних систем чи підходів у велику, загальну систему або методологію. Цей процес може відбуватися в різних галузях, таких як інформаційні технології, наука, бізнес, адміністрування тощо.

У контексті інформаційних технологій, конвергенція систем може означати інтеграцію різних технологічних платформ, пристроїв або програм для створення більш ефективних та уніфікованих рішень. Наприклад, зближення мобільних телефонів і персональних комп'ютерів спричинило розвиток смартфонів, які об'єднують функціональність обох пристроїв.

У науковому дослідженні, конвергенція систем вказує на те, як різні дисципліни або підходи можуть об'єднатися для вирішення складних проблем або досягнення нових відкриттів. Наприклад, в медичній науці конвергенція

може включати в себе поєднання біології, інженерії, інформатики та інших галузей для розробки нових методів діагностики та лікування.

У сутності, конвергенція систем означає спільний розвиток та інтеграцію різних компонентів для досягнення нових можливостей, покращення ефективності і створення більш комплексних рішень у різних галузях життя.

Конвергенція системи фінансового моніторингу та кібербезпеки вказує на об'єднання чи інтеграцію двох ключових аспектів в сфері фінансових послуг та фінансової безпеки: системи фінансового моніторингу і системи кібербезпеки.

1. Система фінансового моніторингу (СФМ) - це комплекс заходів і технологічних рішень, спрямованих на виявлення та відслідковування незаконних фінансових транзакцій і операцій, таких як відмивання грошей та фінансування тероризму. СФМ використовує різні аналітичні методи та програми для моніторингу фінансової діяльності та виявлення потенційних порушень.

2. Система кібербезпеки - це набір заходів та технологій, спрямованих на захист інформації, комп'ютерних систем та мереж від кіберзагроз, таких як хакерські атаки, віруси, шахрайство тощо.

Конвергенція цих систем включає в себе об'єднання або інтеграцію технічних засобів, процесів та експертних знань для забезпечення взаємодії між фінансовим моніторингом та кібербезпекою. Мета такої конвергенції - забезпечити безпечну та надійну фінансову систему, у якій фінансові транзакції перевіряються на наявність сумнівних або незаконних операцій, а також захищені від кібератак та порушень безпеки даних.

Ця об'єднана підхід може включати в себе моніторинг мережевого трафіку та аналіз великих обсягів даних для виявлення незаконних операцій, а також заходи для захисту фінансових інформаційних систем від кіберзагроз. Такий підхід допомагає забезпечити більш ефективний контроль і безпеку фінансових операцій у цифровому світі.

Конвергенція між системою фінансового моніторингу та системою кібербезпеки має кілька завдань та цілей:

1. Забезпечення безпеки фінансових операцій. Головною метою є захист фінансових транзакцій від шахраїв, злочинців та кіберзлочинців. Конвергенція дозволяє виявляти незаконні або сумнівні фінансові операції та надавати належну відповідь.

2. Виявлення кіберзагроз. Інтеграція систем кібербезпеки дозволяє виявляти та реагувати на кібератаки, які можуть вплинути на безпеку фінансових даних та транзакцій. Це може включати в себе виявлення зламів, вірусів, шахрайства тощо.

3. Моніторинг фінансових ризиків. Конвергенція дозволяє створити комплексну систему для виявлення та оцінки фінансових ризиків, включаючи ризики відмивання грошей, фінансування тероризму та інші.

4. Забезпечення відповідності регуляціям. У багатьох країнах існують правила та регуляції щодо фінансового моніторингу та кібербезпеки.

Конвергенція допомагає фінансовим установам дотримуватися цих вимог та стандартів.

5. Ефективність та економія ресурсів. Об'єднання фінансового моніторингу та кібербезпеки дозволяє ефективніше використовувати ресурси, зменшуючи дублювання функцій та процесів.

6. Забезпечення захисту конфіденційності та приватності даних: Конвергенція допомагає забезпечити, що фінансові дані та особиста інформація клієнтів залишаються конфіденційними та захищеними від незаконного доступу.

Узагальнюючи, конвергенція між системою фінансового моніторингу та системою кібербезпеки спрямована на створення інтегрованої та безпечної середовища для фінансових операцій, що відповідає вимогам законодавства та забезпечує захист від фінансових злочинів та кіберзагроз.

Існує декілька напрямків, в рамках яких відбувається конвергенція фінансового моніторингу та кібербезпеки:

1. Об'єднання технологічних рішень. Один із головних напрямків полягає у спільному використанні та інтеграції технологічних засобів і рішень для фінансового моніторингу та кібербезпеки. Це включає в себе створення спільних платформ, які можуть виявляти як фінансові, так і кіберзагрози, і забезпечувати їхню взаємодію для більш ефективного виявлення та реагування на можливі порушення.

2. Спільний аналіз даних. Об'єднання фінансового моніторингу та кібербезпеки може включати спільний аналіз великих обсягів даних. Аналітичні інструменти та алгоритми можуть використовуватися для виявлення аномалій або незаконних дій, які можуть вказувати на фінансовий злочин чи кібератаку.

3. Обмін інформацією. Фінансові установи та органи кібербезпеки можуть співпрацювати для обміну інформацією про виявлені загрози та атаки. Це допомагає у швидкому реагуванні на нові загрози та спільному вирішенні проблем.

4. Освіта та навчання. Кадри важливі для успішної конвергенції. Організації повинні навчати своїх співробітників і експертів як виявляти фінансові порушення та кіберзагрози, і як ефективно реагувати на них.

5. Захист інфраструктури. Інфраструктура, яка використовується для фінансового моніторингу та кібербезпеки, повинна бути належно захищеною від кібератак та вторгнень. Це включає в себе застосування найсучасніших методів захисту та кібербезпеки.

6. Законодавство та регуляція. У багатьох країнах необхідні зміни в законодавстві та регулюючих вимогах для врахування конвергенції фінансового моніторингу та кібербезпеки. Правила і норми повинні визначати вимоги до захисту фінансових даних і інформації про клієнтів.

Ці напрямки допомагають створити більш ефективну та безпечну систему фінансового моніторингу, яка враховує сучасні кіберзагрози та ризики.

Існує кілька моделей конвергенції фінансового моніторингу та кібербезпеки, які можуть бути використані в організаціях та фінансових установах для підвищення безпеки та ефективності. Ось декілька з них:

1. Інтегрована модель (Integrated Model). Ця модель передбачає створення єдиної системи, яка об'єднує фінансовий моніторинг та кібербезпеку. Це означає, що одна платформа відслідковує і аналізує як фінансові транзакції, так і потенційні кіберзагрози. Інформація про фінансові операції та кіберзаходи обробляється разом для виявлення незаконних дій та порушень безпеки.

2. Спільна модель (Collaborative Model). У цій моделі фінансові установи співпрацюють з кібербезпековими фахівцями та органами, обмінюючи інформацією та аналізами. Фінансові установи можуть виявляти сумнівні фінансові транзакції та повідомляти про них спеціалізованим організаціям з кібербезпеки для подальшого розслідування.

3. Модель захисту кібербезпеки фінансових операцій (Financial Cybersecurity Protection Model). В цій моделі основний акцент робиться на захисті фінансових операцій від кіберзагроз. Основною метою є забезпечення безпеки фінансових даних та транзакцій, а також виявлення та запобігання кібератак.

4. Фінансово-кібербезпекова екосистема (Financial Cybersecurity Ecosystem). У цій моделі створюється екосистема, яка включає в себе фінансові установи, органи кібербезпеки, правоохоронні органи, інші галузеві гравці та технологічні компанії. Вони спільно працюють для виявлення та реагування на загрози та порушення.

5. Кіберінтелектуальна модель (Cyber Threat Intelligence Model). В цій моделі фінансові установи використовують кіберінтелект та аналіз кіберзагроз для виявлення потенційних атак та вдосконалення захисту. Це може включати в себе використання спеціалізованих інструментів та платформ для збору та аналізу інформації про кіберзагрози.

Кожна з цих моделей має свої переваги та недоліки, і вибір конкретної залежить від потреб та особливостей конкретної організації чи фінансової установи. У будь-якому випадку, головною метою є забезпечення безпеки фінансових операцій та даних у світі, де кіберзагрози стають все більш серйозними та складними.

Підготовка існуючих систем до конвергенції фінансового моніторингу та кібербезпеки може бути складним завданням, але вона є важливою для забезпечення безпеки та ефективності в організації. Ось кроки, які можуть бути вжиті для підготовки систем до конвергенції:

1. Оцінка потреб. Ретельно оцініть потреби та цілі вашої організації в конвергенції фінансового моніторингу та кібербезпеки. Розгляньте, які конкретні загрози і ризики важливі для вашої організації і як вони пов'язані з фінансовими операціями.

2. Визначення обсягу інтеграції. Визначте, які системи, процеси та дані потрібно інтегрувати для досягнення цілей конвергенції. Це може включати в себе фінансовий моніторинг, системи кібербезпеки, моніторинг мережевого трафіку та інші.

3. Створення команди. Створіть команду, яка буде відповідальна за розробку та впровадження конвергенції. Ця команда повинна включати фахівців

з фінансового моніторингу, кібербезпеки, програмісти, аналітиків та інших спеціалістів.

4. Аналіз існуючих процесів. Ретельно проаналізуйте існуючі процеси та технології, які використовуються в вашій організації для фінансового моніторингу та кібербезпеки. Визначте, які аспекти можуть бути оптимізовані або підвищені за допомогою конвергенції.

5. Вибір та налаштування інструментів. Виберіть відповідні інструменти та технології для інтеграції. Це можуть бути програми для аналізу даних, системи моніторингу мережевого трафіку, інструменти кібербезпеки, тощо. Налаштуйте їх так, щоб вони взаємодіяли між собою та відповідали потребам організації.

6. Організація навчання та свідомості. Забезпечте навчання співробітників та членів команди щодо нових інструментів і процесів, які вводяться в результаті конвергенції. Підвищте свідомість про кібербезпеку серед всіх учасників.

7. Розробка плану впровадження. Розробіть детальний план впровадження конвергенції, включаючи часові рамки, відповідальність та кроки для виконання. Постійно відстежуйте виконання плану та здійснюйте необхідні корективи.

8. Моніторинг та підтримка. Після впровадження системи конвергенції, не треба забувати про її моніторинг та підтримку. Постійно оновлюйте технології та процеси, щоб вони відповідали сучасним вимогам та загрозам.

Для визначення готовності існуючих систем до конвергенції фінансового моніторингу та кібербезпеки можна виконати наступні кроки:

1. Аудит систем і процесів. Проведіть докладний аудит існуючих систем фінансового моніторингу та кібербезпеки. Оцініть, як вони функціонують, які процеси і технології використовуються, та які дані обробляються. Цей аналіз допоможе вам зрозуміти, які аспекти можуть бути піддані конвергенції.

2. Визначення загроз і ризиків. Оцініть потенційні кіберзагрози та ризики, яким піддаються ваші фінансові та кібербезпекові системи. Визначте, які з них можуть бути зменшені або усунуті за допомогою конвергенції.

3. Визначення цілей конвергенції. Визначте чіткі цілі та очікування від конвергенції. Це може включати в себе покращення безпеки, збільшення ефективності моніторингу, скорочення ризиків та інші мети.

4. Оцінка технічної готовності. Визначте, чи потрібні нові технології або оновлення існуючих для конвергенції. Оцініть, чи системи та інфраструктура готові для інтеграції та спільної роботи.

5. Оцінка організаційної готовності. Переконайтесь, що ваша організація готова до змін, які принесе конвергенція. Це включає в себе підготовку персоналу, створення команди, яка відповідатиме за впровадження конвергенції, та забезпечення необхідних ресурсів.

6. Розробка плану впровадження. На основі результатів аудиту та оцінки готовності, розробіть детальний план впровадження конвергенції. Визначте кроки, ресурси, відповідальних та часові рамки для кожного етапу проекту.

7. Тестування та пілотний запуск. Перед повним впровадженням проведіть тестування та пілотний запуск конвергенції. Використовуйте реальні дані та сценарії для перевірки ефективності та безпеки нових систем.

8. Оцінка та корекція. Після впровадження постійно оцінюйте ефективність конвергенції та реагуйте на будь-які проблеми чи незадовільні результати. Здійсніть необхідні корективи в план впровадження.

9. Навчання та підтримка. Забезпечте навчання та підтримку для персоналу, щоб вони могли ефективно використовувати нові системи та процеси.

10. Моніторинг та підтримка в майбутньому. Після успішного впровадження конвергенції забезпечте постійний моніторинг та підтримку для збереження безпеки та ефективності систем в майбутньому.

Зазначені кроки допоможуть визначити готовність існуючих систем до конвергенції та забезпечити успішне впровадження цього процесу. Підготовка існуючих систем до конвергенції вимагає планування, ретельного аналізу та співпраці різних структурних підрозділів в організації. Добре спроектована та виконана конвергенція може покращити безпеку та ефективність ваших фінансових операцій та захистити вашу організацію від кіберзагроз.

У світі існують відомі практики конвергенції фінансового моніторингу та кібербезпеки, які впроваджуються різними організаціями та фінансовими установами для забезпечення безпеки фінансових операцій та даних. Деякі з цих практик включають:

1. Створення центру операційного моніторингу. Багато великих організацій створюють центри операційного моніторингу, де спеціалісти з фінансового моніторингу та кібербезпеки працюють разом для виявлення та вирішення загроз. Це дозволяє об'єднати різні аспекти безпеки в одній місцевості та спільно аналізувати дані.

2. Використання аналітики великих даних. Однією з практик є використання аналітики великих даних для виявлення аномалій та незаконних дій у фінансових транзакціях і мережевому трафіку. Ця аналітика допомагає виявляти сумнівні патерни та забезпечує більш ефективний моніторинг.

3. Спільний обмін інформацією. Багато країн створюють механізми для спільного обміну інформацією між фінансовими установами та органами кібербезпеки. Це допомагає виявляти загрози та швидко реагувати на них.

4. Використання машинного навчання та штучного інтелекту. Деякі організації використовують технології машинного навчання та штучного інтелекту для автоматизації процесів виявлення аномалій та незаконних дій. Ці системи можуть надавати більше точних результатів та реагувати на загрози в реальному часі.

5. Розвиток стандартів та регуляцій. Багато країн встановлюють стандарти та регуляції щодо фінансового моніторингу та кібербезпеки, які вимагають від організацій дотримуватися певних правил та стандартів безпеки.

6. Консультація з експертами: Деякі організації консультуються з експертами з областей фінансового моніторингу та кібербезпеки для розробки та впровадження конвергентних рішень.

Ці практики допомагають організаціям покращити безпеку та ефективність своїх фінансових операцій та захистити себе від сучасних кіберзагроз. Вони можуть бути використані як великими корпораціями, так і малими та середніми підприємствами для підвищення безпеки та зменшення ризиків.

Конвергенція фінансового моніторингу та кібербезпеки може призвести до ряду позитивних результатів та ефектів, які сприяють забезпеченню безпеки та ефективності фінансових операцій та захисту від кіберзагроз. Деякі з цих ефектів включають:

1. Покращення безпеки фінансових операцій. Конвергенція дозволяє виявляти сумнівні та незаконні фінансові транзакції та вчасно реагувати на них. Це допомагає попереджати фінансові злочини, відмивання грошей, фінансування тероризму та інші незаконні дії.

2. Виявлення кіберзагроз. Конвергенція дозволяє виявляти кіберзагрози та атаки на фінансові системи в реальному часі. Це допомагає реагувати на загрози швидше та запобігати можливим втратам та порушенням безпеки.

3. Зменшення ризику втрат. Конвергенція допомагає зменшити ризик втрат через незаконні або кібератаки. Шляхом інтеграції фінансового моніторингу та кібербезпеки можна виявляти та усувати потенційні загрози до фінансових операцій.

4. Зменшення витрат. Єдині системи фінансового моніторингу та кібербезпеки можуть зменшити витрати на обслуговування та адміністрування окремих систем. Крім того, автоматизація процесів та використання штучного інтелекту можуть підвищити ефективність та знизити витрати.

5. Підвищення ефективності моніторингу. Конвергенція дозволяє отримувати більше повний та інтегрований огляд фінансових операцій та кіберзагроз. Це робить моніторинг більш ефективним та допомагає виявляти патерни та аномалії, які можуть бути важко помітити в ізоляції.

6. Збільшення відповідності. Конвергенція допомагає відповідати вимогам законодавства та регуляцій у сферах фінансового моніторингу та кібербезпеки. Вона дозволяє забезпечити належну звітність та дотримання стандартів безпеки.

7. Покращення реакції на інциденти. Завдяки конвергенції можна ефективно реагувати на інциденти та кризові ситуації. Об'єднання фінансового моніторингу та кібербезпеки допомагає координувати заходи та швидко відновлювати безпеку після інциденту.

Загалом, конвергенція фінансового моніторингу та кібербезпеки сприяє покращенню безпеки, підвищенню ефективності та зменшенню ризиків для організацій та фінансових установ.

Сьогодні складно оцінити реальну готовність всіх українських банків до конвергенції фінансового моніторингу та кібербезпеки, оскільки це залежить від конкретних банків та їхніх індивідуальних ініціатив. Проте можна сказати, що тема кібербезпеки та фінансового моніторингу стала більш актуальною в Україні через зростання кіберзагроз і вимоги до відповідності законодавству у цих сферах. Регулятори можуть ставити більше вимог стосовно забезпечення безпеки та виявлення фінансових злочинів, що може стимулювати банки до розвитку конвергенції фінансового моніторингу та кібербезпеки. Багато банків можуть вивчати та впроваджувати технологічні рішення для вдосконалення своїх систем моніторингу та захисту. Проте готовність кожного банку буде варіювати в залежності від його фінансових можливостей, рівня технічної компетентності та підготовленості персоналу.

Конвергенція фінансового моніторингу та кібербезпеки може стати важливим завданням для українських банків у контексті забезпечення безпеки фінансових операцій та даних. Ось деякі можливі проблеми та виклики, з якими стикаються українські банки в цьому контексті:

1. Законодавча та регуляторна складність. Україна має специфічне законодавство щодо фінансового моніторингу та кібербезпеки, і воно може бути вельми складним та надзвичайно вимогливим. Банки повинні дотримуватися цих правил та стандартів, а також встановлювати власні заходи безпеки, щоб відповідати вимогам регуляторів.
2. Недостатні ресурси. Для впровадження конвергенції фінансового моніторингу та кібербезпеки банки повинні виділити достатні ресурси, включаючи фінансові, технічні та людські ресурси. Не всі банки можуть мати можливість витратити велику кількість коштів і часу на цей процес.
3. Кваліфікований персонал. Необхідно мати достатньо кваліфікований персонал, який розуміє як фінансовий моніторинг, так і кібербезпеку. Робота з обома аспектами вимагає різних навичок та знань, і банки повинні інвестувати в навчання свого персоналу.
4. Інтеграція існуючих систем. Багато українських банків вже мають існуючі системи фінансового моніторингу та кібербезпеки. Інтеграція цих систем та їх взаємодія може бути складною та вимагати додаткових зусиль та ресурсів.
5. Забезпечення конфіденційності даних. Збільшена інтеграція може вимагати обміну більшим обсягом даних між різними системами. Забезпечення конфіденційності цих даних та відповідність стандартам GDPR та інших регуляцій може бути складним завданням.
6. Моніторинг та аналіз даних. Після впровадження конвергенції банки повинні здійснювати ефективний моніторинг та аналіз даних для виявлення аномалій та кіберзагроз. Це вимагає великої кількості ресурсів та технологій аналітики даних.

7. Комплексність і реалізм. Впровадження конвергенції може бути складним завданням, і банки повинні бути реалістичними щодо своїх можливостей та ресурсів. Важливо створити план впровадження, який враховує поточні можливості та швидко зростаючі загрози.

Загалом, конвергенція фінансового моніторингу та кібербезпеки в українських банках може бути корисною, але вимагатиме великих зусиль та інвестицій для досягнення успіху. Банки повинні враховувати всі ці аспекти та виклики, щоб забезпечити надійну та ефективну систему безпеки.

У сучасному цифровому світі, де кіберзагрози стають все більшими і складнішими, конвергенція фінансового моніторингу та кібербезпеки стає надзвичайно важливою для боротьби з кібершахрайствами. Забезпечення безпеки фінансових операцій та захисту фінансових установ від кіберзагроз стає завданням високого пріоритету. Конвергенція цих двох областей дозволяє не лише виявляти та реагувати на кіберзагрози у реальному часі, але й попереджувати фінансові злочини, відмивання грошей, фінансування тероризму та інші незаконні дії. Вона сприяє покращенню безпеки фінансових операцій, зменшенню ризиків втрат, забезпечує відповідність законодавству та регуляціям, а також підвищує загальну ефективність моніторингу. Крім того, конвергенція допомагає забезпечити захист фінансових даних та конфіденційності клієнтів банків. Вона спрямована на забезпечення безпеки та надійності фінансових систем, що є важливим фактором довіри клієнтів та інвесторів.

У підсумку, конвергенція фінансового моніторингу та кібербезпеки є необхідною для захисту фінансових установ та їх клієнтів від кібершахрайств, забезпечення безпеки фінансових операцій та дотримання нормативів. Вона сприяє створенню більш безпечного і надійного фінансового середовища в умовах зростання обсягів кіберзагроз.

2.1.2.Оцінювання станів системи протидії фінансовим та кібершахрайствам

Сьогодні однією із пріоритетних завдань для українського суспільства є розробка механізму для захисту від внутрішніх загроз. Потреба у цьому механізмі посилюється через проведення війни з зовнішнім ворогом. Ця необхідність виникає з двох причин. З одного боку, існування військових конфліктів в країні призводить до збільшення привабливості країни для легалізації кримінальних доходів та фінансування тероризму. З іншого боку, зростає ймовірність кібершахрайських атак на різні об'єкти державної та недержавної інфраструктури. Збільшення кібератак відзначалося ще до початку військової агресії. Наприклад, 14 лютого 2022 року була зафіксована обширна атака на понад 70 урядових веб-сайтів (BBC, 2022), а 15 лютого 2022 року були атаковані банківські установи України (Euronews, 2022). За аналітичними даними, наданими DNS-платформою Quad9, у березні спостерігалося суттєве збільшення кібератак на українських громадян. З 121 мільйонах зловмисних подій, які мали місце в світі станом на 9 березня 2022 року, 4,6 мільйона були

пов'язані з Україною та Польщею, куди на початку березня 2022 року було переміщено 1,4 мільйона українських громадян (Krebsonsecurity, 2022).

Покрім атак на інформаційні системи населення України, також спостерігається випадки фінансового кібершахрайства. Наприклад, 14 квітня 2022 року було зафіксовано поширення банківського трояна «IcedID» з метою збору особистих банківських даних українців. У квітні 2022 року також виявлено випадки інтернет-шахрайства через фіктивні сторінки в соціальних мережах, де збиралася фінансова допомога з країн ЄС. Це вимагало від потерпілих сплачувати платежі з порушенням конфіденційності даних їх платіжних карток (згідно зі звітом CyberPeace Institute, 2022).

Надані приклади свідчать про актуальність проблеми боротьби з фінансовим та кібершахрайством і вимагають втручання на різних рівнях управління держави. Це потребує системного підходу, який включає в себе об'єднання зусиль у сферах боротьби з фінансовим та кібершахрайством, зокрема шляхом інтеграції інформаційних, технічних, програмних та організаційних ресурсів як на рівні держави в цілому, так і на рівні окремих суб'єктів господарювання. Наголошується, що необхідність такої конвергенції процесів у сферах протидії легалізації кримінальних доходів, фінансуванню тероризму, кібербезпеці та бізнесу визнана Office of Law Enforcement Support Financial Crimes Enforcement Network (FinCEN, 2009). Крім того, цю проблему також досліджують у своїх звітах світові консалтингові компанії Deloitte (Deloitte, 2019) та PwC (PwC, 2018).

Для оцінки готовності діючої системи протидії фінансовим та кібершахрайствам було зібрано та впорядковано вхідні дані з 76 країн світу за допомогою двох наборів показників. Перший набір оцінює рівень кібербезпеки в країні на національному та глобальному рівнях, а також вказує на рівень її цифрової та інформаційної трансформації. Другий набір показників аналізує умови, які можуть зробити країни привабливими для легалізації кримінальних доходів. Ці показники допомагають зрозуміти, наскільки ефективними є країни в боротьбі з фінансовими загрозами, пов'язаними з відмиванням коштів та фінансуванням тероризму на макрорівні. Перший набір показників включає такі 5 складових: глобальний індекс кібербезпеки, індекс розвитку інформаційно-комунікаційних технологій, індекс мережевої готовності, національний індекс кібербезпеки та рівень цифрового розвитку. Другий набір показників включає індекс політичної стабільності, індекс ефективності уряду, легкість ведення бізнесу, індекс злочинності, індекс сприйняття корупції, глобальний індекс тероризму та індекс фінансової таємниці.

Перші результати статистичного аналізу обраних показників наведено в таблиці 2.1.

При аналізі показників кібербезпеки виявлено, що лише три набори країн є однорідними, і це стосується індексу розвитку інформаційно-комунікаційних технологій, індексу мережевої готовності та рівня цифрового розвитку. Це обумовлено тим, що значення коефіцієнта варіації для цих наборів не перевищує припустимого рівня 33%. У разі глобального індексу кібербезпеки та

національного індексу кібербезпеки спостерігається нерівномірний розподіл серед 76 розглянутих країн світу.

Таблиця 2.1 – Результати первинного статистичного аналізу

Variable	Left Set	Right Set
Variance extracted	100.00%	86.67%
Total redundancy	65.51%	49.39%
Variable 1	Global Cybersecurity Index	Political Stability Index
Variable 2	ICT Development Index	Government Effectiveness Index
Variable 3	Network Readiness Index	Ease of Doing Business
Variable 4	National Cybersecurity Index	Crime Index
Variable 5	Digital Development Level	Corruption Perceptions Index
Variable 6	-	Global Terrorism Index
Variable 7	-	Financial Secrecy Index
Canonical R	0.91	
Chi-sqr(35)	196.50	
p	0.0000	

Джерело: розроблено на основі (Kuzmenko et al., 2023; Яровенко та ін., 2021)

Подальший аналіз показав, що найбільше поширене значення, яке незначно відрізняється від максимального, стосується глобального індексу кібербезпеки і становить 89. Це свідчить про високий рівень цього показника для більшості країн світу. Щодо інших чотирьох показників кібербезпеки, модальні значення розташовуються в діапазоні від 57 до 72 та перевищують середні значення. Аналогічно, глобальний індекс кібербезпеки має найвищий середній рівень, який становить 66,08%. Серед медіанних рівнів, тобто рівнів, які ділять множину країн навпіл, найнижче значення спостерігається для національного індексу кібербезпеки і становить 57.

При аналізі основних статистичних показників другої групи можна зазначити, що серед семи розглянутих показників лише один, а саме "легкість ведення бізнесу," показує однорідність вибірки з 76 країн світу. Усі інші показники виявляють значну нерівномірність, оскільки коефіцієнт варіації коливається від 33,87% (у випадку індексу злочинності) до 241,37% (за індексом політичної стабільності). Модальне значення спостерігається лише для індексу політичної стабільності та глобального індексу тероризму. У разі всіх інших п'яти показників значення досить різноманітні.

Отримана нерівномірність вибірки пов'язана з різним рівнем економічного розвитку країн, які були включені до дослідження. Тому для визначення причинно-наслідкових зв'язків між показниками кібербезпеки та показниками, що визначають спроможність країн боротися з фінансовими злочинами, потрібно провести канонічний аналіз. Цей аналіз був здійснений за допомогою аналітичного пакету Statistica, і його результати представлені в таблиці 2.2.

Аналіз результатів показує, що більшість варіації в наборі показників кібербезпеки (65,51%) може бути пояснена за допомогою набору показників, що оцінюють спроможність країн боротися з фінансовими злочинами. З іншого боку, тільки 49,39% варіації в наборі показників, які оцінюють спроможність країн боротися з фінансовими загрозами, може бути пояснена за допомогою

набору показників кібербезпеки. Тобто, показники, що вказують на здатність країн протидіяти фінансовим і кіберзагрозам, грають більш важливу роль і впливають на показники кібербезпеки.

Таблиця 2.2 – Результати канонічного аналізу

Root Removed	Canonical R	Canonical R-sqr	Chi-sqr.	df	p	Lambda Prime
0	0.9126	0.8328	196.4981	35	0.0000	0.0568
1	0.6730	0.4530	73.9741	24	0.0000	0.3396
2	0.5662	0.3206	32.6488	15	0.0053	0.6209
3	0.2727	0.0744	6.1705	8	0.6281	0.9139
4	0.1128	0.0127	0.8765	3	0.8311	0.9873

Джерело: розроблено на основі (Kuzmenko et al., 2023; Яровенко та ін., 2021)

Крім того, 100% варіативності в наборі показників кібербезпеки пояснюється самим набором показників кібербезпеки, в той час як 86,67% варіативності в наборі показників, що оцінюють спроможність країн боротися з фінансовими загрозами, може бути пояснено цим набором.

Значущість канонічної кореляції підтверджується статистичними значеннями, такими як Chi-Square=196,5 та рівень значущості p=0,00, що свідчить про наявність сильної залежності між групами змінних.

Для оптимізації обсягу вхідних даних ми провели аналіз кореляції між обома наборами показників – тими, що оцінюють кібербезпеку та тими, що характеризують спроможність країн боротися з фінансовими і кібершахрайствами. У таблиці 2.3 подана кореляційна матриця показників кібербезпеки. Отримані дані вказують на значну кореляційну залежність між індексом розвитку інформаційно-комунікаційних технологій та рівнем цифрового розвитку, де значення коефіцієнта кореляції становить 0,96. Для оптимізації множини вхідних показників, що стосуються характеристик кібербезпеки, рекомендується вилучити один із індикаторів, які мають високий рівень колінеарності, з подальших розрахунків.

Таблиця 2.3 – Кореляційна матриця множини показників кібербезпеки

Variables	GCI	ICT DI	NRI	NCSI	DDL
GCI	1.0000	0.5358	0.7114	0.7094	0.5792
ICT DI	0.5358	1.0000	0.5834	0.6430	0.9607
NRI	0.7114	0.5834	1.0000	0.6813	0.6467
NCSI	0.7094	0.6430	0.6813	1.0000	0.6547
DDL	0.5792	0.9607	0.6467	0.6547	1.0000

Джерело: розроблено на основі (Kuzmenko et al., 2023; Яровенко та ін., 2021)

Для вирішення, який із показників слід залишити в масиві вхідних даних, а який вилучити, розглянемо факторну структуру, сконцентруючись на перших трьох статистично значущих канонічних коренях, визначених на основі шматково-лінійного графіку та результатів тестів Chi-Square (див. таблицю 2.4).

Таблиця 2.4 – Факторна структура множини показників кібербезпеки

Variables	Root 1	Root 2	Root 3	Root 4	Root 5
GCI	0.7935	-0.5738	0.0325	-0.1962	-0.0389
ICT DI	0.8712	0.1721	-0.3910	0.2355	-0.0550
NRI	0.8026	-0.2408	0.3794	0.3538	0.1697
NCSI	0.7257	-0.2962	-0.2189	0.0341	0.5801
DDL	0.9428	0.2574	-0.1977	0.0756	0.0015

Джерело: розроблено на основі (Kuzmenko et al., 2023; Яровенко та ін., 2021)

За результатами аналізу даних, наведених у таблиці 2.4, можна зазначити, що найбільший вплив спостерігається у відношенні до показника "рівень цифрового розвитку". Тому рекомендується залишити цей показник для подальших обчислень.

Проведемо аналіз кореляційної матриці, яка включає в себе показники, що характеризують спроможність країн протидіяти фінансовим і кібершахрайствам (див. Таблиця 2.5). За отриманими даними можна зробити висновок про значну кореляційну залежність між двома показниками: індекс ефективності уряду та індекс сприйняття корупції. Підтвердженням цьому є значення коефіцієнта кореляції на рівні 0,904. З метою оптимізації множини вхідних показників, що стосуються спроможності країн протидіяти фінансовим і кібершахрайствам, рекомендується виключити один із колінеарних показників для подальших обчислень.

Таблиця 2.5 – Кореляційна матриця показників спроможності країн протидіяти фінансовим і кібершахрайствам

Variables	PSI	GEI	EDB	CI	CPI	GTI	FSI
PSI	1.0000	0.6575	0.4557	-0.4952	0.7503	-0.6489	0.1353
GEI	0.6575	1.0000	0.8029	-0.6215	0.9037	-0.0476	0.4352
EDB	0.4557	0.8029	1.0000	-0.5826	0.6465	0.0023	0.2687
CI	-0.4952	-0.6215	-0.5826	1.0000	-0.5570	0.1732	-0.2272
CPI	0.7503	0.9037	0.6465	-0.5570	1.0000	-0.1809	0.3449
GTI	-0.6489	-0.0476	0.0023	0.1732	-0.1809	1.0000	0.2143
FSI	0.1353	0.4352	0.2687	-0.2272	0.3449	0.2143	1.0000

Джерело: розроблено на основі (Kuzmenko et al., 2023; Яровенко та ін., 2021)

Для ухвалення рішення щодо включення чи виключення показника (конкретно індекс ефективності уряду та індекс сприйняття корупції) в масиві вхідних даних розглянемо факторну структуру, зосереджуючись на перших трьох статистично значущих канонічних коренях (див. таблиця 2.6).

З аналізу даних таблиці 2.6 видно, що більший вплив здійснюється завдяки показнику "індекс ефективності уряду", і тому рекомендується залишити його в масиві вхідних даних для подальших обчислень.

Для оцінки зрілості діючої системи протидії фінансовим і кібершахрайствам заплановано провести кілька послідовних етапів.

Таблиця 2.6 – Факторна структура показників спроможності країн протидіяти фінансовим і кібершахрайствам

Variables	Root 1	Root 2	Root 3	Root 4	Root 5
PSI	0.4314	0.6131	-0.5319	0.1180	0.0254
GEI	0.9545	0.1915	-0.1801	0.0406	-0.1027
EDB	0.8542	-0.2170	-0.2463	0.1014	0.2660
CI	-0.5569	0.0130	0.6724	-0.1198	-0.1878
CPI	0.8162	0.5048	-0.2211	-0.1246	-0.0019
GTI	0.1495	-0.6210	0.3207	-0.6026	-0.2745
FSI	0.5055	0.0899	0.3227	-0.3200	0.2829

Джерело: розроблено на основі (Kuzmenko et al., 2023; Яровенко та ін., 2021)

На першому етапі передбачено зведення індикативних показників в єдиний інтегральний індекс кібербезпеки, використовуючи методику Сундаровського. Цей процес включає застосування формули (2.1), яка дозволяє об'єднати різні показники в один комплексний показник кібербезпеки (Kuzmenko et al., 2023; Яровенко та ін., 2021):

$$IS_j = \prod_{i=1}^{n} \left[a_{ij} - a_i^*\right]^{\alpha} \tag{2.1}$$

де IS_j – інтегральний індекс кібербезпеки для j-ої країни;

a_{ij} – фактичне значення і-го показника кібербезпеки для j-ої країни;

a_i^*- рівноважне значення і-го показника кібербезпеки для розглянутої множини країн;

α – константа, показник ступеня (Kuzmenko et al., 2023; Яровенко та ін., 2021).

Для практичного використання формули (2.1) та для розрахунку інтегрального індексу кібербезпеки зробимо наступні припущення:

Оберемо абсолютне значення різниці між середньоквадратичним відхиленням та мінімально допустимим рівнем як рівноважні рівні складових індикаторів за формулою (2.2) (Kuzmenko et al., 2023; Яровенко та ін., 2021):

$$a_i^* = \left|\min_j a_{ij} - \sigma_i\right| = \left|\min_j a_{ij} - \sqrt{\frac{\sum_{j=1}^{m}\left(a_{ij} - \bar{a}_\iota\right)}{n-1}}\right| \tag{2.2}$$

де σ_i – середньоквадратичне відхилення і-го показника кібербезпеки;

$\bar{a}_\iota$ – середнє арифметичне значення і-го показника кібербезпеки (Kuzmenko et al., 2023; Яровенко та ін., 2021);

2) використовуватимемо постійне значення показника ступеня функціональної залежності (2.1) як співвідношення одиничного значення до кількості релевантних показників кібербезпеки. З урахуванням зазначених

припущень, формула (2.1) буде мати наступний вигляд (2.3) (Kuzmenko et al., 2023; Яровенко та ін., 2021):

$$IS_j = \prod_{i=1}^{n} \left[a_{ij} - \left| \min_j a_{ij} - \sqrt{\frac{\sum_{j=1}^{m} \left(a_{ij} - \bar{a}_{\iota} \right)}{n-1}} \right| \right]^{1/n} \quad (2.3)$$

де n - кількість релевантних показників характеристики кібербезпеки (Kuzmenko et al., 2023; Яровенко та ін., 2021).

Другий етап передбачає визначення показників, які є важливими для оцінки спроможності країн протидіяти фінансовим шахрайствам. Цей відбір показників виконується за допомогою методу сигма-обмеженої параметризації та Парето-оптимізації. У якості результативної ознаки використовується інтегральний індекс кібербезпеки, розрахований за методом Сундаровського, а факторами впливу є показники, які відображають спроможність країн протидіяти фінансовим та кіберзагрозам. Сигма-обмежена параметризація включає в себе одномірний тест значущості впливу цих показників на результативний фактор. Парето-оптимізація включає в себе побудову діаграми Парето t-значень для оцінки важливості кожного показника.

На третьому етапі проводиться створення нелінійної регресійної моделі, яка визначає залежність інтегрального індексу кібербезпеки від релевантних предикторів, виявлених на попередньому етапі. Цей процес включає послідовне виключення параметрів, які не є статистично значущими. У цьому процесі враховуються різноманітні функційні залежності, такі як логарифмічні, квадратичні та мультиплікативні, між вибраними показниками. Все це необхідно для подальшого проведення біфуркаційного аналізу ступеня зрілості діючої системи протидії фінансовим та кібершахрайствам та створення їх фазових портретів.

Четвертий етап передбачає проведення біфуркаційного аналізу для визначення ступеня зрілості системи протидії фінансовим та кібершахрайствам і створення фазових портретів, що відображають рівень "зрілості" і "релаксаційних коливань втрати стійкості". Для виконання цього етапу необхідно здійснити проміжні обчислення з використанням методів диференційного числення. Ці обчислення включають в себе знаходження часткових похідних від функції, яка описує залежність інтегрального індексу кібербезпеки від релевантних предикторів. На основі цих похідних створюється система диференційних рівнянь, які становлять основу для подальшого дослідження динамічної стійкості розглянутої системи.

П'ятий етап включає в себе створення нелінійної регресійної моделі, що описує взаємозв'язок між інтегральним індексом кібербезпеки та релевантними предикторами. Ця модель базується на поєднанні степеневої, тригонометричної та мультиплікативної функцій з метою подальшого проведення аналізу біфуркації для визначення ступеня зрілості системи протидії фінансовим та

кібершахрайствам та побудови фазових портретів, які відображають "стані рівноваги".

На шостому етапі проводиться біфуркаційний аналіз для оцінки зрілості системи протидії фінансовим та кібершахрайствам та побудови фазових портретів "станів рівноваги". Для виконання цього етапу потрібно спершу провести проміжні обчислення з використанням інструментів диференціального числення, включаючи обчислення часткових похідних функції, що визначає залежність інтегрального індексу кібербезпеки від вибраних релевантних предикторів. Ці обчислення стануть основою для подальшого дослідження динамічної стійкості розглянутої системи.

На першому етапі було проведено обчислення за допомогою форм. (2.3).

На другому етапі використано аналітичний пакет Statistica для виконання сигма-обмеженої параметризації та Парето-оптимізації. Результати цих обчислень проілюстровано на рисунках 2.1 і 2.2.

Univariate Tests of Significance for IS (Spreadsheet1.sta)
Sigma-restricted parameterization
Effective hypothesis decomposition

Effect	SS	Degr. of Freedom	MS	F	p
Intercept	15,932	1	15,932	0,19911	0,656838
Political stability index	60,262	1	60,262	0,75310	0,388504
Government effectiveness index	651,476	1	651,476	8,14157	0,005706
Ease of doing business	1068,591	1	1068,591	13,35430	0,000499
Crime Index	197,796	1	197,796	2,47187	0,120474
Global Terrorism Index	185,399	1	185,399	2,31695	0,132540
Financial Secrece Index	63,668	1	63,668	0,79566	0,375494
Error	5521,278	69	80,019		

Рисунок 2.1 – Одномірний тест значущості впливу показників спроможності країн протидіяти фінансовим шахрайствам на інтегральний індекс кібербезпеки

Джерело: розроблено на основі (Kuzmenko et al., 2023; Яровенко та ін., 2021)

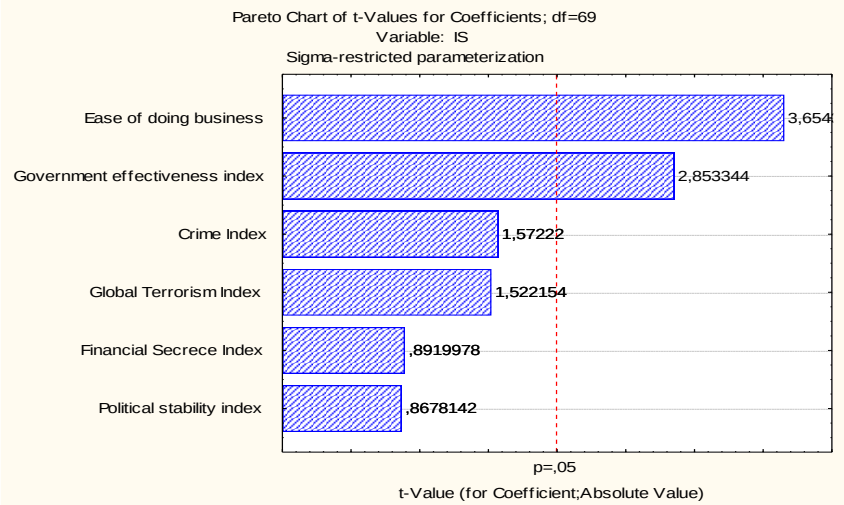


Рисунок 2.2 – Діаграма Парето t-значень значущості впливу показників спроможності країн протидіяти фінансовим шахрайствам на інтегральний індекс кібербезпеки

Джерело: розроблено на основі (Kuzmenko et al., 2023; Яровенко та ін., 2021)

На основі даних рисунку 2.2 можна зазначити, що статистично значущими є лише два впливи: індекс ефективності уряду та легкість ведення бізнесу, оскільки їхні рівні значущості за критерієм Фішера менше 0,05. Найбільший внесок в загальну модель вносить показник "легкість ведення бізнесу", оскільки сума квадратів відхилень SS, яка становить 1068,59, має найбільше значення, а рівень значущості p приймає найменше значення, а саме 0,000499. Другим статистично значущим впливом є "індекс ефективності уряду", для якого SS=651,48, а рівень значущості p становить 0,0057. На третьому місці за пріоритетністю знаходиться показник спроможності країн протидіяти фінансовим шахрайствам, хоча для цього показника рівень значущості p становить 0,12. Графічної ілюстрацією важливості розглянутих факторів є діаграма Парето t-значень, яка підтверджує значущість впливу показників спроможності країн протидіяти фінансовим загрозам на інтегральний індекс кібербезпеки (рисунок 2.2). Отримана діаграма Парето не лише визначає статистично значущі впливи (регресори) на інтегральний індекс кібербезпеки, але й систематизує їх в порядку від найбільшого до найменшого впливу. Цей статистичний інструментарій ілюструє правило 80 на 20, виділяючи 80% найбільш важливих факторів зовнішнього середовища, включаючи індекс ефективності уряду, легкість ведення бізнесу, індекс злочинності, які є важливими і обрані для подальшого дослідження.

Для здійснення третього етапу, потрібно визначити специфікацію нелінійної регресійної залежності між інтегральним індексом кібербезпеки та релевантними предикторами: індексом ефективності уряду, легкістю ведення бізнесу та індексом злочинності. Для цього ми використовуємо можливості програмного пакету Statistica. За допомогою методу покрокового включення було виявлено наявність статистично значущих залежностей у вигляді квадратного кореня для індексу ефективності уряду, логарифмічної залежності для показника легкості ведення бізнесу та квадратичної залежності для показника індексу злочинності (рисунок 2.3). У відношенні до індексу ефективності уряду, через від'ємні значення вихідних статистичних даних, розглядається зв'язок інтегрального індексу кібербезпеки лише у формі мультиплікативної залежності.

Regression Summary for Dependent Variable: IS (Spreadsheet1.sta)
R= ,80929115 R?= ,65495216 Adjusted R?= ,62891081
F(4,53)=25,150 p<,00000 Std.Error of estimate: 9,2027

N=58	Beta	Std.Err. of Beta	B	Std.Err. of B	t(53)	p-level
Intercept			-229,789	67,41833	-3,40840	0,001255
LN-V9	0,421814	0,111687	61,729	16,34451	3,77675	0,000404
SQRV8	0,401105	0,126867	17,088	5,40484	3,16163	0,002595
V10**2	-0,187681	0,088620	-0,003	0,00128	-2,11782	0,038898
1/V8	0,150132	0,093801	0,172	0,10727	1,60054	0,115423

Рисунок 2.3 – Результати регресійної статистики залежності інтегрального індексу кібербезпеки від релевантних предикторів: індексу ефективності уряду, легкості ведення бізнесу, індексу злочинності

Джерело: розроблено на основі (Kuzmenko et al., 2023; Яровенко та ін., 2021)

Враховуючи результати визначення зв'язку між інтегральним індексом кібербезпеки та відповідними предикторами, які включають логарифмічні, квадратичні та мультиплікативні функції трьох показників, проведемо формалізацію наведеної нелінійної залежності. Отримані результати будуть представлені у вигляді таблиці 2.7.

Таблиця 2.7 – Результати статистичного аналізу залежності інтегрального індексу кібербезпеки від релевантних предикторів

Specification	Coefficients	Standard error	t-statistics	P-value	Lower 95%	Upper 95%
Y- cross section	-108,6929	56,5889	-1,9207	0,0587	-221,5009	4,1151
ln(EDI)	35,3774	13,2591	2,6682	0,0094	8,9459	61,8089
CI^2	-0,0019	0,0012	-1,6080	0,1122	-0,0042	0,0005
GEI*EDI*CI	0,0028	0,0008	3,5848	0,0001	0,0012	0,0043

Джерело: розроблено на основі (Kuzmenko et al., 2023; Яровенко та ін., 2021)

Дані таблиці 2.7 дозволили отримати наступну регресійну модель у вигляді формули (2.4) (Kuzmenko et al., 2023; Яровенко та ін., 2021):

$$IS = -108.69 + 35.3774 \cdot \ln(EDI) - 0.00188 \cdot CI^2 + 0.00277 \cdot GEI \cdot EDI \cdot CI \quad (2.4)$$

де IS – інтегральний індекс кібербезпеки;

GEI - індекс ефективності уряду,

EDI – легкість ведення бізнесу,

CI - індекс злочинності (Kuzmenko et al., 2023; Яровенко та ін., 2021).

Статистичну значущість показників ln(EDI) та GEI*EDI*CI підтверджено з рівнем p менше рівня 0,05 та показника CI^2 з рівнем p=0,11. Коефіцієнт детермінації для даної моделі складає 62,73%, фактичне значення критерію Фішера на рівні 40,40 перевищує критично допустимий рівень.

Для виконання четвертого етапу був використаний набір прикладних програм MathCAD. Основою подальшого вивчення динамічної стійкості системи боротьби з фінансовими та кібершахрайствами та побудови фазових портретів їх "зрілості" та "релаксаційних коливань втрати стійкості" є нелінійна функція (2.5), яка отримана на основі нелінійної моделі (2.4) (Kuzmenko et al., 2023; Яровенко та ін., 2021):

$$f(gei, edi, ci) := -108.693 + 35.37739 \cdot \ln(edi) - 0.00188 \cdot ci^2 + 0.002774 \cdot gei \cdot edi \cdot ci \quad (2.5)$$

За допомогою функції (2.5) ми створимо модель системи диференціальних рівнянь (2.6), які описують поведінку динамічної системи для протидії фінансовим та кібершахрайствам (Kuzmenko et al., 2023; Яровенко та ін., 2021):

$$\frac{d}{dgei} f(gei, edi, ci) \rightarrow 0.002774 \cdot ci \cdot edi$$
$$\frac{d}{dedi} f(gei, edi, ci) \rightarrow \frac{35.37739}{edi} + 0.002774 \cdot ci \cdot gei \quad (2.6)$$

$$\frac{d}{dci} f(gei, edi, ci) \rightarrow -0.00376ci + 0.002774edi \cdot gei$$

Представлені три диференційні рівняння (2.6) дозволяють встановити взаємозв'язки між змінними GEI (індекс ефективності уряду), EDI (легкість ведення бізнесу), CI (індекс злочинності) та їх першими частковими похідними $\frac{d}{dgei} f(gei, edi, ci), \frac{d}{dedi} f(gei, edi, ci), \frac{d}{dci} f(gei, edi, ci)$ (Kuzmenko et al., 2023; Яровенко та ін., 2021).

Використовуючи нелінійний підхід, який ґрунтується на теорії біфуркацій, ми створимо "фазові портрети" для інтегрального індексу кібербезпеки. Ці портрети представляють собою відображення траєкторій у фазовому просторі, які розглядаються в попарних площинах: індекс ефективності уряду - легкість ведення бізнесу, легкість ведення бізнесу - індекс злочинності, індекс ефективності уряду - індекс злочинності. Створення рівнянь (2.7) виконано за допомогою програмного забезпечення для математичного аналізу MathCad (Kuzmenko et al., 2023; Яровенко та ін., 2021).

$$\begin{aligned}
&Faza(gei0, edi0, ci0, dt, N) := \left| \begin{array}{l}
\left(gei_0 \leftarrow gei0 \quad edi_0 \leftarrow edi0 \quad ci_0 \leftarrow ci0\right) \\
\text{for } k \in 0..N \\
\quad \left| \begin{array}{l}
fff \leftarrow f\left(gei_k, edi_k, ci_k\right) \\
gei_{k+1} \leftarrow \left[gei_k + dt \cdot \left(0.002774ci_k \cdot edi_k\right)\right] \\
edi_{k+1} \leftarrow \left[edi_k + dt \cdot \left(\frac{35.37739}{edi_k} + 0.002774ci_k \cdot gei_k\right)\right] \\
ci_{k+1} \leftarrow \left[ci_k + dt \cdot \left(-0.00376ci_k + 0.002774edi_k \cdot gei_k\right)\right]
\end{array} \right. \\
(gei \quad edi \quad ci)
\end{array} \right. \\
&(gei1 \quad edi1 \quad ci1) := Faza(1.6, 80, 42, 0.01, 100) \\
&(gei2 \quad edi2 \quad ci2) := Faza(1.45, 78, 20, 0.01, 100) \\
&(gei3 \quad edi3 \quad ci3) := Faza(0.18, 68, 36, 0.01, 100) \\
&(gei4 \quad edi4 \quad ci4) := Faza(0.43, 56, 51, 0.01, 100) \\
&(gei5 \quad edi5 \quad ci5) := Faza(-0.32, 50, 52, 0.01, 100) \\
&(gei6 \quad edi6 \quad ci6) := Faza(-0.45, 57, 70, 0.01, 100)
\end{aligned} \tag{2.7}$$

Для забезпечення візуалізації формули (2.7), яка представляє собою фазовий портрет системи боротьби з фінансовими та кібершахрайствами, і для подальшої ідентифікації її типу, як одного з можливих альтернатив (сідло, вузол чи фокус), розглянемо різні варіації можливих значень як для факторів (індекс ефективності уряду, легкість ведення бізнесу, індекс злочинності), так і для значень функції інтегрального індексу кібербезпеки з вказаною точністю на основі заданої кількості точок реалізації, як показано в формулі 2.8 (Kuzmenko et al., 2023; Яровенко та ін., 2021).

$$\begin{aligned}
&(gei1 \quad edi1 \quad ci1) := Faza(1.6, 80, 42, 0.01, 100) \\
&(gei2 \quad edi2 \quad ci2) := Faza(1.45, 78, 20, 0.01, 100) \\
&(gei3 \quad edi3 \quad ci3) := Faza(0.18, 68, 36, 0.01, 100) \\
&(gei4 \quad edi4 \quad ci4) := Faza(0.43, 56, 51, 0.01, 100) \\
&(gei5 \quad edi5 \quad ci5) := Faza(-0.32, 50, 52, 0.01, 100) \\
&(gei6 \quad edi6 \quad ci6) := Faza(-0.45, 57, 70, 0.01, 100)
\end{aligned} \tag{2.8}$$

Підставивши реальні значення вхідних даних (формули 2.8) в вирази, які дозволяють формалізувати фазові портрети (2.7), ми отримаємо нелінійну залежність інтегрального індексу кібербезпеки від відповідних факторів у двох площинах: "індекс ефективності уряду - легкість ведення бізнесу" (показано на лівому фрагменті рисунку 2.4) та "легкість ведення бізнесу - індекс злочинності" (показано на правому фрагменті рисунку 2.4) для ілюстрації (перше відношення у формулах 2.8).

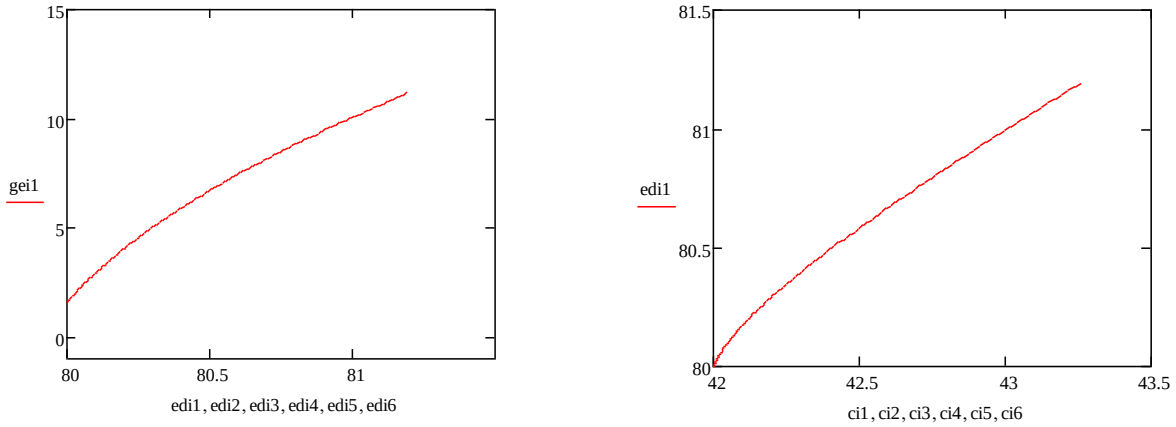


Рисунок 2.4 – Криві нелінійної залежності інтегрального індексу кібербезпеки від релевантних факторів у площинах «індекс ефективності уряду - легкість ведення бізнесу» (лівий фрагмент) та «легкість ведення бізнесу - індекс злочинності» (правий фрагмент)

Джерело: розроблено на основі (Kuzmenko et al., 2023; Яровенко та ін., 2021)

Проведемо аналіз фазового портрету динамічної системи для протидії фінансовим та кібершахрайствам, розглядаючи всі можливі комбінації вхідних показників (згідно з формулою 2.8). Розглянемо спочатку фрагмент фазового портрету цієї системи в контексті площини "індекс ефективності уряду - легкість ведення бізнесу" (рисунок 2.5). Даний фрагмент фазового портрету показує тип біфуркації, який характеризується як "нестійкий фокус," що свідчить про нерівноважний стан системи. При суттєвій зміні одного параметра за фіксованому значенні іншого параметра розглянута система перебуває в нерівноважному стані.

Перехід до аналізу фрагменту фазового портрету динамічної системи для протидії фінансовим та кібершахрайствам в площині "легкість ведення бізнесу - індекс злочинності" (зображено на рисунку 2.6) показує, що система перебуває в нерівноважному стані, який можна охарактеризувати як "нестійкий фокус."

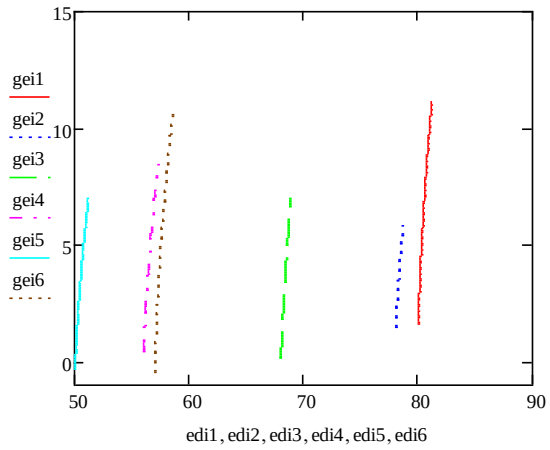


Рисунок 2.5 – Фрагмент фазового портрету «нестійкий фокус» динамічної системи протидії фінансовим та кібершахрайствам, що знаходиться в нерівноважному стані, в розрізі площини «(індекс ефективності уряду - легкість ведення бізнесу»

Джерело: розроблено на основі (Kuzmenko et al., 2023; Яровенко та ін., 2021)

Слід зазначити, що нерівноважний стан динамічної системи для протидії фінансовим та кібершахрайствам у формі фазового портрету, який можна охарактеризувати як "нестійкий вузол," також відзначається в розрізі площини "індекс ефективності уряду - індекс злочинності," як показано на рисунку 2.7.

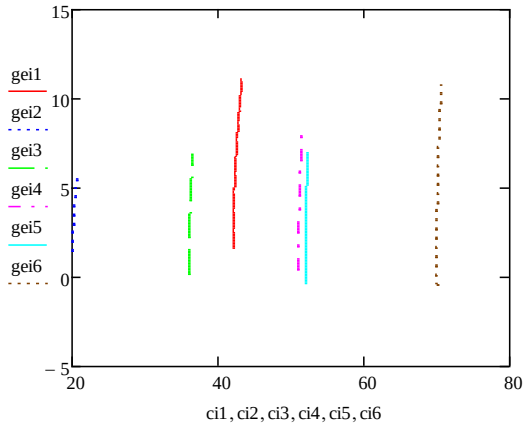


Рисунок 2.6 – Фрагмент фазового портрету «нестійкий фокус» динамічної системи протидії фінансовим та кібершахрайствам, що знаходиться в нерівноважному стані, в розрізі площини «легкість ведення бізнесу - індекс злочинності»

Джерело: розроблено на основі (Kuzmenko et al., 2023; Яровенко та ін., 2021)

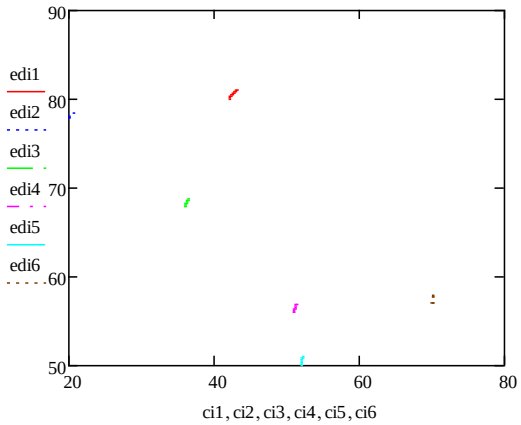


Рисунок 2.7 – Фрагмент фазового портрету «нестійкий вузол» динамічної системи протидії фінансовим та кібершахрайствам, що знаходиться в нерівноважному стані, в розрізі площини «індекс ефективності уряду - індекс злочинності»

Джерело: розроблено на основі (Kuzmenko et al., 2023; Яровенко та ін., 2021)

Проведений біфуркаційний аналіз щодо системи для протидії фінансовим та кібершахрайствам та побудова фазових портретів, які відображаються у вигляді "нестійкого фокусу" та "нестійкого вузла" (рисунки 2.5-2.7), свідчать про те, що ця система перебуває в нерівноважному стані.

Для реалізації п'ятого етапу необхідно встановити характер нелінійної регресійної залежності інтегрального індексу кібербезпеки від релевантних предикторів, таких як індекс ефективності уряду, легкість ведення бізнесу та індекс злочинності. Ми розглянемо специфікацію, починаючи з індексу ефективності уряду. Як результативну ознаку ми обрали інтегральний індекс кібербезпеки, що був визначений за методом Сундаровського. Факторні залежності індексу ефективності уряду включають поліноміальну залежність (другого і третього ступеня), обернену залежність та тригонометричну функцію. Результати регресійного аналізу наведені в таблиці 2.8.

Таблиця 2.8 – Результати статистичного аналізу залежності інтегрального індексу кібербезпеки від індексу ефективності уряду

Specification	Coefficients	Standard error	t-statistics	P-value	Lower 95%	Upper 95%
Y- cross section	47,8568	43,4523	1,1014	0,2746	-38,8281	134,5417
GEI*EDI*CI	0,0004	0,0015	0,2402	0,8109	-0,0026	0,0033
GEI^2	-5,1192	18,2560	-0,2804	0,7800	-41,5390	31,3006
GEI^3	1,7633	2,0450	0,8623	0,3915	-2,3163	5,8428
1/GEI	0,08037	0,09631	0,83447	0,40690	-0,1118	0,2725
Sin(GEI)	14,1229	6,3637	2,21929	0,0298	1,4276	26,8182
Cos(GEI)	-16,8569	43,9954	-0,3832	0,7028	-104,6252	70,9114

Джерело: розроблено на основі (Kuzmenko et al., 2023; Яровенко та ін., 2021)

Згідно із даними таблиці 2.8, зокрема графою P-рівня, можна констатувати, що змінна sin(GEI) є статистично значущою. Це підтверджується тим, що P-рівень становить 0,0298, що менше встановленого порогового значення 0,05. З

цієї причини наступним кроком у специфікації залежності інтегрального індексу кібербезпеки від індексу ефективності уряду рекомендується використовувати синусоїду для подальших обчислень.

Визначимо, як і в попередньому випадку, специфікацію нелінійної залежності інтегрального індексу кібербезпеки від іншої релевантної ознаки, а саме - легкості ведення бізнесу. Для цього, ми також використовуємо інтегральний індекс кібербезпеки, який був визначений методом Сундаровського, в ролі результативної ознаки. Щодо факторних ознак, ми розглядаємо поліноміальні залежності другого і третього ступеня, обернену залежність, логарифмічну залежність, квадратний корінь, а також тригонометричні залежності легкості ведення бізнесу. Використовуючи метод регресійного аналізу, ми отримаємо результат, який буде представлений в таблиці 2.9.

За результатами аналізу таблиці 2.9 (графа P-значення) можна зазначити, що немає жодної змінної, яка була б статистично значущою на рівні значущості менше 0,05. Проте варто відзначити, що рівень значущості для кубічної залежності результативної ознаки від змінної "легкість ведення бізнесу" найменший і становить 0,1773. Тому для подальших обчислень рекомендується використовувати кубічну залежність інтегрального індексу кібербезпеки від показника "легкість ведення бізнесу".

Давайте визначимо специфікацію нелінійної залежності інтегрального індексу кібербезпеки від третьої релевантної ознаки, якою є індекс злочинності. Для цього проведемо аналіз, де інтегральний індекс кібербезпеки, розрахований методом Сундаровського, виступає як результативна ознака, а індекс злочинності представляється поліноміальною (другого і третього ступеня), оберненою, або тригонометричною функціями. Отримані результати аналізу будуть наведені в таблиці 2.10.

Таблиця 2.9 – Результати статистичного аналізу залежності інтегрального індексу кібербезпеки від легкості ведення бізнесу

Specification	Coefficients	Standard error	t-statistics	P-value	Lower 95%	Upper 95%
Y-cross section	-215579,91	167427,76	-1,29	0,20	-549676,79	118516,97
EDI2	5,39	4,03	1,34	0,19	-2,65	13,44
EDI3	-0,02	0,01	-1,36	0,18	-0,05	0,01
1/EDI	890050,46	692798,38	1,28	0,20	-492407,17	2272508,10
ln(EDI)	99794,06	77102,97	1,29	0,20	-54062,51	253650,63
EDI0,5	-28814,34	22124,27	-1,30	0,20	-72962,64	15333,95
Sin(EDI)	0,24	1,78	0,14	0,89	-3,31	3,80
Cos(EDI)	0,86	1,62	0,53	0,60	-2,36	4,08

Джерело: розроблено на основі (Kuzmenko et al., 2023; Яровенко та ін., 2021)

Таблиця 2.10 – Результати статистичного аналізу залежності інтегрального індексу кібербезпеки від індексу злочинності

Specifica-tion	Coefficients	Standard error	t-statistics	P-value	Lower 95%	Upper 95%
Y-cross section	7828,5624	5651,8474	1,3851	0,1705	-3449,5235	19106,6480
CI2	-0,5685	0,4027	-1,4118	0,1626	-1,3721	0,2351
CI3	0,0027	0,0019	1,3904	0,1690	-0,0012	0,0065
1/CI	-24362,1135	18011,5098	-1,3526	0,1807	-60303,5216	11579,2940
ln(CI)	-4624,8443	3329,8799	-1,3889	0,1694	-11269,5160	2019,8275
CI0,5	1679,5597	1203,4889	1,3956	0,1674	-721,9651	4081,0845
Sin(CI)	-3,2419	2,3552	-1,3765	0,1732	-7,9416	1,4579
Cos(CI)	5,7206	2,3725	2,4112	0,0186	0,9864	10,4549

Джерело: розроблено на основі (Kuzmenko et al., 2023; Яровенко та ін., 2021)

На основі результатів, представлених в таблиці 10 (графа P-значення), можна прийти до висновку, що змінна Cos(CI) має статистичну значущість, оскільки значення P-рівня становить 0,0186, що менше за прийнятий поріг 0,05. Тому в подальших обчисленнях для специфікації залежності інтегрального індексу кібербезпеки від індексу злочинності рекомендується використовувати косинусоїду.

Отже, після визначення специфікації залежності інтегрального індексу кібербезпеки від релевантних предикторів (індекс ефективності уряду, легкість ведення бізнесу, індекс злочинності) у формі синусоїди, кубічної залежності і косинусоїди відповідно, а також враховуючи додаткову змінну мультиплікативного впливу на результативну ознаку всіх трьох релевантних факторів, ми створили нелінійну регресійну залежність. Отримані результати представлені в табличному форматі в таблиці 2.11.

Таблиця 2.11 – Результати статистичного аналізу залежності інтегрального індексу кібербезпеки від релевантних предикторів

Specification	Coefficient	Standard error	t-statistics	P-value	Lower 95%	Upper 95%
Y-cross section	10,8979	4,1283	2,6398	0,0102	2,6663	19,1294
Sin(GEI)	9,9771	5,0902	1,9601	0,0539	-0,1724	20,1266
EDI3	0,0001	0,0000	5,6383	0,0000	0,0001	0,0001
Cos(CI)	3,4013	1,6051	2,1191	0,0376	0,2009	6,6017
GEI*EDI*CI	-0,0006	0,0012	-0,4738	0,6371	-0,0030	0,0018

Джерело: розроблено на основі (Kuzmenko et al., 2023; Яровенко та ін., 2021)

На основі інформації, представленої у графі "Коефіцієнти" таблиці 2.11, будемо встановлювати регресійну залежність інтегрального індексу кібербезпеки від релевантних предикторів: індекс ефективності уряду, легкість ведення бізнесу, індекс злочинності. Ця залежність буде виражена у наступному рівнянні (2.9) (Kuzmenko et al., 2023; Яровенко та ін., 2021):

$$IS = 10{,}8989 + 9{,}9771 \cdot \sin(GEI) + 0.00008 \cdot EDI^3 + 3.4013 \cdot \cos(CI) - 0.00057 \cdot GEI \cdot EDI \cdot CI \quad (2.9)$$

Достовірність і точність рівняння (2.9) були перевірені за допомогою наступних критеріїв. Значення коефіцієнтів змінних є статистично значущими, оскільки значення рівня значущості (p-рівня) менше 0,05, за винятком коефіцієнта перед змінною мультиплікативного впливу трьох факторів. Пропонується зберегти цю змінну в моделі для подальшого проведення біфуркаційного аналізу стійкості діючої системи протидії фінансовим та кібершахрайствам та побудови фазових портретів їх "станів рівноваги", оскільки наявність цієї змінної мультиплікативного впливу трьох факторів є необхідною умовою якісного біфуркаційного аналізу. Коефіцієнт детермінації досягає 70,59%, що свідчить про те, що змінні факторів пояснюють 70,59% варіації результативної ознаки інтегрального індексу кібербезпеки, що вказує на задовільний ступінь зв'язку між ними.

Для проведення шостого етапу аналізу стійкості системи протидії фінансовим та кібершахрайствам створимо нелінійну функцію (2.10), використовуючи рівняння (2.9) як основу (Kuzmenko et al., 2023; Яровенко та ін., 2021):

$$f(gei, edi, ci) := 10.8978783 + 9.977087\sin(gei) + 7.643510 \cdot 10^{-5} \cdot (edi^3) + 3.40130281\cos(ci) - 0.00057478\,gei \cdot edi \cdot ci \quad (2.10)$$

На основі розглянутої функції (2.10) створимо систему диференціальних рівнянь, що описують поведінку динамічної системи протидії фінансовим та кібершахрайствам з метою подальшої побудови фазових портретів "станів рівноваги" (формула 2.11) (Kuzmenko et al., 2023; Яровенко та ін., 2021):

$$\frac{d}{dgei} f(gei, edi, ci) \to 9.97708762\cos(gei) + -0.00057478\,ci \cdot edi$$
$$\frac{d}{dedi} f(gei, edi, ci) \to 0.00022930\,5\,edi^2 + -0.00057478\,ci \cdot gei \quad (2.11)$$
$$\frac{d}{dci} f(gei, edi, ci) \to -3.40130281\sin(ci) + -0.00057478\,edi \cdot gei$$

Представлені три диференційні рівняння (2.11) дозволяють встановити взаємозв’язки між змінними GEI (індекс ефективності уряду), EDI (легкість ведення бізнесу), CI (індекс злочинності) та їх першими частковими похідними $\frac{d}{dgei} f(gei, edi, ci), \frac{d}{dedi} f(gei, edi, ci), \frac{d}{dci} f(gei, edi, ci)$ (Kuzmenko et al., 2023; Яровенко та ін., 2021).

На підставі нелінійного підходу, який є основою теорії біфуркації, ми створимо фазові портрети "станів рівноваги" інтегрального індексу кібербезпеки, в яких фазові траєкторії будуть відображені як проекції на різні плоскості, такі як: індекс ефективності уряду - легкість ведення бізнесу, легкість

ведення бізнесу - індекс злочинності, індекс ефективності уряду - індекс злочинності. Побудову цих портретів було виконано на основі системи диференційних рівнянь (2.12) за допомогою програмного забезпечення для математичного аналізу MathCad (Kuzmenko et al., 2023; Яровенко та ін., 2021):

$$
\begin{aligned}
&Faza(gei0, edi0, ci0, dt, N) := \left|
\begin{array}{l}
\left(gei_0 \leftarrow gei0 \quad edi_0 \leftarrow edi0 \quad ci_0 \leftarrow ci0\right) \\
\text{for } k \in 0..N \\
\quad \left|
\begin{array}{l}
fff \leftarrow f\left(gei_k, edi_k, ci_k\right) \\
gei_{k+1} \leftarrow \left[gei_k + dt \cdot \left(9.97708762 \cos\left(gei_k\right) + -0.00057478 ci_k \cdot edi_k\right)\right] \\
edi_{k+1} \leftarrow \left[edi_k + dt \cdot \left[0.00022930 \left(edi_k\right)^2 + -0.00057478 ci_k \cdot gei_k\right]\right] \\
ci_{k+1} \leftarrow \left[ci_k + dt \cdot \left(-3.40130281 \sin\left(ci_k\right) + -0.00057478 edi_k \cdot gei_k\right)\right]
\end{array}
\right. \\
(gei \quad edi \quad ci)
\end{array}
\right.
\end{aligned}
\tag{2.12}
$$

З метою візуалізації і подальшої ідентифікації типу фазового портрету "станів рівноваги", який був представлений за допомогою формули (2.12), для системи протидії фінансовим та кібершахрайствам, ми розглядаємо різні можливі комбінації значень як факторів (індекс ефективності уряду, легкість ведення бізнесу, індекс злочинності), так і значень функції, що описує інтегральний індекс кібербезпеки, з певним рівнем точності на основі заданої кількості точок реалізації (Kuzmenko et al., 2023; Яровенко та ін., 2021):

$$
\begin{aligned}
(gei1 \quad edi1 \quad ci1) &:= Faza(1.6, 80, 42, 0.01, 100) \\
(gei2 \quad edi2 \quad ci2) &:= Faza(1.45, 78, 20, 0.01, 100) \\
(gei3 \quad edi3 \quad ci3) &:= Faza(0.18, 68, 36, 0.01, 100) \\
(gei4 \quad edi4 \quad ci4) &:= Faza(0.43, 56, 51, 0.01, 100) \\
(gei5 \quad edi5 \quad ci5) &:= Faza(-0.32, 50, 52, 0.01, 100) \\
(gei6 \quad edi6 \quad ci6) &:= Faza(-0.45, 57, 70, 0.01, 100)
\end{aligned}
\tag{2.13}
$$

Підставляючи конкретні значення вхідних даних (за формулою 2.13) у відповідні співвідношення, які використовуються для формалізації фазових портретів (за формулою 2.12), ми визначаємо рівноважні точки, які відображені на площині «індекс ефективності уряду - легкість ведення бізнесу» (за рисунком 2.8). Отже, для стану рівноваги системи протидії фінансовим та кібершахрайствам відповідають такі значення її параметрів (які позначені точками перетину графіків на рисунку 2.8): індекс ефективності уряду – 1,4838, легкість ведення бізнесу – 80,183.

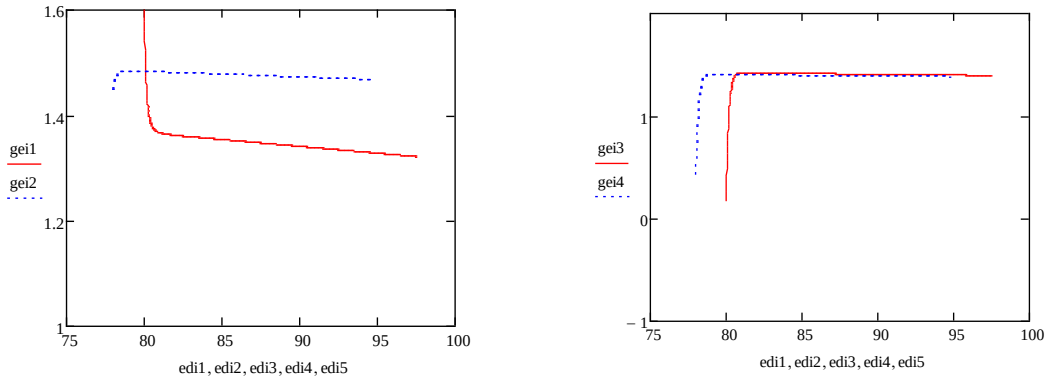


Рисунок 2.8 – Зображення рівноважних точок системи протидії фінансовим та кібершахрайствам у площині «індекс ефективності уряду - легкість ведення бізнесу»

Джерело: розроблено на основі (Kuzmenko et al., 2023; Яровенко та ін., 2021)

Проведемо аналіз фазового портрету динамічної системи, яка протидіє фінансовим та кібершахрайствам, за всіма можливими значеннями вхідних показників (згідно з формулою 2.13). Розглянемо спершу частину фазового портрету цієї системи в контексті площини "індекс ефективності уряду - легкість ведення бізнесу" (представлено на рисунку 2.9). Відзначимо, що цей фазовий портрет демонструє наявність точки рівноваги.

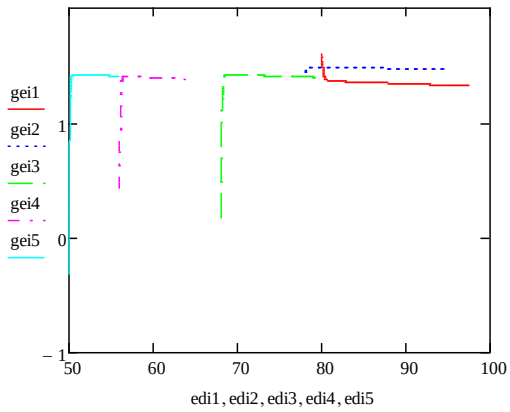


Рисунок 2.9 – Фрагмент фазового портрету «стан рівноваги» динамічної системи протидії фінансовим та кібершахрайствам в розрізі площини «індекс ефективності уряду - легкість ведення бізнесу»

Джерело: розроблено на основі (Kuzmenko et al., 2023; Яровенко та ін., 2021)

Перехід до розгляду частини фазового портрету динамічної системи, що протидіє фінансовим та кібершахрайствам, в площині "легкість ведення бізнесу - індекс злочинності" (показано на рисунку 2.10), розкриває наявність "сідлової" точки. Цей вид біфуркації свідчить про нестабільний стан системи, що означає, що при суттєвій зміні одного параметра при фіксованому значенні іншого параметра система перебуває в нерівноважному стані.

Нерівноважний стан динамічної системи, спрямованої на протидію фінансовим та кібершахрайствам, відображений у фазовому портреті типу

"сідло" і спостерігається також в площині "індекс ефективності уряду - індекс злочинності", як видно на рисунку 2.11.

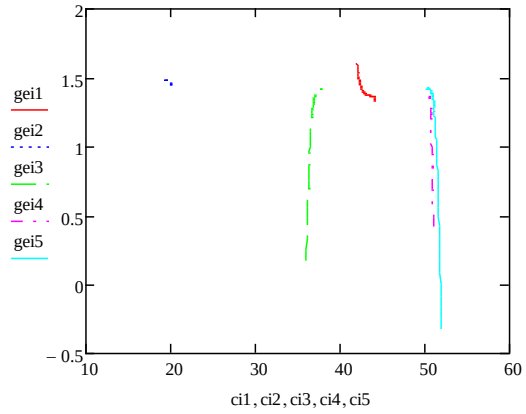


Рисунок 2.10 – Фрагмент фазового портрету «сідло» динамічної системи протидії фінансовим та кібершахрайствам, що знаходиться в нерівноважному стані, в розрізі площини «легкість ведення бізнесу - індекс злочинності»
Джерело: розроблено на основі (Kuzmenko et al., 2023; Яровенко та ін., 2021)

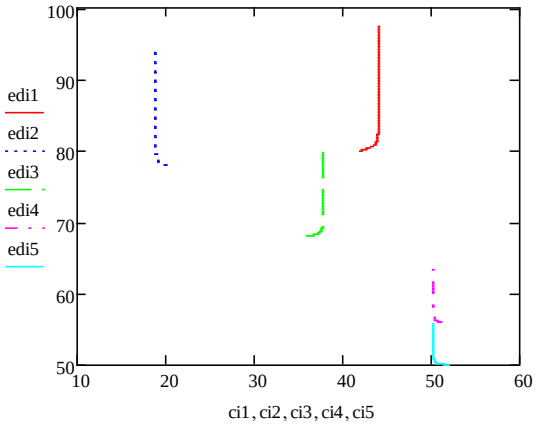


Рисунок 2.11 – Фрагмент фазового портрету «сідло» динамічної системи протидії фінансовим та кібершахрайствам, що знаходиться в нерівноважному стані, в розрізі площини «індекс ефективності уряду - індекс злочинності»
Джерело: розроблено на основі (Kuzmenko et al., 2023; Яровенко та ін., 2021)

Отже, за допомогою аналізу біфуркації для оцінки стабільності системи протидії фінансовим та кібершахрайствам (рисунки 2.9-2.11), було визначено фазовий портрет "станів рівноваги" в площині "індекс ефективності уряду - легкість ведення бізнесу", а також виявлено нерівноважні фазові портрети типу "сідло" в інших проекціях.

Отже, була проведена оцінка зрілості системи для протидії фінансовим та кібершахрайствам з метою визначення її готовності до інтеграції на різних рівнях державного управління. Оскільки досліджувані системи мають динамічний характер, тобто їх стан змінюється під впливом різноманітних зовнішніх і внутрішніх факторів, то був проведений біфуркаційний аналіз та створені фазові

портрети їх зрілості та стабільності. Результатом цих досліджень стали фазові портрети, що вказують на "нестабільний фокус" динамічної системи протидії фінансовому та кібершахрайству, в яких враховані такі параметри, як "легкість ведення бізнесу - індекс злочинності" та "індекс ефективності державного управління - легкість ведення бізнесу". У розділі, що стосується "індексу ефективності державного управління - індексу злочинності", був побудований фазовий портрет, що відображає "нестабільний вузол".

Аналіз показав, що система протидії фінансовому та кібершахрайству перебуває у нестабільному стані, що означає значний вплив рівня злочинності, неефективних державних рішень та обмежень для розвитку бізнесу на її функціонування. У той же час, такі фактори, як фінансова таємниця, політична стабільність, рівень корупції та тероризм, не викликають значних коливань та не суттєво впливають на систему кібербезпеки. Для успішної інтеграції системи боротьби з фінансовим та кібершахрайством, передусім, потрібні законодавчі зміни, які покращать якість життя громадян і знизять рівень злочинності загалом, включаючи фінансові та кіберзагрози. Також необхідно створити сприятливі умови для розвитку бізнесу, що сприяє економічному зростанню країни. Ці аспекти слід розглядати на стратегічному рівні під час процесів інтеграції розглянутих систем.

Згідно з запропонованою методикою були визначені точки досягнення рівноваги системи та створені фазові портрети, які представляють собою "сідла" на трьох відповідних площинах. Отримані результати вказують на те, що система протидії фінансовому та кібершахрайству не може досягти стану рівноваги. Навіть незначна зміна одного з параметрів призводить до зміни цього стану, за умови, що інший фактор залишається незмінним. Це підтверджує попередні висновки про нестабільність та дисбаланс системи.

Підсумовуючи, були створені передумови для зближення системи протидії фінансовому та кібершахрайству, які підвищують рівень захисту та сприяють її стабільності. У майбутньому можливо рекомендувати такий підхід профільним державним органам для поліпшення стратегії розвитку державного фінансового моніторингу та національної кібербезпеки.

2.1.3. Сценарії взаємодії систем кібербезпеки та протидії фінансовим злочинам для країн з різним рівнем економічного розвитку

Сьогодні проблема боротьби з відмиванням кримінальних доходів та фінансуванням тероризму є вельми актуальною для багатьох країн світу. Це виникає через те, що завдяки процесу легалізації коштів, які мають незаконний початок, значні суми уникають оподаткування, що сприяє розвитку тіньового сектору, стимулює зростання рівня злочинності та може призвести до дестабілізації економіки країни, конфліктів у суспільстві та погіршення довіри міжнародних партнерів. Згідно з опитуванням, проведеним консалтинговою компанією "PwC" у 2018 році, обсяг операцій з відмивання кримінальних доходів та фінансування тероризму становив 1 трлн. доларів, що становило від 2% до 5%

світового ВВП (Acwalks, 2021). Ця ситуація викликає серйозні обурення у світовій спільноті через загрози, які вона ставить перед міжнародною фінансовою системою. Міжнародна організація FATF пропонує необхідні заходи для боротьби та запобігання легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення. У цьому контексті розроблені спеціальні стандарти та інструменти, які регулярно оновлюються для відповідності реальності функціонування фінансової системи.

З іншого боку, результати Четвертої промислової революції призвели до швидкого розроблення і впровадження інформаційних технологій в усі сфери життя людини. Процеси автоматизації та цифровізації спричинили зростання кіберзлочинів, особливо в фінансовій сфері, яка вважається однією з п'яти найбільш атакованих галузей у світі (Morgan, 2019). Також втрати від кіберзлочинності зростають експоненційно, і за прогнозами експертів до 2021 року вони можуть скласти 6 трлн. доларів (Morgan, 2019). Тому проблема забезпечення високого рівня кіберзахисту фінансової системи країни та інших сфер стає критично важливою та має велике практичне значення.

Для вирішення цих проблем можливий підхід, який передбачає поєднання системи кібербезпеки та заходів щодо протидії легалізації кримінальних доходів у єдину інтегровану систему. Спільна дія цих систем може призвести до синергетичного ефекту, який значно перевершує ефекти від їх окремого функціонування. Цю інтеграцію можна здійснити на різних рівнях, включаючи технологічний, програмний, інформаційний, правовий та організаційний.

Здійснення процесу інтеграції є складним завданням і вимагає особливої обережності, оскільки невірні рішення в цьому процесі можуть призвести до серйозних наслідків. Тому перед початком інтеграції необхідно провести детальну оцінку поточного стану системи кібербезпеки та заходів протидії фінансовим злочинам. Ця оцінка допоможе визначити потенційний рівень можливої конвергенції для різних країн та зменшити ризик невдачі в процесі інтеграції.

Питання щодо злиття системи кібербезпеки та протидії легалізації кримінальних доходів є відносно новим та мало вивченим напрямком для сучасної наукової спільноти. Тому наявні обмежені наукові дослідження, які проводилися в цьому контексті.

Один з найбільш актуальних аспектів цього питання стосується боротьби з шахрайством, пов'язаним із використанням кредитних карток. Це обумовлено зростанням кількості шахраїв, які здійснюють шахрайські операції щодо фізичних осіб – клієнтів банків за допомогою різних методів, включаючи соціальну інженерію. Науковці та практики, які присвятили свої дослідження цій темі, включають Dileep et al. (2021), Wang & Liu (2021), Mishra & Kumari (2020), Mekterović et al. (2021) та інших дослідників. Ці науковці розглядали питання, пов'язані зі злочинними активностями, які використовують кредитні картки, та вивчали методи боротьби з цими видами шахрайства.

Також наукова спільнота вивчає інструменти для боротьби з фінансовими та кібершахрайствами. Зокрема, набули популярності технології машинного навчання та штучного інтелекту, які використовуються для виявлення потенційних шахрайських операцій. Наприклад, дослідники, такі як Chen et al. (2018), досліджували можливості використання машинного навчання для виявлення операцій, що можуть вказувати на легалізацію кримінальних доходів. Інші, такі як Zhou et al. (2021), запропонували метод бустінгу для прогнозування шахрайських операцій. Була розроблена мультиагентна система для виявлення операцій, які можуть свідчити про легалізацію коштів, одержаних злочинним шляхом, і цю систему можна інтегрувати в банківські інформаційні системи. Gao et al. (2009) були одними з авторів цієї розробки. Крім того, дослідники, такі як Karpunina et al. (2021), досліджували можливості використання блокчейн-технологій для протидії фінансовим та кібершахрайствам.

Суттєвими є аспекти організаційного, технологічного, правового та інформаційного забезпечення системи кібербезпеки та протидії легалізації кримінальних доходів. Наприклад, Dawson (2018) досліджував інтеграцію політичної, освітньої та технологічної сфер для підвищення ефективності системи кібербезпеки та протидії фінансовим шахрайствам. Dionysios S. Demetis (2010) досліджував різні технології виявлення операцій, які можуть свідчити про легалізацію незаконних коштів, включаючи аналіз ризиків та методи їх оцінювання. Gagliani (2020) звертав увагу на концепцію "технологічної нейтральності" у контексті кібербезпеки та формування міжнародної правової бази для цього.

Незважаючи на значну кількість наукових публікацій, що висвітлюють питання боротьби з фінансовими та кібершахрайствами, існують багато аспектів, які залишаються слабо дослідженими та потребують подальшого вивчення та уточнення. Однією з таких невивчених областей є можливість інтеграції системи кібербезпеки та боротьби з фінансовими шахрайствами та легалізацією кримінальних доходів.

Метою нашого дослідження є оцінка потенційного рівня інтеграції системи кібербезпеки та протидії легалізації кримінальних доходів і фінансуванню тероризму. Ми плануємо визначити їх інтегральні показники та використовувати функцію Харрінгтона–Менчера в рамках розроблення сценаріїв інтеграції.

Для цього ми плануємо використовувати методологію, яку запропонував Yarovenko (2020) для оцінки загроз інформаційній безпеці. Основна ідея полягає у визначенні інтегрального показника, проте в нашому дослідженні ми плануємо розраховувати два композитних індикатори. Один із них буде характеризувати рівень кібербезпеки в країні, а інший – рівень протидії легалізації кримінальних доходів.

На початковому етапі виберемо вхідні дані, які будуть використовуватися для проведення розрахунків. Першу групу даних складають світові індекси, призначені для оцінки різних аспектів кібербезпеки країн, та взяті з офіційного сайту організації «e-Governance Academy Foundation» за даними на 2018 рік. Ці індекси включають:

1. Глобальний індекс кібербезпеки (Global Cybersecurity Index), який визначає здатність країн світу протидіяти кіберзагрозам та ідентифікує їхні сильні та слабкі сторони, а також потенційні можливості.
2. Національний індекс кібербезпеки (National Cyber Security Index), який оцінює готовність окремої країни протидіяти кіберзагрозам та керувати кіберінцидентами.
3. Індекс мережевої готовності (Networked Readiness Index), який дозволяє визначити технологічну готовність країни для впровадження сучасних інформаційних систем та технологій для автоматизації різних сфер суспільства.
4. Рівень цифрового розвитку (Digital Development Level), який вказує на ступінь цифрової трансформації країни.

Кожен з цих обраних показників охоплює різні аспекти кібербезпеки країни. Аналіз цих показників в комплексі допоможе сформувати всебічне уявлення про рівень розвитку та можливості інтеграції в галузі кібербезпеки.

Друга група індикаторів включає індекси, які дозволяють оцінити стан системи протидії легалізації кримінальних доходів та фінансування тероризму. Серед них:

Індекс політичної стабільності (Political Stability Index), який враховує ймовірність дестабілізації уряду країни через неконституційні та насильницькі заходи. Цей показник може мати як позитивний, так і негативний вплив на процеси легалізації незаконних коштів.

1. Індекс ефективності уряду (Government Effectiveness Index), який вимірює якість управління державними органами, їх незалежність від політичного впливу, ефективність роботи та рівень довіри до уряду.
2. Легкість ведення бізнесу (Ease of Doing Business), що оцінює умови для підприємництва в країні, що впливає на ризики зростання тіньового сектору та відмивання коштів.
3. Індекс злочинності (Crime Index), який вказує на рівень злочинності в країні і впливає на стабільність соціальної, політичної та економічної сфер.
4. Глобальний індекс тероризму (Global Terrorism Index), який свідчить про рівень терористичної активності, що може впливати на ризики легалізації кримінальних доходів та фінансування тероризму.
5. Індекс фінансової таємниці (Financial Secrecy Index), який вказує на ступінь захисту фінансових операцій і може сприяти приховуванню незаконних доходів та фінансових операцій з кримінальними джерелами коштів.

Дані для цих індексів були зібрані з офіційного джерела Світового банку і охоплюють 76 країн світу за 2018 рік, що дозволяє провести аналіз з використанням повного набору даних за цей період.

У дослідженні, яке провели Кузьменко та інші (2021), був проведений вхідний аналіз процесу конвергенції систем кібербезпеки та фінансового моніторингу. Цей аналіз підтвердив важливість та актуальність саме цих показників для подальших досліджень.

На другому етапі ми виконаємо процедуру нормалізації вхідних даних для того, щоб привести їх до єдності у вигляді, який дозволить їх ефективну

порівняльну обробку. Для цього застосуємо нелінійний метод нормалізації, який дозволяє краще вирівнювати різні дані за їхніми характеристиками і значеннями, ніж інші методи (згідно з формулою (2.14) (Yarovenko et al., 2021; Яровенко та ін., 2021):

$$Z_{ij} = \left(1 + e^{\frac{\overline{y_j} - y_{ij}}{\sigma(y)}}\right)^{-1}, \quad (2.14)$$

де Z_{ij}– нормалізоване значення j-го показника, обраного для здійснення оцінки рівня конвергенції системи кібербезпеки та протидії легалізації кримінальних доходів, в розрізі і-ої країни;

$\overline{y_j}$– середнє значення j-го показника в межах досліджуваного переліку країн;

y_{ij} – фактичне значення j-го показника в розрізі і-ої країни;

$\sigma(y_j)$ – середнє квадратичне відхилення j-го показника в межах досліджуваного переліку країн (Yarovenko et al., 2021; Яровенко та ін., 2021).

Всі вибрані показники, за своїм впливом на систему, виступають як чинники стимуляції, за винятком двох - індексу злочинності та фінансової таємниці, які є чинниками дестимуляції. Тому, для належного врахування їх ваги при формуванні інтегрального показника, ми віднімемо їх нормалізовані значення від одиниці.

На третьому етапі, ми перетворимо нормалізовані значення вибраних показників з бази дослідження на безрозмірну шкалу захисту, використовуючи формулу (2.15) (Yarovenko et al., 2021; Яровенко та ін., 2021):

$$d_{ij} = \exp(-\exp(-Z_{ij})), \quad (2.15)$$

де d_{ij} - проміжне значення j-го показника, обраного для здійснення оцінки рівня конвергенції системи кібербезпеки та протидії легалізації кримінальних доходів, в розрізі і-ої країни, приведене до безрозмірної шкали бажаності Харрінгтона;

Z_{ij} – нормалізоване значення j-го показника, в розрізі і-ої країни (Yarovenko et al., 2021; Яровенко та ін., 2021).

Для подальшого формування комплексного показника, оцінюючи рівень конвергенції між системою кібербезпеки та заходами протидії фінансовому шахрайству, потрібно провести дослідження характеру кривої перетворення Харрінгтона-Менчера, яка визначає залежність d_ij від фактичних значень кожного вхідного показника. З цією метою, на четвертому етапі, ми візуалізували ці залежності. Результати вказують на те, що більшість показників характеризується першим типом кривої - S-подібною, зростаючою та симетричною. З іншого боку, індекси злочинності та фінансової таємниці відповідають четвертому типу - S-подібні, спадаючі та симетричні криві.

Приклади отриманих графіків для першого та другого типів подані на рисунках 2.12 та 2.13.

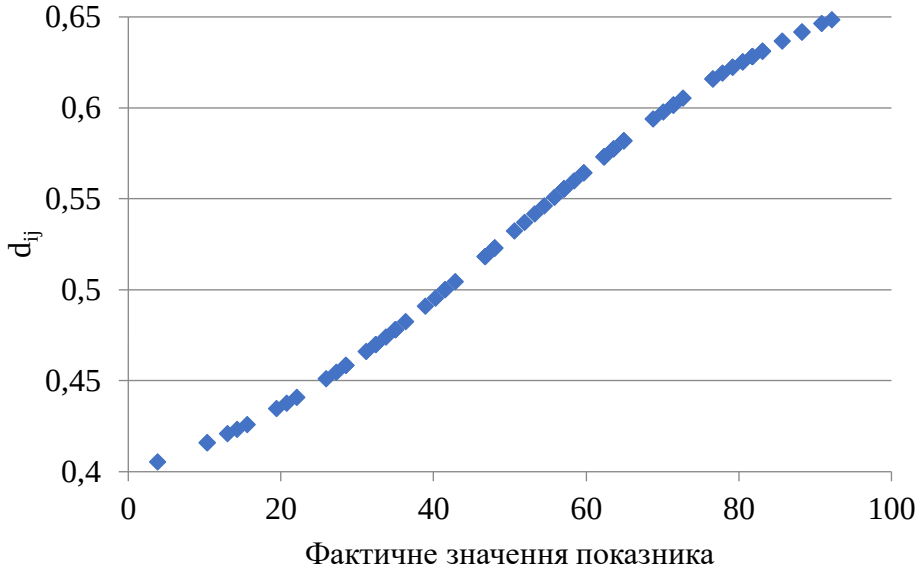


Рисунок 2.12 – Графік кривої першого типу для «Національного індексу кібербезпеки»

Джерело: розроблено авторами на основіYarovenko et al. (2021) та Яровенко та ін. (2021)

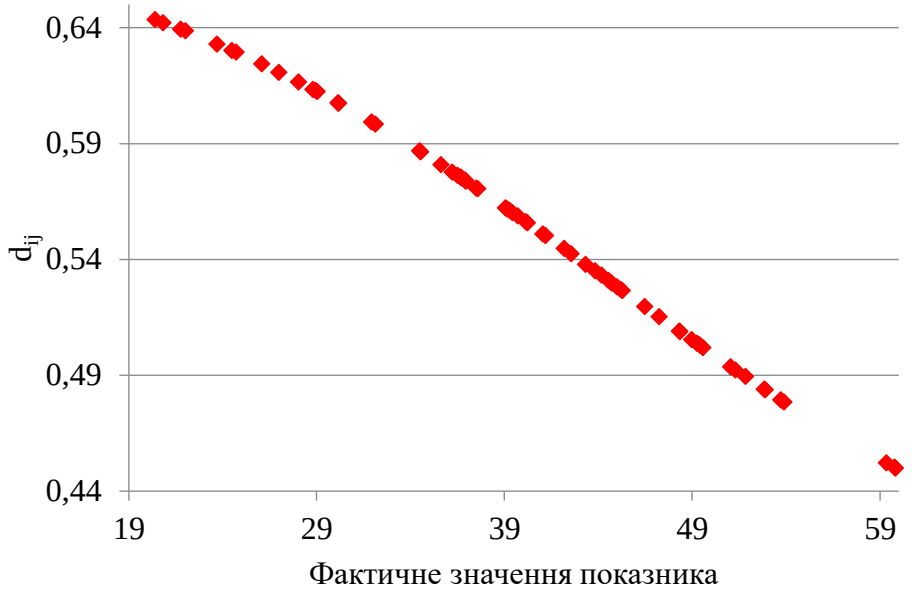


Рисунок 2.13 – Графік кривої четвертого типу для «Індексу злочинності»

Джерело: розроблено авторами на основіYarovenko et al. (2021) та Яровенко та ін. (2021)

На п'ятому етапі ми впровадимо формалізацію перетворення Харрінгтона-Менчера, враховуючи залежність d_{ij} від фактичних значень кожного вхідного показника, як було визначено на попередньому етапі. Іншими словами, ми розрахуємо проміжні значення показників для оцінки рівня конвергенції між системою кібербезпеки та протидії фінансовому шахрайству, керуючись їх

приведенням до безрозмірної шкали бажаності Харрінгтона-Менчера відповідно до визначеного типу кривої.

Для показників, для яких залежність описується кривою першого типу, ми використовуватимемо формулу (2.16) (Yarovenko et al., 2021; Яровенко та ін., 2021):

$$d_{ij}^{*} = \exp\left(-\exp\left(-\left(9\left(\frac{Z_{ij}-\min\limits_{i} Z_{ij}}{\max\limits_{i} Z_{ij}-\min\limits_{i} Z_{ij}}\right)^{1.927}-2\right)\right)\right), \qquad (2.16)$$

де d_{ij}^{*} - проміжне значення j-го показника, обраного для здійснення оцінки рівня конвергенції системи кібербезпеки та протидії легалізації кримінальних доходів, в розрізі і-ої країни, приведене до безрозмірної шкали бажаності Харрінгтона-Менчера;

$\min\limits_{i} Z_{ij}$ – мінімальне значення нормалізованого j-го показника в розрізі і-ої країни;

$\max\limits_{i} Z_{ij}$ – максимальне значення нормалізованого j-го показника в розрізі і-ої країни (Yarovenko et al., 2021; Яровенко та ін., 2021).

Для тих показників, де залежності відповідають кривій четвертого типу, ми будемо застосовувати формулу (2.17) (Yarovenko et al., 2021; Яровенко та ін., 2021):

$$d_{ij}^{*} = \exp\left(-\exp\left(-\left(9\left(\frac{\max\limits_{i} Z_{ij}-Z_{ij}}{\max\limits_{i} Z_{ij}-\min\limits_{i} Z_{ij}}\right)^{1.927}-2\right)\right)\right). \qquad (2.17)$$

На шостому етапі, необхідно визначити вагові коефіцієнти для показників, щоб обчислити загальну оцінку. Для цього ми проведемо канонічний аналіз, який дозволить встановити ступінь зв'язку між двома групами показників і розрахувати їх канонічні вагові коефіцієнти. Ці вагові коефіцієнти будуть використовуватися для узагальненої оцінки. Аналіз проведено за допомогою аналітичного пакету "STATISTICA", і результати представлені на рисунку 2.14.

З рисунку 2.14 видно, що значення канонічної кореляції становить R = 0,93762, що свідчить про наявність дуже сильного кореляційного зв'язку між групою факторів, що визначають рівень розвитку системи кібербезпеки та протидії фінансовим шахрайствам.

N=76	Canonical Analysis Summary (Konvergentcia2.sta) Canonical R: .93762 Chi²(24)=200.41 p=0.0000 **Left Set**	Right Set
No. of variables	4	6
Variance extracted	100.000%	83.8201%
Total redundancy	70.3694%	47.9580%
Variables: 1	Global Cybersecurity Index	Political stability index
2	Networked Readiness Index	Government effectiveness index
3	National Cyber Security Index	Ease of doing business
4	Digital Development Level	Crime Index
5		Global Terrorism Index
6		Financial Secrece Index

Рисунок 2.14 – Підсумки канонічного аналізу

Джерело: розроблено авторами на основіYarovenko et al. (2021) та Яровенко та ін. (2021)

Високе значення критерію Пірсона (χ^2=200,00) та рівень значущості не вище 0,05 (p = 0,0000) підтверджують статистичну значущість коефіцієнта кореляції. Значення надмірності для лівої множини, що формується індексами кібербезпеки, складає 70,3694%. Це свідчить про те, що фактори, пов'язані з рівнем протидії фінансовим шахрайствам у країні, в пояснюють 70,3694% варіації показників кібербезпеки. Це свідчить про суттєвий вплив цих факторів. Розвиток системи протидії відмиванню коштів в країні в певній мірі залежить від її рівня кібербезпеки. Фактори кібербезпеки пояснюють 47,9580% варіації факторів, що визначають рівень протидії фінансовим шахрайствам. Хоча це значення є помірним, воно все ж достатнє для обґрунтування впливу показників кібербезпеки на економічні процеси в країні.

Отримані значення канонічних коренів та аналіз статистичних характеристик дозволили з'ясувати, що у нас є 3 значущі канонічні корені. Проте для надійних оцінок їх навантажень для трьох пар канонічних змінних необхідно мати вибірку, що перевищує кількість вихідних даних в 40-60 разів [117, с. 190]. Тому ми вирішили, що для визначення ваги кожного з канонічних коренів доцільно використовувати тільки значення першого канонічного кореня. Це рішення обумовлено тим, що канонічний R2 для першого кореня досягає найвищого значення - 0,8791. На основі цих розрахунків ми будемо користуватися канонічними вагами, визначеними для першого кореня (див. рисунки 2.15-2.16) в подальших дослідженнях.

Variable	Canonical Weights, left set (Konvergentcia2.sta) Root 1	Root 2	Root 3	**Root 4**
Global Cybersecurity Index	0,313261	-0,781709	0,63400	1,14199
Networked Readiness Index	0,264381	-0,713150	-1,56282	-0,64848
National Cyber Security Index	-0,021339	0,026080	0,91519	-1,29626
Digital Development Level	0,557799	1,355225	0,21392	0,67528

Рисунок 2.15 – Канонічні ваги для показників кібербезпеки

Джерело: розроблено авторами на основіYarovenko et al. (2021) та Яровенко та ін. (2021)

Variable	Canonical Weights, right set (Konvergentcia2.sta)			
	Root 1	Root 2	Root 3	Root 4
Political stability index	-0,269140	0,923250	1,32088	0,990101
Government effectiveness index	0,780788	0,200480	-1,68893	0,203985
Ease of doing business	0,341713	-0,672184	0,64477	-0,816572
Crime Index	0,050110	0,111717	0,73583	-0,231753
Global Terrorism Index	0,009265	-0,080100	1,17396	1,219424
Financial Secrece Index	-0,091481	0,070369	0,35190	-0,048788

Рисунок 2.16 – Канонічні ваги для показників, що характеризують рівень протидії легалізації кримінальних доходів

Джерело: розроблено авторами на основіYarovenko et al. (2021) та Яровенко та ін. (2021)

Виявлено, що отримані канонічні ваги мають як позитивний, так і негативний внесок у значення канонічного кореня. Однак для розрахунку узагальненої функції необхідно, щоб їх значення були в межах від 0 до 1. Тому відповідні негативні ваги буде використано з їх модулем.

На сьомому етапі проводиться розрахунок двох інтегральних індексів для оцінки рівня розвитку системи кібербезпеки та протидії легалізації кримінальних доходів. Для цього будуть використані формули (2.18)-(2.19) (Yarovenko et al., 2021; Яровенко та ін., 2021):

$$IC_i = \sqrt[\sum_{j=1}^{n} a_j]{\prod_{j=1}^{n} \left(d_{ij}^*\right)^{a_j}}, \tag{2.18}$$

$$IP_i = \sqrt[\sum_{j=1}^{m} a_j]{\prod_{j=1}^{m} \left(d_{ij}^*\right)^{a_j}}, \tag{2.19}$$

де IC_i – інтегральний індекс, що характеризує рівень розвитку системи кібербезпеки для і-тої країни;

IP_i – інтегральний індекс, що характеризує рівень розвитку системи протидії легалізації кримінальних доходів для і-тої країни;

n – кількість показників кібербезпеки країни (n = 4);

m – кількість показників, що характеризують рівень розвитку системи протидії легалізації кримінальних доходів (m = 6);

a_j – ваги відповідного j-го вхідного показника кібербезпеки або протидії легалізації кримінальних доходів;

d_{ij}^* - проміжне значення j-го показника кібербезпеки або протидії легалізації кримінальних доходів в розрізі і-ої країни, приведене до безрозмірної шкали бажаності Харрінгтона-Менчера (Yarovenko et al., 2021; Яровенко та ін., 2021).

Розраховані інтегральні показники можуть бути проінтерпретовані з використанням якісної оцінки, де діапазон значень визначає ступінь розвитку країни: якщо значення знаходиться в інтервалі від 0,80 до 1,00, то це відповідає рівню "дуже добре"; від 0,63 до 0,80 - "добре"; від 0,37 до 0,63 - "задовільно"; від 0,20 до 0,37 - "погано"; від 0,00 до 0,20 - "дуже погано".

Отримані результати можна візуалізувати, створюючи діаграми та карти за допомогою програмного продукту MS Excel. Подані результати можна знайти на рисунках 2.17-2.18.

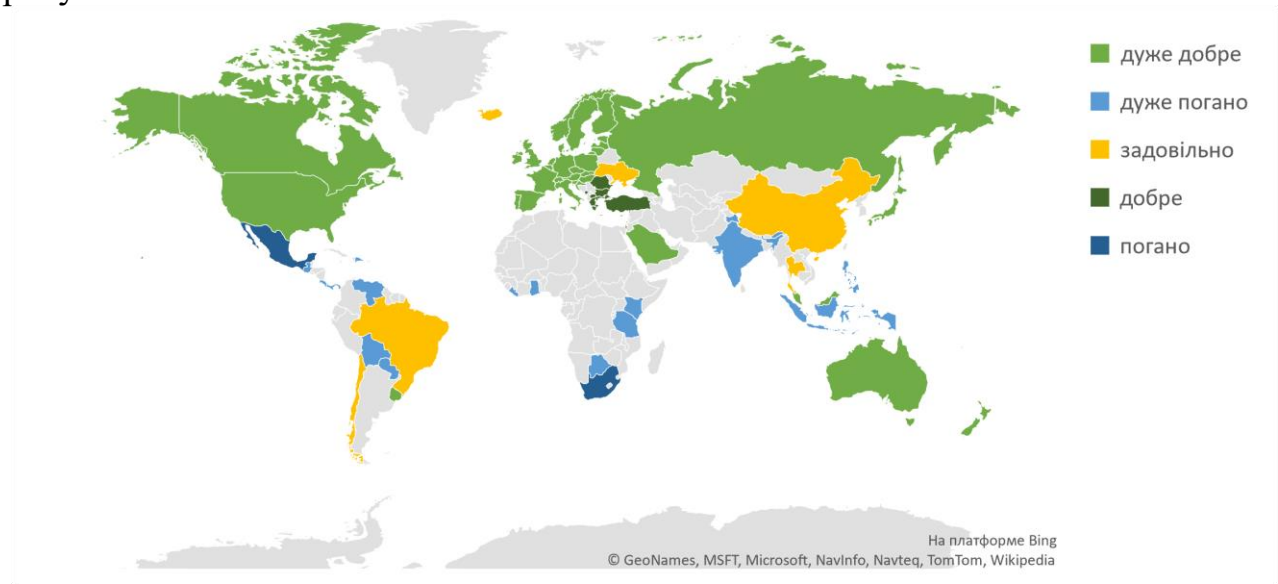


Рисунок 2.17 – Карта розподілу країн за інтегральним індексом, що характеризує рівень розвитку їх системи кібербезпеки

Джерело: розроблено авторами на основіYarovenko et al. (2021) та Яровенко та ін. (2021)

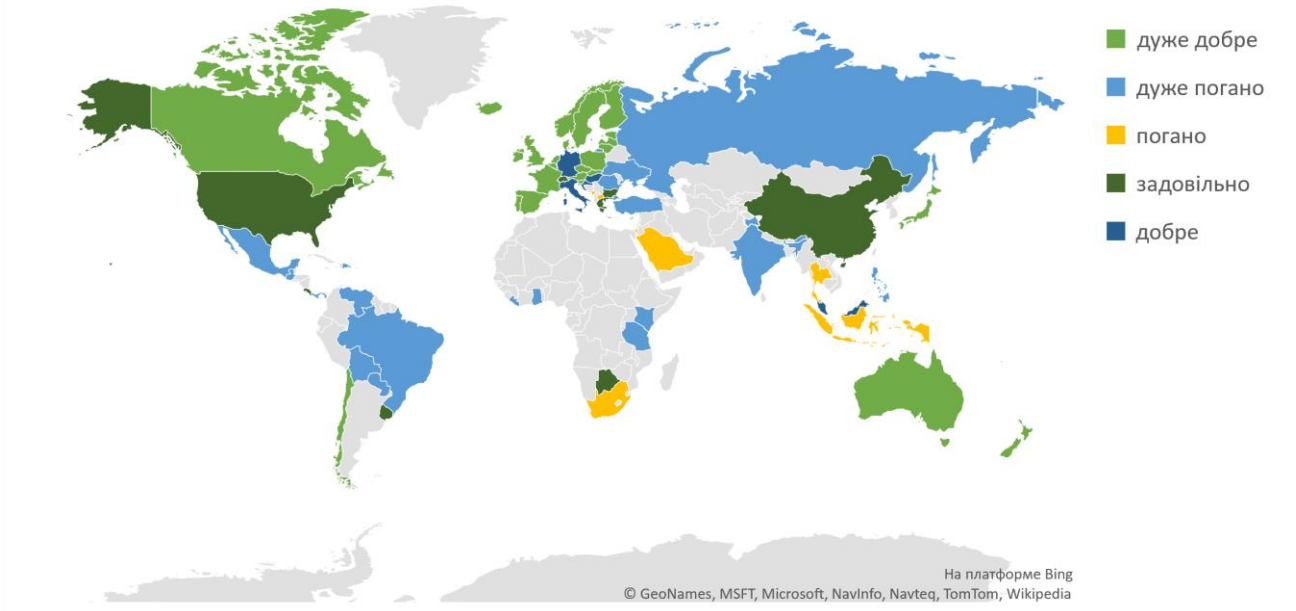


Рисунок 2.18 – Карта розподілу країн за інтегральним індексом, що характеризує рівень розвитку системи протидії легалізації кримінальних доходів

Джерело: розроблено авторами на основіYarovenko et al. (2021) та Яровенко та ін. (2021)

За інтегральним рівнем кібербезпеки можна виділити кілька категорій країн. Оцінку "дуже добре" отримали 38 країн, включаючи Австрію, Австралію, Канаду, Данію, Естонію, Фінляндію, Німеччину, Великобританію, США та інші, які в основному є розвиненими країнами (див. рис. 2.17). Інші країни, такі як Болгарія, Греція, Маврикій, Чорногорія, Північна Македонія, Туреччина та Румунія, отримали оцінку "добре" щодо рівня кібербезпеки. Задовільний рівень кібербезпеки характерний для країн, як Україна, Бразилія, Чилі, Китай, Ісландія, Мальта та Тайланд. З іншого боку, оцінку "погано" та "дуже погано" отримали 24 країни, включаючи Барбадос, Болівію, Ботсвану, Домініканську республіку, Гану, Гватемалу, Індію, Індонезію, Кенію, Ліберію та інші країни, які розвиваються або є найменш розвиненими. Узагальнюючи, можна сказати, що рівень кібербезпеки корелює з економічним розвитком країни. Розвинені країни мають високий рівень кіберзахисту, тоді як країни, які розвиваються або є найменш розвиненими, стикаються з численними проблемами в цій сфері, включаючи відсутність кваліфікованих фахівців, низький рівень інвестицій, слабкий правовий захист та інші аспекти.

З огляду на інтегральний рівень протидії фінансовим шахрайствам виділяються кілька категорій країн. Оцінку "дуже добре" отримали 28 країн, включаючи Австралію, Австрію, Бельгію, Канаду, Ірландію, Нідерланди, Норвегію, Великобританію, Швецію, Чехію та інші (див. рис. 2.18). Інші країни, такі як Хорватія, Німеччина, Угорщина, Італія, Малайзія, Мальта та Сингапур, отримали оцінку "добре" щодо рівня протидії легалізації кримінальних доходів. Оцінку "задовільно" отримали Ботсвана, Болгарія, Китай, Коста Ріка, Греція, Люксембург, Сейшельські острови, Швейцарія, США та Уругвай. Водночас 9 країн отримали рівень "погано", а 22 країни – "дуже погано". До останніх відносяться, зокрема, Болівія, Бразилія, Індія, Україна, Російська Федерація, Мексика, Південна Африка, Таїланд, Індонезія та інші. Таким чином, країни з високим рівнем злочинності та тероризму, озброєними конфліктами, низьким рівнем економічного розвитку виявляються привабливими для легалізації кримінальних доходів та фінансування тероризму. Системи протидії таким операціям в цих країнах є досить слабкими та недорозвиненими. Також країни з високим рівнем фінансової таємниці створюють сприятливі умови для відмивання коштів, отриманих злочинним шляхом. На сьогодні такими країнами є Швейцарія, Люксембург та США.

Для оцінки рівня конвергенції систем кібербезпеки та протидії фінансовим шахрайствам, ми обчислимо середнє арифметичне двох інтегральних індексів. Після розрахунків ми покажемо результати на карті, що відображає розподіл країн за рівнем конвергенції систем кібербезпеки та протидії фінансовим шахрайствам (див. рис. 2.19).

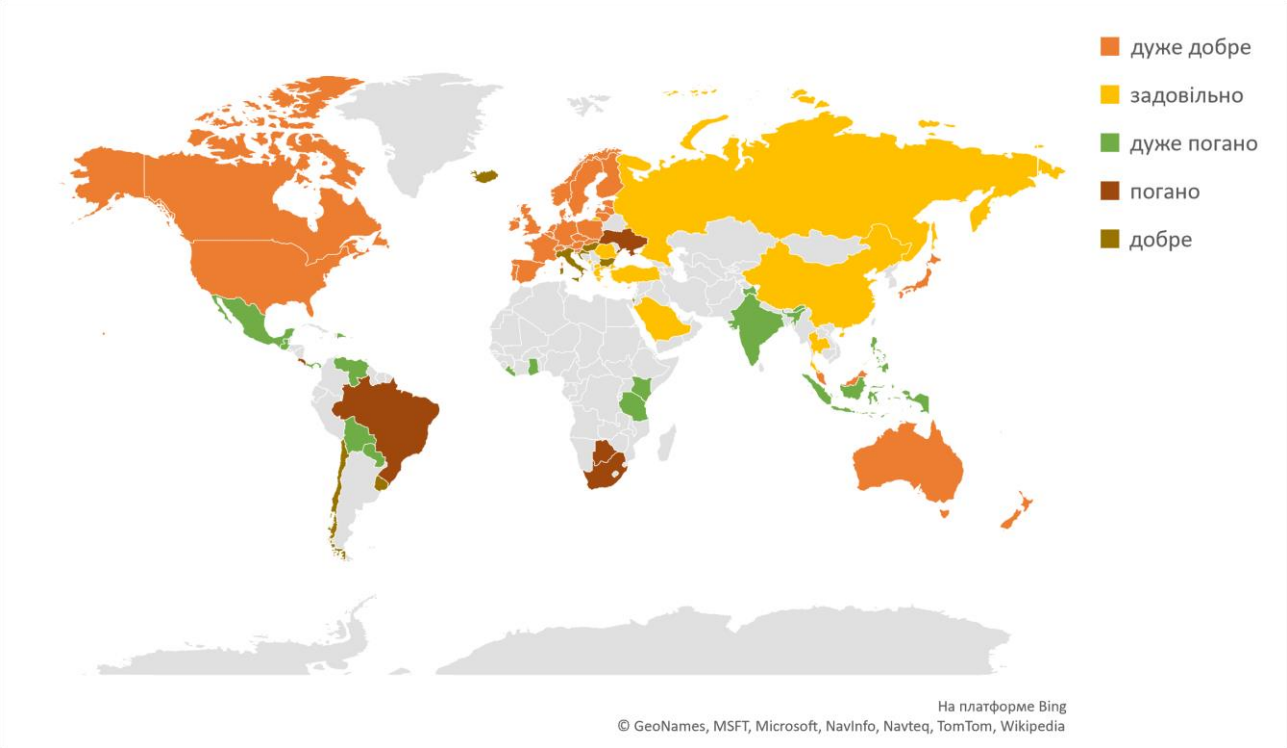


Рисунок 2.19 – Карта розподілу країн за рівнем конвергенції систем кібербезпеки та протидії легалізації кримінальних доходів

Джерело: розроблено авторами на основіYarovenko et al. (2021) та Яровенко та ін. (2021)

У разі конвергенції системи кібербезпеки та протидії фінансовим шахрайствам у країнах з низьким рівнем протидії, спостерігатиметься посилення їх потенційних можливостей завдяки вдосконаленій системі кіберзахисту. Інакше кажучи, порівнюючи результати, представлені на рисунках 2.17-2.19, можна визначити, що країни, такі як Бахрейн, Ботсвана, Бразилія, Бруней, Болгарія, Чилі, Коста Рика, Ісландія, Ізраїль, Люксембург, Мальта, Чорногорія, Північна Македонія, Румунія, Російська Федерація, Саудівська Аравія, Сейшельські острови, Сінгапур, Швейцарія, Таїланд, Туреччина, Україна, Сполучені Штати Америки та Уругвай, скористаються позитивними перевагами, що випливають із процесу конвергенції.

Актуальні тенденції, які відзначаються у збільшенні кількості кібершахрайств та легалізації кримінальних доходів, вимагають використання нових підходів та технологій для боротьби із цими явищами. Це можливо лише через системний підхід, що включає в себе програмні, технічні, інформаційні, організаційні, правові та технологічні заходи. Інакше кажучи, ця проблема потребує конвергенції системи кібербезпеки та протидії фінансовим шахрайствам. Варто зазначити, що цей процес вельми складний і, отже, потребує обережного та обґрунтованого підходу до його впровадження. Таким чином, проведення попередньої оцінки можливостей конвергенції цих двох систем є необхідним етапом у стратегії по вдосконаленню та підвищенню ефективності боротьби зі злочинністю на світовому рівні.

Було розглянуто показники, які відображають рівень розвитку системи кібербезпеки в країні та її здатність до протидії легалізації кримінальних доходів і фінансуванню тероризму. Метод Харрінгтона – Менчера, який був використаний, дозволив нам створити два комплексні показники. Під час оцінювання рівня кібербезпеки виявлено, що розвинуті країни володіють високим рівнем кіберзахисту, у той час як країни з менш розвиненими економіками або у стані розвитку мають нижчий рівень захисту. Щодо інтегральної оцінки рівня протидії легалізації кримінальних доходів, було встановлено, що серйозні проблеми у цьому плані спостерігаються в країнах із високим рівнем злочинності, активною терористичною діяльністю, недостатньою ефективністю державного управління та конфліктами з використанням зброї, а також в країнах з високим рівнем фінансової секретності. Це створює умови для потенційного відмивання кримінальних доходів та обмежує можливості системи протидіяти таким операціям.

Аналіз загального рівня конвергенції системи кібербезпеки та протидії відмиванню кримінальних доходів дозволяє зробити висновок, що цей процес може призвести до позитивного впливу для 32% країн, які були розглянуті в нашому дослідженні. Іншими словами, інтеграція цих систем корисна для підвищення потенційних можливостей країн у протистоянні фінансовим та кібершахрайствам. У майбутньому ми плануємо оцінити можливий вплив здійснення цих процесів на визначені групи країн.

2.2. Модернізація інструментарію протидії легалізації кримінальних доходів та кібершахрайствам

2.2.1. Алгоритми розпізнавання поведінки кібершахраїв

Один із засобів боротьби з кібершахрайством включає в себе використання математичних методів і моделей для створення алгоритмів, які можуть розпізнавати злочинну поведінку в кіберпросторі. Існують численні підходи, які можна використовувати для вирішення різних завдань у сфері протидії та виявлення шахрайств. Серед них особливо поширеними є статистичні методи. Однією з ключових особливостей статистичних методів при аналізі даних є їх здатність усереднювати характеристики вибірки. В більшості випадків ці характеристики представляють собою агреговані значення, і особливо це важливо в реальних процесах, таких як банківська справа, де статистика досліджує широкомасштабні явища, а не окремі випадки. При цьому для ефективного дослідження таких показників важливо враховувати якісний характер даних. Основною метою статистичного аналізу є виявлення закономірностей та залежностей між явищами, перевірка гіпотез, групування даних, аналіз взаємозв'язків між різними величинами та інші аспекти.

При глибшому вивченні методів статистичного аналізу, наприклад, дослідження проведеного Nuha et al. (2021), були ідентифіковані ключові

фактори, що призводять до зростання шахрайства в галузі електронного та мобільного банкінгу. Застосовуючи кореляційний аналіз, вчені встановили значну залежність між відсутністю належного інформування та ймовірністю негативних наслідків у випадках шахрайства. Дослідження вказує на те, що 86,3% осіб, які стали жертвами шахрайства у сфері електронного або мобільного банкінгу, не були свідомі такого виду злочинності, і тому зловмисники здебільшого використовували тактику та емоційні маніпуляції для отримання конфіденційної інформації замість технічних методів вторгнення.

Статистичні методи обмежені в їхній здатності робити припущення в ситуаціях, пов'язаних із кіберзлочинами. Сучасні системи боротьби з кіберзагрозами вдаються до використання інтелектуального аналізу даних (Data Mining). Ця концепція орієнтована на аналіз даних різної природи та перевірку великих обсягів збережених даних, які можуть бути неточними, неповними, суперечливими і різноманітними (Ланде та ін., 2018). Крім того, інтелектуальний аналіз даних — це процес обробки великого обсягу інформації з метою виявлення латентних правил і закономірностей; це процес відкриття раніше невідомих, нетривіальних, практично корисних знань в "сирих" даних, які можуть бути доступними для інтерпретації і прийняття рішень (Дюк та Самойленко, 2001).

З развитком інформаційних технологій з'явилися різноманітні методи інтелектуального аналізу, такі як дерева рішень, нейронні мережі, логістична регресія, системи міркувань на основі аналогій, методи штучного інтелекту, метод BSC (збалансування системи показників), еволюційне програмування, генетичні алгоритми, візуалізація багатовимірних даних, методи обмеженого перебору, предметно-орієнтовані аналітичні системи та інші (Дюк та Самойленко, 2001).

Методи інтелектуального аналізу в банківській справі застосовуються для виявлення шахрайства з використанням дебетових та кредитних карт клієнтів, а також для аналізу сфер електронного та мобільного банкінгу. Вони також використовуються для клієнтської сегментації, щоб вдосконалити маркетингову стратегію, прогнозування змін клієнтури та моделювання обсягів використання банківських послуг. Цей аналіз включає в себе широкий спектр традиційних методів, таких як перевірка гіпотез, факторний аналіз, кореляційний аналіз, канонічний аналіз, регресійний аналіз, кластерний аналіз, а також сучасні методи, такі як дерева класифікації, багатомірне шкалювання, структурне моделювання, дискримінантний аналіз, логлінійний аналіз, дисперсійний аналіз, компоненти дисперсії та аналіз асоціативних правил. Для впровадження цих методів інтелектуального аналізу використовують різноманітні статистичні пакети, такі як Statistica, SPSS, SAS, STATGRAPHICS, STADIA, Python, R, Deductor та інші.

Alshamasi & Menai (2022) розробили метод для виявлення порушень стилю написання в текстових документах та визначення можливих змін авторства, який передбачає розкладання тексту на авторські компоненти. Найбільш ефективним підходом для цієї задачі є групування тексту у стилістично однорідні кластери,

де схожі за стилем фрагменти тексту об'єднуються. Застосування методу кластеризації авторства всередині тексту має важливе застосування в областях, таких як розслідування кіберзлочинів у банківській сфері, судова лінгвістика та інші.

Результати кластеризації часто бувають важко піддати інтерпретації, оскільки вони можуть не відповідати очікуванням або досвіду у відповідній галузі. Під час кластеризації показників у базі даних важливо ретельно аналізувати як позитивні, так і негативні аспекти цього процесу і обирати найбільш підходящі алгоритми. Швидкий прогрес у галузі комп'ютерних технологій призводить до виникнення нових методів обробки інформації, і обсяги доступної інформації невпинно зростають. Отже, сучасним статистичним методам іноді важко ефективно опрацьовувати великі обсяги даних.

Використання нейромереж дозволяє виявляти приховані взаємозв'язки та виділяти схожі класи об'єктів у процесі функціонування системи. Зокрема, нейронні мережі дозволяють обробляти великі обсяги даних та поєднувати алгоритми ієрархічної кластеризації з іншими методами. Важливо відзначити, що нейронні мережі можуть знаходити рішення, навіть якщо вихідні дані не мають очевидних закономірностей або взаємозв'язків між змінними, і навіть при відсутності попередніх знань про вибірку даних. Тим не менше, статистичний аналіз та математичні методи також успішно використовуються для вирішення відповідних завдань. Потенційна швидкодія нейронних мереж базується на їхньому здатності обробляти велику кількість даних паралельно. Нейронні мережі вражають своєю здатністю надавати точні прогнози, визначаючи високу точність у порівнянні зі статистичним аналізом. Крім того, вони мають перевагу у роботі з неповними даними та можуть навчатися (експерт може вільно вибирати математичну модель, оскільки вона адаптивно будується під час навчання). Інші переваги включають високу точність, можливість враховувати нелінійні залежності, а також здатність системи до адаптації, тобто до реакції та пристосування до змін в навколишньому середовищі.

Lekha & Prakasam (2017) вивчають дані щодо кіберзлочинності, використовуючи методи інтелектуального аналізу даних, такі як K-Means, Influenced Association Classifier і Prediction tree. Основною метою їх аналізу є розпізнавання закономірностей в кіберзлочинах з метою передбачення та запобігання їм. В рамках науково-методичного підходу використовується алгоритм K-Means для вибору початкових центроїдів, щоб класифікатор міг обробляти дані і формулювати прогнози щодо кіберзлочинів за допомогою алгоритму Prediction tree. Комбінування цих методів обіцяє поліпшені, об'єднані та точні результати щодо показників кіберзлочинності в банківському секторі, з метою боротьби з кіберзагрозами, передбачення неплатежів, виявлення фальшивих транзакцій та інших аспектів.

Vinayakumar et al. (2019) проводять дослідження щодо використання глибоких нейронних мереж (DNN) – це модель глибокого навчання, для створення гнучкой та ефективної системи IDS (система виявлення вторгнень), призначеної для виявлення та класифікації непередбачуваних кібератак. Це

дослідження спрямоване на визначення найкращого алгоритму, який може надійно виявляти майбутні кібератаки. В рамках комплексної оцінки експериментів DNN порівнюється з різними традиційними класифікаторами машинного навчання за допомогою різних загальнодоступних наборів даних про зловмисне програмне забезпечення.

Kanimozhi & Prem Jacob (2019) розробили методологічний підхід, спрямований на виявлення та класифікацію ботнет-атак, які становлять серйозну загрозу для фінансового сектора та банківських послуг. Використання штучного інтелекту грає важливу роль у процесі виявлення цих кібератак у системах виявлення вторгнень (IDS). Дослідження ґрунтується на реальному наборі даних щодо виявлення вторгнень у галузі кіберзахисту (CSE-CIC-IDS2018), який був створений Канадським інститутом кібербезпеки (CIC) у 2018 році на платформі веб-сервісів Amazon (AWS). Отримана оцінка точності становить 99,97%, і коефіцієнт помилкових позитивних результатів дорівнює 0,001. Тобто використаний метод штучного інтелекту для виявлення атак ботнету є значущим та може бути використаний для аналізу мережевого трафіку в режимі реального часу.

Syniavska et al. (2019) представили математичну модель, спрямовану на вивчення питань протидії кібератакам у сфері електронного банкінгу. В цій моделі використовується класична модель Лотки-Вольтерра з логістичним зростанням і динамічна модель Холлінга-Таннера. В ході застосування теорії біфуркації було виділено різні типи фіксованих точок, такі як сідло, стабільний вузол, стабільний вироджений вузол та лінії стабільних фіксованих точок. Важливо зазначити, що останні з них є малоймовірними в реальних умовах. Однак дану модель можна використовувати для теоретичних та емпіричних досліджень з метою удосконалення системи протидії кібератакам у банківському секторі.

Fedotova et al. (2019) застосували методи Data Mining, включаючи вертикальний, горизонтальний, фінансовий та трендовий аналіз великих обсягів даних для оцінки динаміки та тенденцій розвитку кіберзлочинності в банківській сфері. В рамках дослідження було проведено аналіз ситуації з кіберзлочинністю в банківській системі, розглянуті механізми забезпечення безпеки особистих рахунків, і були розроблені стратегії для вдосконалення інформаційної безпеки платіжних систем у банківському секторі. Дослідники використали методи інтелектуального аналізу даних, такі як систематизація, аналогія та порівняння, для формулювання висновків та рекомендацій з приводу зазначених шляхів підвищення економічної безпеки інформаційних систем банків.

Akinbowale et al. (2020) використовують підхід BSC (збалансування системи показників) для проведення аналізу впливу кіберзлочинності на банківський сектор. На основі цього аналізу запропоновано систему оповіщення з метою запобігання значним збиткам, завданим кіберзлочинністю. Потенційними користувачами цієї системи можуть бути банки та їх клієнти. Шляхом ефективної інтеграції технологій обробки великих обсягів даних у їхні системи, можна пом'якшити негативний вплив кіберзлочинності.

Оскільки методи інтелектуального аналізу є надзвичайно ефективними у боротьбі з кіберзлочинністю, то були розроблені алгоритми для виявлення кіберзлочинних операцій на основі різних підходів, включаючи регресійний аналіз, дерево рішень та нейронні мережі.

Перший алгоритм ґрунтується на використанні регресійного підходу. У випадку шахрайств, розумним рішенням є використовувати логістичну регресію.

Проте, нашим даним не вдалося піддатися побудову логістичної регресійної моделі через незбіжність матриці. Тому ми вирішили застосувати узагальнену регресію, яка дозволить нам робити прогнози не в бінарному вигляді, а у вигляді значень в інтервалі від 0 до 1. Якщо ми маємо значення, що наближаються до 1, то ця ознака вважається вказівкою на можливе зловживання. В іншому випадку, вона не розглядається як зловживання. Під час побудови регресії ми також врахували фіктивні змінні, оскільки наш набір даних включає велику кількість категоріальних ознак, які ми перетворили на фіктивні. Результати узагальненої регресійної моделі наведено на Рисунку 2.20. Всі змінні мають статистичну значущість на рівні значущості менше 0,05, що означає, що вони внесуть вагому вклад до рівняння. Коефіцієнт детермінації становить 0,775, що в цілому свідчить про задовільну якість моделі.

Оскільки модель регресії не є оптимальною для складних алгоритмів, особливо коли маємо велику кількість змінних та нормальний розподіл не враховується, ми створили і перевірили інші моделі регресії, такі як LASSO, RIDGE та Elastic Net. Оцінки цих моделей менше зміщені, що може призвести до кращих результатів у прогнозуванні цільової змінної. Результати оцінок цих регресій представлені на рисунках 2.21-2.23.

OLS Regression Results

Dep. Variable:	y	R-squared:	0.775
Model:	OLS	Adj. R-squared:	0.775
Method:	Least Squares	F-statistic:	5335.
Date:	Thu, 08 Dec 2022	Prob (F-statistic):	0.00
Time:	20:13:28	Log-Likelihood:	4017.0
No. Observations:	193384	AIC:	-7782.
Df Residuals:	193258	BIC:	-6500.
Df Model:	125		
Covariance Type:	nonrobust		

	coef	std err	t	P>|t|	[0.025	0.975]
const	1.3710	0.007	184.444	0.000	1.356	1.386
CNT_CHILDREN	-0.0739	0.002	-36.548	0.000	-0.078	-0.070
AMT_INCOME_TOTAL	2.234e-09	8.23e-10	2.714	0.007	6.2e-10	3.85e-09
AMT_CREDIT	1.43e-07	8.49e-09	16.835	0.000	1.26e-07	1.6e-07
AMT_ANNUITY	2.78e-07	6.29e-08	4.418	0.000	1.55e-07	4.01e-07
AMT_GOODS_PRICE	-1.731e-07	9.42e-09	-18.384	0.000	-1.92e-07	-1.55e-07
DAYS_EMPLOYED	6.704e-06	2.79e-07	24.047	0.000	6.16e-06	7.25e-06
CNT_FAM_MEMBERS	0.0617	0.002	34.713	0.000	0.058	0.065
REGION_RATING_CLIENT	-0.0231	0.003	-7.941	0.000	-0.029	-0.017
REGION_RATING_CLIENT_W_CITY	0.0249	0.003	8.452	0.000	0.019	0.031
HOUR_APPR_PROCESS_START	-0.0019	0.000	-10.478	0.000	-0.002	-0.002
NAME_CONTRACT_TYPE_Cash loans	-0.0487	0.004	-12.731	0.000	-0.056	-0.041
NAME_CONTRACT_TYPE_Revolving loans	-0.0777	0.004	-18.509	0.000	-0.086	-0.069
CODE_GENDER_F	-0.0629	0.002	-36.519	0.000	-0.066	-0.059
CODE_GENDER_M	-0.0434	0.002	-23.715	0.000	-0.047	-0.040
FLAG_OWN_CAR_N	-0.0601	0.002	-36.586	0.000	-0.063	-0.057
FLAG_OWN_CAR_Y	-0.0997	0.002	-51.133	0.000	-0.104	-0.096
FLAG_OWN_REALTY_N	-0.0872	0.002	-44.361	0.000	-0.091	-0.083
FLAG_OWN_REALTY_Y	-0.0681	0.002	-41.674	0.000	-0.071	-0.065
NAME_TYPE_SUITE_Children	-0.1091	0.008	-13.685	0.000	-0.125	-0.093
NAME_TYPE_SUITE_Family	-0.1125	0.003	-41.072	0.000	-0.118	-0.107
NAME_TYPE_SUITE_Group of people	-0.0740	0.025	-2.985	0.003	-0.123	-0.025
NAME_TYPE_SUITE_Other_A	-0.1194	0.013	-8.964	0.000	-0.145	-0.093
NAME_TYPE_SUITE_Other_B	-0.1112	0.010	-11.544	0.000	-0.130	-0.092
NAME_TYPE_SUITE_Spouse, partner	-0.1177	0.004	-27.509	0.000	-0.126	-0.109
NAME_TYPE_SUITE_Unaccompanied	-0.0684	0.002	-39.181	0.000	-0.072	-0.065
NAME_INCOME_TYPE_Businessman	-0.1427	0.084	-1.700	0.089	-0.307	0.022
NAME_INCOME_TYPE_Commercial associate	-0.1076	0.002	-53.949	0.000	-0.112	-0.104
NAME_INCOME_TYPE_Maternity leave	-0.1334	0.237	-0.563	0.574	-0.598	0.331
NAME_INCOME_TYPE_State servant	-0.0878	0.003	-25.912	0.000	-0.094	-0.081
NAME_INCOME_TYPE_Student	-0.1630	0.090	-1.817	0.069	-0.339	0.013
NAME_INCOME_TYPE_Working	-0.0690	0.002	-43.108	0.000	-0.072	-0.066
NAME_EDUCATION_TYPE_Academic degree	-0.1618	0.030	-5.481	0.000	-0.220	-0.104
NAME_EDUCATION_TYPE_Higher education	-0.1036	0.002	-47.031	0.000	-0.108	-0.099
NAME_EDUCATION_TYPE_Incomplete higher	-0.1149	0.004	-29.209	0.000	-0.123	-0.107
NAME_EDUCATION_TYPE_Lower secondary	-0.0900	0.009	-9.873	0.000	-0.108	-0.072
NAME_EDUCATION_TYPE_Secondary / secondary special	-0.0632	0.002	-38.518	0.000	-0.066	-0.060
NAME_FAMILY_STATUS_Civil marriage	-0.1603	0.003	-58.961	0.000	-0.166	-0.155
NAME_FAMILY_STATUS_Married	-0.1353	0.002	-77.191	0.000	-0.139	-0.132
NAME_FAMILY_STATUS_Separated	-0.1087	0.003	-33.060	0.000	-0.115	-0.102
NAME_FAMILY_STATUS_Single / not married	-0.0907	0.002	-36.351	0.000	-0.096	-0.086
NAME_FAMILY_STATUS_Widow	-0.1479	0.005	-30.694	0.000	-0.157	-0.138
NAME HOUSING TYPE Co-op apartment	-0.0665	0.011	-5.883	0.000	-0.089	-0.044
NAME_HOUSING_TYPE_House / apartment	-0.0423	0.002	-23.078	0.000	-0.046	-0.039
NAME_HOUSING_TYPE_Municipal apartment	-0.0678	0.004	-17.497	0.000	-0.075	-0.060
NAME_HOUSING_TYPE_Office apartment	-0.0897	0.008	-10.726	0.000	-0.106	-0.073
NAME_HOUSING_TYPE_Rented apartment	-0.0568	0.007	-8.477	0.000	-0.070	-0.044
NAME_HOUSING_TYPE_With parents	-0.0604	0.004	-16.082	0.000	-0.068	-0.053
OCCUPATION_TYPE_Accountants	-0.2913	0.004	-75.091	0.000	-0.299	-0.284
OCCUPATION_TYPE_Cleaning staff	-0.2803	0.005	-53.581	0.000	-0.291	-0.270
OCCUPATION_TYPE_Cooking staff	-0.2834	0.005	-54.843	0.000	-0.294	-0.273
OCCUPATION_TYPE_Core staff	-0.2447	0.003	-79.875	0.000	-0.251	-0.239
OCCUPATION_TYPE_Drivers	-0.2386	0.003	-73.936	0.000	-0.245	-0.232
OCCUPATION_TYPE_HR staff	-0.2650	0.013	-20.519	0.000	-0.290	-0.240
OCCUPATION_TYPE_High skill tech staff	-0.2792	0.004	-78.292	0.000	-0.286	-0.272
OCCUPATION_TYPE_IT staff	-0.2872	0.013	-21.401	0.000	-0.313	-0.261
OCCUPATION_TYPE_Laborers	-0.2062	0.002	-97.241	0.000	-0.210	-0.202
OCCUPATION_TYPE_Low-skill Laborers	-0.2197	0.009	-24.926	0.000	-0.237	-0.202
OCCUPATION_TYPE_Managers	-0.2613	0.003	-89.404	0.000	-0.267	-0.256
OCCUPATION_TYPE_Medicine staff	-0.2749	0.005	-53.376	0.000	-0.285	-0.265
OCCUPATION_TYPE_Private service staff	-0.3049	0.007	-44.512	0.000	-0.318	-0.291
OCCUPATION_TYPE_Realty agents	-0.3057	0.012	-25.755	0.000	-0.329	-0.282
OCCUPATION_TYPE_Sales staff	-0.2516	0.003	-94.429	0.000	-0.257	-0.246
OCCUPATION_TYPE_Secretaries	-0.2671	0.009	-30.272	0.000	-0.284	-0.250
OCCUPATION_TYPE_Security staff	-0.2583	0.006	-46.931	0.000	-0.269	-0.247
OCCUPATION_TYPE_Waiters/barmen staff	-0.2767	0.010	-27.917	0.000	-0.296	-0.257

Рисунок 2.20 – Результати побудованої узагальненої регресії (початок)

Джерело: розроблено авторами на основі Яровенко та Колотіліна (2022)

ORGANIZATION_TYPE_Advertising	-0.3818	0.016	-23.670	0.000	-0.413	-0.350
ORGANIZATION_TYPE_Agriculture	-0.3875	0.015	-26.396	0.000	-0.416	-0.359
ORGANIZATION_TYPE_Bank	-0.3843	0.007	-56.184	0.000	-0.398	-0.371
ORGANIZATION_TYPE_Business Entity Type 1	-0.3897	0.005	-76.269	0.000	-0.400	-0.380
ORGANIZATION_TYPE_Business Entity Type 2	-0.3858	0.004	-97.820	0.000	-0.393	-0.378
ORGANIZATION_TYPE_Business Entity Type 3	-0.2964	0.002	-142.228	0.000	-0.301	-0.292
ORGANIZATION_TYPE_Cleaning	-0.3882	0.023	-16.797	0.000	-0.433	-0.343
ORGANIZATION_TYPE_Construction	-0.3707	0.005	-78.912	0.000	-0.380	-0.361
ORGANIZATION_TYPE_Culture	-0.3956	0.019	-21.133	0.000	-0.432	-0.359
ORGANIZATION_TYPE_Emergency	-0.4101	0.016	-24.973	0.000	-0.442	-0.378
ORGANIZATION_TYPE_Government	-0.3884	0.004	-87.467	0.000	-0.397	-0.380
ORGANIZATION_TYPE_Hotel	-0.3938	0.014	-28.001	0.000	-0.421	-0.366
ORGANIZATION_TYPE_Housing	-0.4130	0.007	-59.994	0.000	-0.426	-0.399
ORGANIZATION_TYPE_Industry: type 1	-0.4087	0.012	-35.176	0.000	-0.431	-0.386
ORGANIZATION_TYPE_Industry: type 10	-0.3994	0.031	-13.017	0.000	-0.460	-0.339
ORGANIZATION_TYPE_Industry: type 11	-0.4124	0.007	-57.910	0.000	-0.426	-0.398
ORGANIZATION_TYPE_Industry: type 12	-0.4215	0.018	-22.996	0.000	-0.457	-0.386
ORGANIZATION_TYPE_Industry: type 13	-0.3995	0.061	-6.522	0.000	-0.520	-0.279
ORGANIZATION_TYPE_Industry: type 2	-0.4377	0.015	-29.751	0.000	-0.467	-0.409
ORGANIZATION_TYPE_Industry: type 3	-0.4039	0.007	-55.707	0.000	-0.418	-0.390
ORGANIZATION_TYPE_Industry: type 4	-0.3951	0.013	-31.243	0.000	-0.420	-0.370
ORGANIZATION_TYPE_Industry: type 5	-0.4192	0.013	-31.296	0.000	-0.445	-0.393
ORGANIZATION_TYPE_Industry: type 6	-0.4425	0.038	-11.786	0.000	-0.516	-0.369
ORGANIZATION_TYPE_Industry: type 7	-0.4159	0.009	-43.851	0.000	-0.435	-0.397
ORGANIZATION_TYPE_Industry: type 8	-0.2662	0.075	-3.548	0.000	-0.413	-0.119
ORGANIZATION_TYPE_Industry: type 9	-0.4144	0.006	-65.382	0.000	-0.427	-0.402
ORGANIZATION_TYPE_Insurance	-0.4044	0.014	-29.124	0.000	-0.432	-0.377
ORGANIZATION_TYPE_Kindergarten	-0.3839	0.005	-78.271	0.000	-0.394	-0.374
ORGANIZATION_TYPE_Legal Services	-0.3731	0.018	-20.687	0.000	-0.408	-0.338
ORGANIZATION_TYPE_Medicine	-0.3740	0.005	-79.411	0.000	-0.383	-0.365
ORGANIZATION_TYPE_Military	-0.4046	0.008	-50.557	0.000	-0.420	-0.389
ORGANIZATION_TYPE_Mobile	-0.3518	0.018	-19.126	0.000	-0.388	-0.316
ORGANIZATION_TYPE_Other	-0.3811	0.004	-101.841	0.000	-0.388	-0.374
ORGANIZATION_TYPE_Police	-0.3974	0.008	-50.638	0.000	-0.413	-0.382
ORGANIZATION_TYPE_Postal	-0.4205	0.009	-47.057	0.000	-0.438	-0.403
ORGANIZATION_TYPE_Realtor	-0.3115	0.016	-19.238	0.000	-0.343	-0.280
ORGANIZATION_TYPE_Religion	-0.3998	0.053	-7.535	0.000	-0.504	-0.296
ORGANIZATION_TYPE_Restaurant	-0.3589	0.009	-39.170	0.000	-0.377	-0.341
ORGANIZATION_TYPE_School	-0.4010	0.005	-80.566	0.000	-0.411	-0.391
ORGANIZATION_TYPE_Security	-0.3829	0.008	-50.124	0.000	-0.398	-0.368
ORGANIZATION_TYPE_Security Ministries	-0.3957	0.009	-44.663	0.000	-0.413	-0.378
ORGANIZATION_TYPE_Self-employed	-0.3208	0.003	-125.543	0.000	-0.326	-0.316
ORGANIZATION_TYPE_Services	-0.3772	0.009	-42.413	0.000	-0.395	-0.360
ORGANIZATION_TYPE_Telecom	-0.4029	0.014	-28.669	0.000	-0.430	-0.375
ORGANIZATION_TYPE_Trade: type 1	-0.3748	0.018	-21.282	0.000	-0.409	-0.340
ORGANIZATION_TYPE_Trade: type 2	-0.3975	0.008	-51.227	0.000	-0.413	-0.382
ORGANIZATION_TYPE_Trade: type 3	-0.3609	0.006	-58.289	0.000	-0.373	-0.349
ORGANIZATION_TYPE_Trade: type 4	-0.4726	0.042	-11.258	0.000	-0.555	-0.390
ORGANIZATION_TYPE_Trade: type 5	-0.4704	0.045	-10.483	0.000	-0.558	-0.382
ORGANIZATION_TYPE_Trade: type 6	-0.3970	0.014	-28.382	0.000	-0.424	-0.370
ORGANIZATION_TYPE_Trade: type 7	-0.3725	0.004	-84.000	0.000	-0.381	-0.364
ORGANIZATION_TYPE_Transport: type 1	-0.3946	0.029	-13.679	0.000	-0.451	-0.338
ORGANIZATION_TYPE_Transport: type 2	-0.4077	0.008	-51.645	0.000	-0.423	-0.392
ORGANIZATION_TYPE_Transport: type 3	-0.3382	0.010	-32.387	0.000	-0.359	-0.318
ORGANIZATION_TYPE_Transport: type 4	-0.3816	0.005	-73.222	0.000	-0.392	-0.371
ORGANIZATION_TYPE_University	-0.3939	0.010	-40.649	0.000	-0.413	-0.375
HOUSETYPE_MODE_block of flats	-0.0534	0.004	-14.316	0.000	-0.061	-0.046
HOUSETYPE_MODE_specific housing	-0.0719	0.008	-9.044	0.000	-0.087	-0.056
HOUSETYPE_MODE_terraced house	-0.0794	0.009	-8.885	0.000	-0.097	-0.062

Omnibus:	85722.900	Durbin-Watson:	1.933
Prob(Omnibus):	0.000	Jarque-Bera (JB):	383793.968
Skew:	2.207	Prob(JB):	0.00
Kurtosis:	8.306	Cond. No.	4.42e+08

Рисунок 2.20 – Результати побудованої узагальненої регресії (продовження)

Джерело: розроблено авторами на основі Яровенко та Колотіліна (2022)

LASSO регресія (рис. 2.21) має значення коефіцієнта детермінації 0,485, що свідчить про менш задовільну якість моделі. Однак, оскільки оцінки менше зміщені, ніж у випадку узагальненої регресії, цей тип регресії не рекомендується для використання в алгоритмі виявлення кіберзлочинів.

Результат Elastic Net регресії (рис. 2.22) показує коефіцієнт детермінації 0,645, що вказує на середню якість моделі. Ці результати можуть бути корисними в процесі боротьби з кіберзагрозами.

Найбільш ефективною виявилася RIDGE регресія, для якої коефіцієнт детермінації становить 0,775 (рис. 2.23). Хоча це значення відповідає аналогічному для узагальненої регресії, у випадку з даними про кібершахрайства цей вид регресії виявився більш ефективним. Отже, серед запропонованих регресійних моделей ми обираємо RIDGE регресію.

```
[ 0.          -0.           0.          -0.          -0.          -0.
  0.00709414   0.          -0.          -0.          -0.           0.
 -0.          -0.17002758 -0.07068182 -0.07034849 -0.14391311 -0.12767708
 -0.11409848 -0.          -0.02288539 -0.          -0.          -0.
 -0.          -0.          -0.          -0.12148423 -0.          -0.04697268
 -0.          -0.06914145 -0.          -0.10276462 -0.          -0.
 -0.0052286   -0.05142318 -0.12352886 -0.03566322 -0.06989978 -0.00110099
 -0.          -0.          -0.          -0.          -0.          -0.
 -0.          -0.          -0.          -0.02688197 -0.          -0.
 -0.00278777 -0.          -0.04276375 -0.          -0.00402532 -0.
 -0.          -0.          -0.01437364 -0.          -0.          -0.
 -0.          -0.          -0.          -0.          -0.          -0.02625839
 -0.          -0.          -0.          -0.          -0.          -0.
 -0.          -0.          -0.          -0.          -0.          -0.
 -0.          -0.          -0.          -0.          -0.          -0.
 -0.          -0.          -0.          -0.          -0.          -0.
 -0.          -0.          -0.          -0.          -0.          -0.
 -0.          -0.          -0.          -0.          -0.          -0.
 -0.013564    -0.          -0.          -0.          -0.          -0.
 -0.          -0.          -0.          -0.          -0.          -0.
 -0.          -0.          -0.          -0.          -0.          -0.        ]
MSE train: 0.5145631, test: 0.5141511
R^2 train: 0.4854337, test: 0.4858315
```

Рисунок 2.21 – Результати побудованої LASSO регресії

Джерело: розроблено авторами на основі Яровенко та Колотіліна (2022)

```
[ 0.         -0.01195471  0.         -0.         -0.         -0.
  0.02756828  0.         -0.         -0.         -0.          0.
 -0.         -0.14838179 -0.07969526 -0.0889707  -0.14068873 -0.12803405
 -0.1151974  -0.         -0.0554265  -0.         -0.         -0.
 -0.01131085 -0.03925029 -0.         -0.13516669 -0.         -0.06805381
 -0.         -0.09783352 -0.         -0.12103528 -0.0247224  -0.
 -0.0524418  -0.08499625 -0.15366117 -0.07023511 -0.10681343 -0.03914577
 -0.         -0.01679104 -0.00547173 -0.         -0.         -0.
 -0.03612119 -0.02410465 -0.02056971 -0.09074713 -0.0542794  -0.
 -0.05793286 -0.         -0.10552381 -0.         -0.06719768 -0.03489841
 -0.00047365 -0.         -0.07605948 -0.         -0.02778745 -0.
 -0.         -0.         -0.         -0.         -0.01205588 -0.04883392
 -0.         -0.         -0.         -0.         -0.         -0.00404568
 -0.         -0.         -0.         -0.         -0.         -0.
 -0.         -0.         -0.         -0.         -0.         -0.
 -0.         -0.         -0.         -0.         -0.         -0.
 -0.0172396  -0.         -0.         -0.02055019 -0.         -0.
 -0.         -0.         -0.         -0.         -0.         -0.
 -0.03792866 -0.         -0.         -0.         -0.         -0.
 -0.         -0.         -0.         -0.00306903 -0.         -0.
 -0.         -0.         -0.         -0.         -0.         -0.        ]
MSE train: 0.355, test: 0.355
R^2 train: 0.645, test: 0.645
```

Рисунок 2.22 – Результати побудованої Elastic Net регресії

Джерело: розроблено авторами на основі Яровенко та Колотіліна (2022)

```
[ 0.         -0.0935649   0.00296911  0.11892204  0.00761869 -0.12913517
  0.02907017  0.10521608 -0.02273391  0.02370381 -0.01219976 -0.03006902
 -0.04096166 -0.06171671 -0.03961367 -0.05895927 -0.08629575 -0.06966483
 -0.06604109 -0.01495996 -0.05761171 -0.0056295  -0.00891418 -0.01353051
 -0.03252201 -0.05715769 -0.00186482 -0.08727753 -0.00061832 -0.03567371
 -0.00140046 -0.06880264 -0.00650444 -0.08127442 -0.03521828 -0.00921614
 -0.06114914 -0.08044876 -0.1354045  -0.04329814 -0.0566609  -0.03632243
 -0.00629059 -0.03384819 -0.02165712 -0.01174937 -0.0118305  -0.0197203
 -0.0961641  -0.06422306 -0.06753818 -0.13185843 -0.10355067 -0.02263505
 -0.1039079  -0.02503478 -0.15910371 -0.0281121  -0.13233491 -0.08087302
 -0.05384816 -0.02883609 -0.14721941 -0.03208359 -0.06368    -0.03264186
 -0.02671673 -0.02959126 -0.06487991 -0.08927476 -0.12119003 -0.23233962
 -0.01987878 -0.09207939 -0.02309125 -0.04150343 -0.02694944 -0.10920965
 -0.02940132 -0.06811247 -0.03740234 -0.01335678 -0.06399749 -0.02604187
 -0.00782066 -0.0322204  -0.0620455  -0.03387124 -0.03377689 -0.01207303
 -0.04952477 -0.00639443 -0.07446286 -0.03104605 -0.09803155 -0.02329821
 -0.11949942 -0.0584315  -0.02155258 -0.12947565 -0.05920128 -0.05335531
 -0.02226548 -0.00756368 -0.04304942 -0.10174997 -0.06590341 -0.05091359
 -0.18651761 -0.05025029 -0.03154031 -0.02348703 -0.05775551 -0.06606384
 -0.01226029 -0.01163781 -0.03195566 -0.10147148 -0.01543445 -0.05851367
 -0.03635182 -0.0854006  -0.04534433 -0.01753266 -0.00932793 -0.00966927]
MSE train: 0.225, test: 0.225
R^2 train: 0.775, test: 0.775
```

Рисунок 2.23 – Результати побудованої RIDGE регресії

Джерело: розроблено авторами на основі Яровенко та Колотіліна (2022)

Як наступний крок, ми рекомендуємо використовувати дерево рішень. Оскільки наша цільова змінна є бінарною, належить побудувати класифікаційне дерево рішень. Проте перед побудовою такої моделі ми вважаємо за потрібне провести аналіз збалансованості наших змінних, оскільки це має важливе

значення для цього типу моделей. З метою збалансування нашого набору даних, ми застосували метод передискретизації синтетичної меншості. Результати порівняння незбалансованого початкового набору даних і даних після збалансування представлені на Рисунку 2.24.

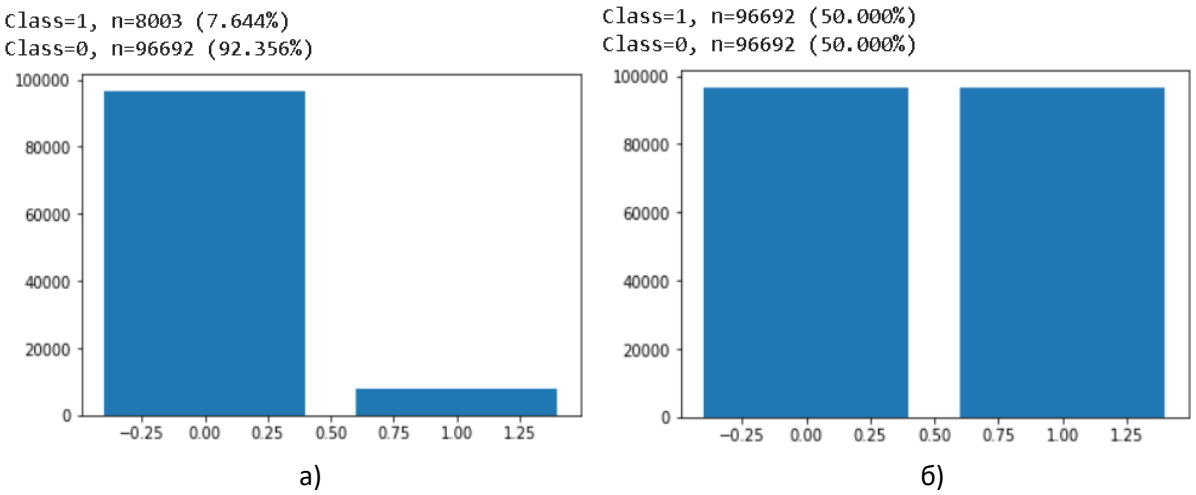


Рисунок 2.24 – Дані до (а) і після (б) методу передискретизації синтетичної меншості

Джерело: розроблено авторами на основі Яровенко та Колотіліна (2022)

Як видно з Рисунку 2.24(а), вихідні дані відповідають кіберзлочинам, становлять лише 7,64% від загального набору. Іншими словами, набір даних не збалансований. Застосування методу передискретизації синтетичної меншості дозволило отримати збалансований набір даних, як показано на Рисунку 2.24(б). Подальше побудова дерев рішень на основі різних видів збалансованих та незбалансованих вибірок підтвердила, що цей алгоритм ефективніше застосовувати на основі збалансованого набору даних.

Для побудови дерева рішень, необхідно визначити його глибину таким чином, щоб модель була зрозумілою та готовою до використання в майбутньому. Тому було проведено аналіз точності розділення гілок дерева рішень для незбалансованих даних за допомогою тестів Джині та ентропії. Результати цього аналізу наведено на Рисунку 2.25.

З даних, представлених на Рисунку 2.25, видно, що максимальну точність можна досягти при глибині дерева рішень рівній 9. Однак, практичний досвід свідчить, що використання великого дерева рішень може ускладнити інтерпретацію моделі. Тому ми готові пожертвувати деякою частиною точності моделі, аби спростити її структуру. В результаті, ми обираємо глибину рівну 7 при умові досягнення точності на рівні 0,9, що є задовільним показником. Ця точність досягається як при використанні ентропійного критерію, так і критерію Джині. Для побудови дерева рішень ми обираємо ентропійний підхід. Результати точності цієї конфігурації представлені на Рисунку 2.26, а сама модель описана на Рисунку 2.27.

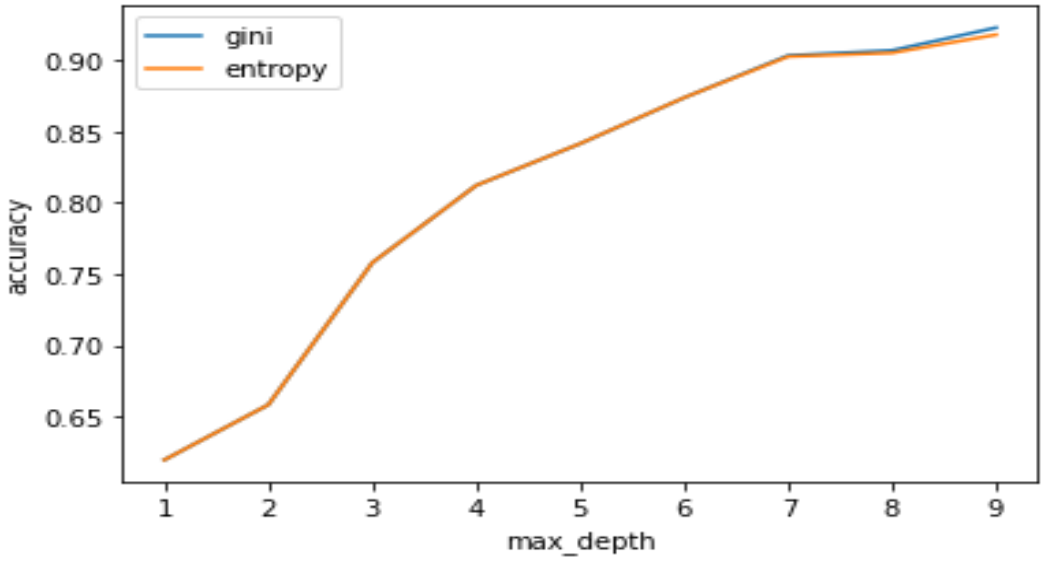


Рисунок 2.25 – Визначення точності поділу гілок дерева рішень за допомогою тесту Джині та ентропії

Джерело: розроблено авторами на основі Яровенко та Колотіліна (2022)

```
Confusion Matrix:
[[19408   161]
 [ 3574 15534]]
Classification Report:
              precision    recall  f1-score   support

           0       0.84      0.99      0.91     19569
           1       0.99      0.81      0.89     19108

    accuracy                           0.90     38677
   macro avg       0.92      0.90      0.90     38677
weighted avg       0.92      0.90      0.90     38677

Accuracy: 0.9034309796519896
```

Рисунок 2.26 – Оцінки якості дерева рішень

Джерело: розроблено авторами на основі Яровенко та Колотіліна (2022)

Загальна ефективність моделі для класів "0" та "1" дуже висока і становить 0,9034. Дерево рішень забезпечує правильний прогноз з імовірністю на рівні 90,34%. Точність класифікації позитивних результатів коливається від 0,84 до 0,99, що свідчить про високу імовірність того, що модель дає багато правильних позитивних прогнозів і мало неправильних позитивних класифікацій. Параметр чутливості для всіх класів знаходиться в діапазоні від 0,81 до 0,99, що підтверджує високу здатність моделі до правильного визначення позитивних результатів. Оскільки немає значних відхилень в показниках точності та відновного виклику, показник F1 має високі значення, що наближаються до 1. Це свідчить про високу ефективність моделі в поєднанні точності та повторюваності. Отже, запропонована модель виявляється дуже якісною. Оскільки її точність перевищує регресійні моделі, можна зробити висновок, що класифікаційне дерево рішень буде більш ефективним.

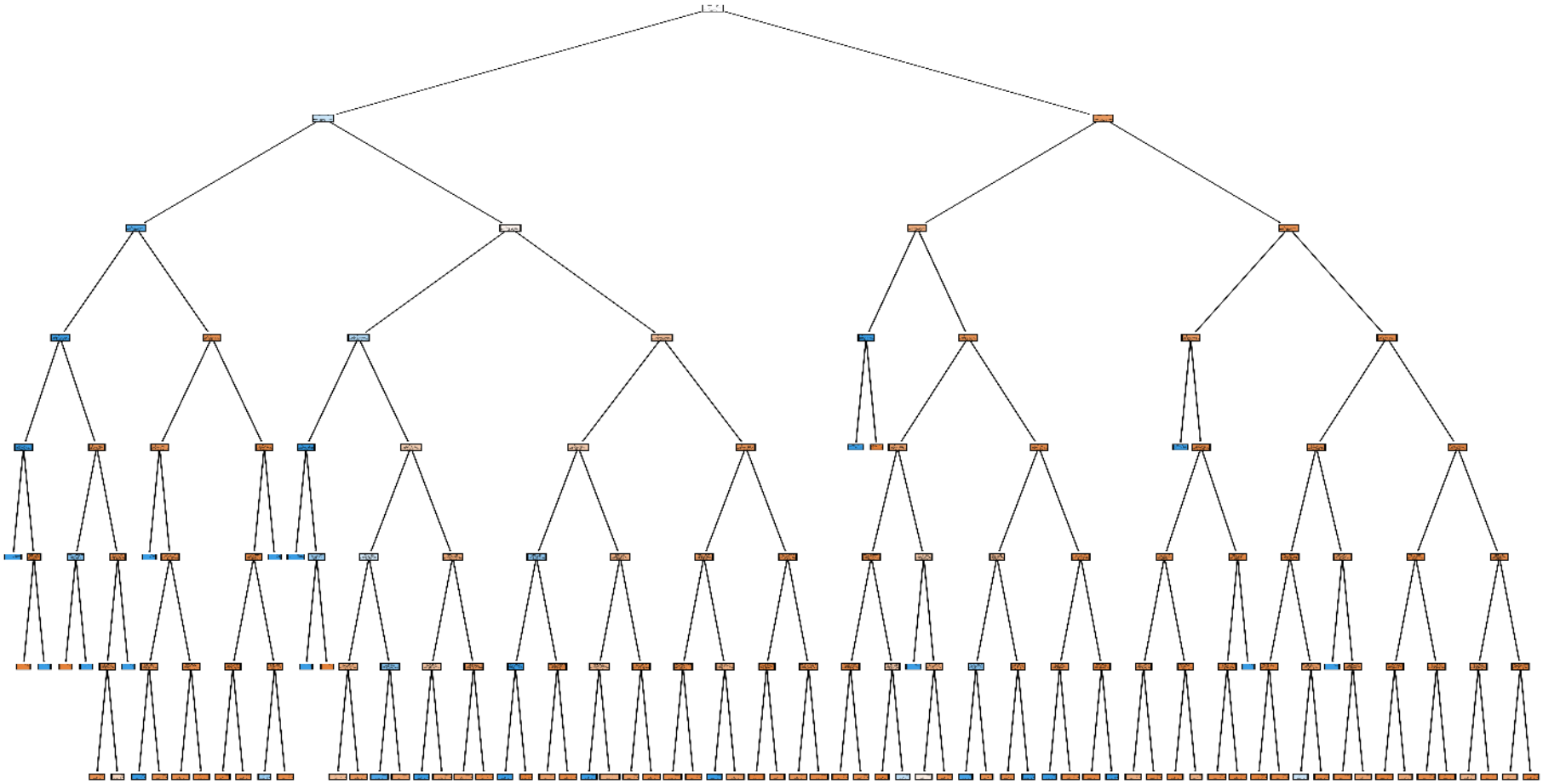


Рисунок 2.27 – Алгоритм розпізнавання поведінки кібершахраїв на основі моделі дерева прогнозних рішень

Джерело: розроблено авторами на основі Яровенко та Колотіліна (2022)

Розглянемо третій алгоритм, який включає в себе створення нейронної мережі. Для цього дослідження ми скористалися Deductor Academic, оскільки цей інструмент дозволяє візуалізувати нейронну мережу, що є важливим завданням і складним для виконання за допомогою інших аналітичних пакетів.

Математичну модель нейронної мережі з урахуванням вхідних та вихідних змінних, пов'язаних з кібершахрайством у сфері кредитних операцій, можна представити за допомогою наступних формул (формули 2.20-2.22) (Яровенко та Колотіліна, 2022):

$$h_1^{(2)} = f\left(w_{1_1}^{(1)} x_1 + w_{1_2}^{(1)} x_2 + \cdots + w_{1_{126}}^{(1)} x_{126} + b_1^{(1)}\right), \quad (2.20)$$

$$h_2^{(2)} = f\left(w_{2_1}^{(1)} x_1 + w_{2_2}^{(1)} x_2 + \cdots + w_{2_{126}}^{(1)} x_{126} + b_2^{(1)}\right), \quad (2.21)$$

$$y\left(\frac{p}{1-p}\right) = f\left(w_1^{(2)} h_1^{(2)} + w_2^{(2)} h_2^{(2)}\right) \quad (2.22)$$

де $f(\cdot)$ – активаційна функція вузла (сигмоїдна або логістична) функція;

$h_1^{(2)}$ – вихід першого вузла у другому шарі нейронної мережі, входами у якій є вихід першого вузла, тобто $\left(w_{1_1}^{(1)} x_1 + w_{1_2}^{(1)} x_2 + \cdots + w_{1_{126}}^{(1)} x_{126}\right)$ та вільний член для даних першого шару $b_1^{(1)}$. Ці входи складаються та передаються в активаційну функцію для розрахунку виходу першого вузла. Інший вузол $h_2^{(2)}$ формується аналогічно;

y – вихід другого вузла у третьому шарі, в якому беруться зважені виходи вузлів другого шару $h_1^{(2)}, h_2^{(2)}$. Для кінцевого виходу p відповідає цільовій змінній, що дорівнює 0, $1-p$ – цільовій змінній, що дорівнює 1 (Яровенко та Колотіліна, 2022).

Для активації внутрішніх шарів та виходів нашої мережі була використана сигмоїдальна (логістична) функція. Функція для активації вихідних вузлів мережі представлена наступним чином (формула 2.23) (Яровенко та Колотіліна, 2022):

$$OUT = \frac{1}{1+\exp(-a \times net)}, \quad (2.23)$$

де OUT – виходи вузлів нейронної мережі у другому та третьому шарах, тобто $h_1^{(2)}, h_2^{(2)}$ та y;

net – сума вхідних сигналів, помножена на відповідні ваги для другого та третього шару, наприклад, $\left(w_{1_1}^{(1)} x_1 + w_{1_2}^{(1)} x_2 + \cdots + w_{1_{126}}^{(1)} x_{126} + b_1^{(1)}\right)$ для $h_1^{(1)}$ (див. формули 2.20-2.22);

a – ступінь крутизни логістичної функції (Яровенко та Колотіліна, 2022).

Візуалізація створеної нейронної мережі представлена на рисунку 2.28. На цій візуалізації можна зауважити, що в мережі наявні 126 вхідних змінних та 3

шари. Третій шар відповідає прогнозуванню значення змінної, яка вказує на наявність або відсутність кіберзлочину.

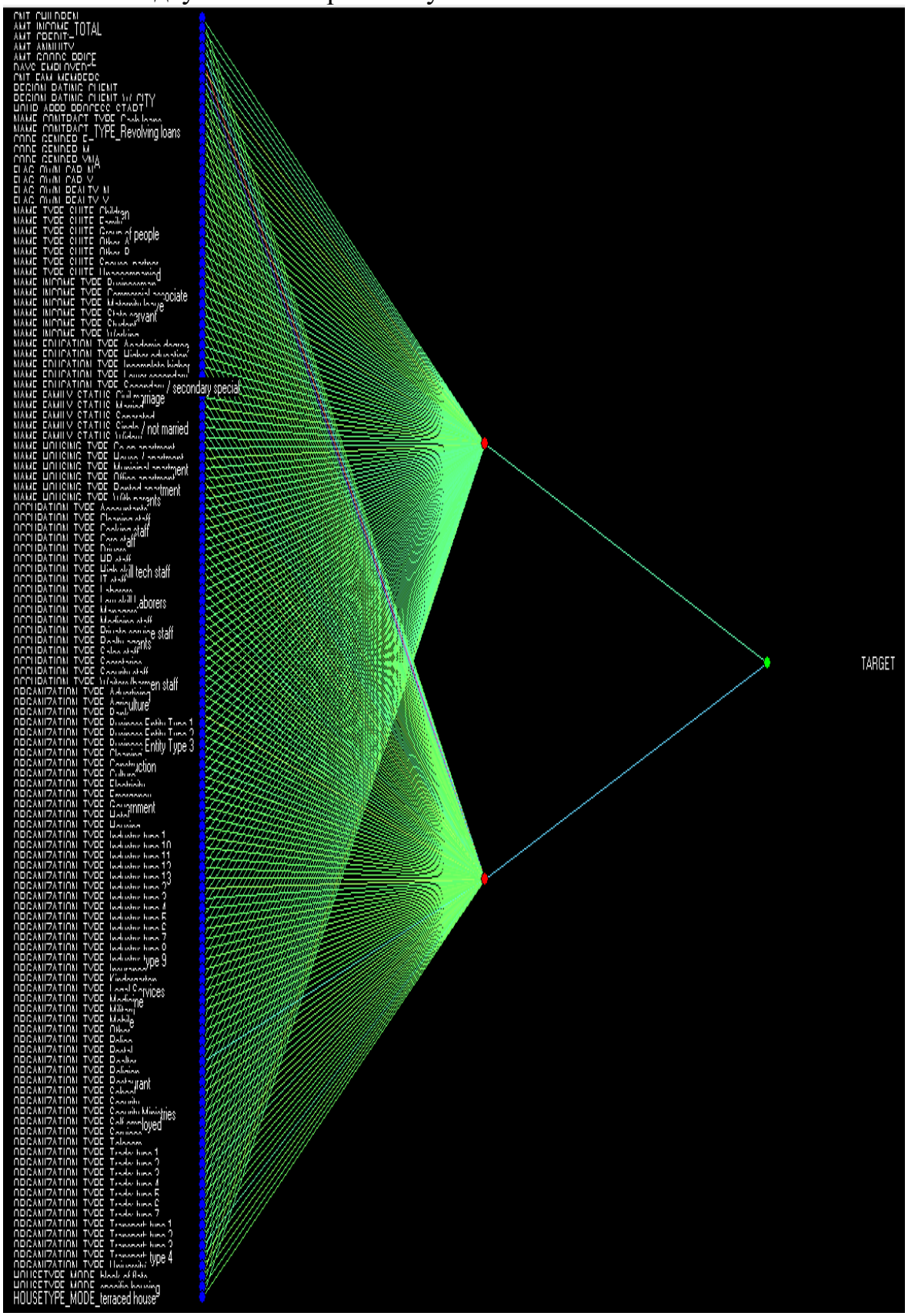


Рисунок 2.28 – Алгоритм розпізнавання поведінки кібершахраїв на основі нейронної моделі

Джерело: розроблено авторами на основі Яровенко та Колотіліна (2022)

Запропонована структура нейронної мережі може здатися насамперед спрощеною. Для оцінки ефективності цієї моделі розглянемо отримані результати, які наведені на рисунку 2.29.

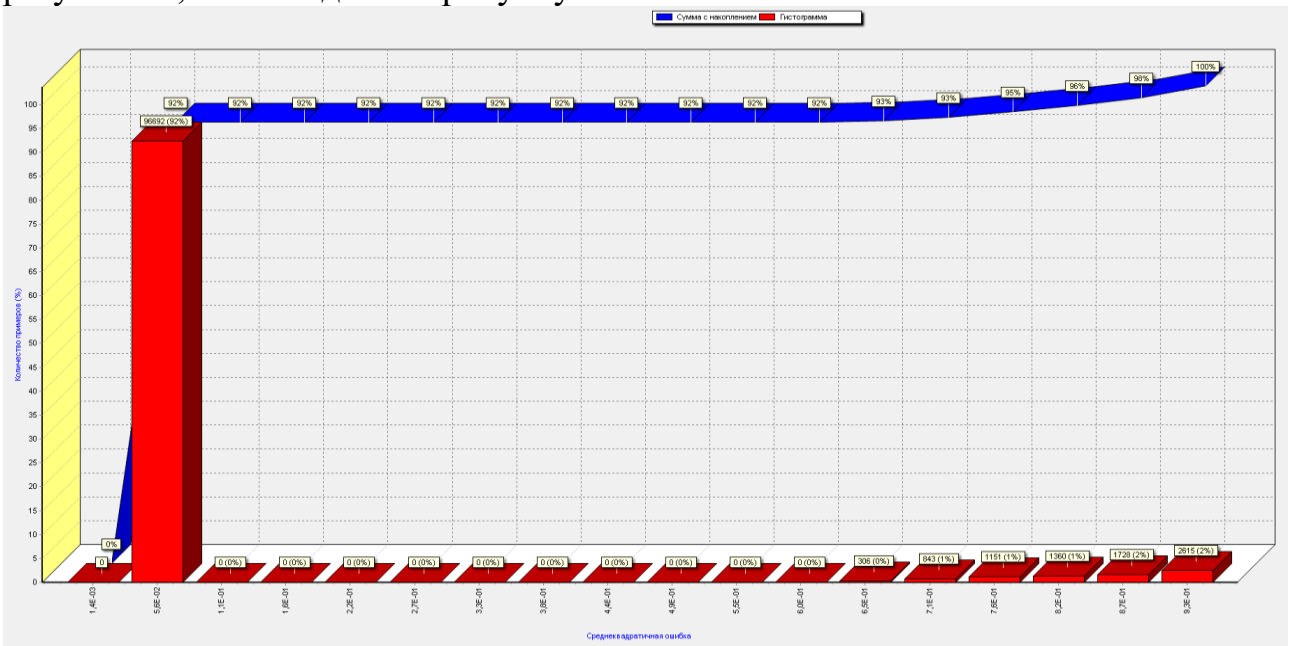


Рисунок 2.29 – Оцінка якості нейронної моделі

Джерело: розроблено авторами на основі Яровенко та Колотіліна (2022)

Графік на рисунку 2.29 вказує на те, що середньоквадратична похибка практично дорівнює 0 для 92% випадків. Навіть при подальших експериментах, які досягають 100%, похибка не перевищує 0,05. Отримані значення свідчать про високу якість алгоритму, побудованого на основі нейронної мережі.

В цьому контексті методи виявлення та протидії кіберзагрозам залишаються актуальними, особливо у відношенні створення відповідних алгоритмів для розпізнавання поведінки кібершахраїв. В даному дослідженні були представлені алгоритми, що базуються на регресійних моделях, класифікаційному дереві рішень та нейронних мережах. Отримані моделі проявили непогані показники якості. Виявилося, що для оцінки поведінки кібершахраїв більш точними є класифікаційне дерево рішень та нейронна мережа. Тому рекомендується впроваджувати їх на практиці в банківських установах для виявлення кіберзагроз на основі створених профілів кіберзлочинців.

2.2.2. Розробка кіберпрофілів сучасних фінансових кіберзлочинів

Профілювання - це процес створення профілів злочинців, які визначають можливі загрози на основі передбачених характеристик. Зазвичай вони формуються на основі існуючих випадків кіберзлочинів. Профілі використовують ретроспективний підхід для аналізу подій, що дозволяє їх постійно оновлювати при надходженні нової інформації про нові кіберзлочини.

Профілювання кіберзлочинів важливо проводити спеціалізованим підрозділам кібербезпеки, які належать до суб’єктів господарювання або державних установ. Саме вони збирають статистичну інформацію щодо кіберзлочинів, загроз, порушень та шахрайства. Проте практично важкості реалізовують цей інструмент кіберзахисту через складність збору та аналізу інформації, який вимагає постійного оновлення і підтримки. Оскільки кіберзлочини постійно еволюціонують завдяки новітнім технологіям, використовуваним злочинцями, процес профілювання повинен базуватися на багатьох ознаках кіберзахисників та злочинів. База даних ознак повинна постійно оновлюватися новою інформацією, яка надходить при виявленні різних кіберзагроз. При розробці профілів також слід враховувати, що вони застосовуються як до самого злочину, так і до осіб, які його вчинили.

Ключовими ознаками, які можуть бути використані при формуванні профілів, є поведінкові риси злочинців в онлайн-середовищі. Це стає актуальним через той факт, що багато фінансових і кіберзлочинів відбуваються в Інтернеті. Злочини можуть бути вчинені через соціальні мережі, інтернет-магазини, блоги, онлайн-повідомлення і інше. Тому важливо враховувати ці аспекти при створенні профілів. Особливу увагу слід звертати на частоту відвідування конкретних веб-ресурсів, способи використання різних інструментів та додатків, незвичайну та непередбачувану поведінку, а також проведення тіньових фінансових операцій і незаконних грошових транзакцій.

Також можна розглядати характеристику щодо відношення злочинця до законодавства своєї країни. Більшість злочинців порушують закони, оскільки багато країн не мають чітко визначених санкцій за кіберзлочини. Зазвичай, за це передбачена адміністративна відповідальність, але у деяких країнах, таких як США і Великобританія, існує кримінальна відповідальність за кіберзлочини. Цю характеристику можна також включити при формуванні профілю кіберзлочинця. Наприклад, на основі бази даних кримінальних злочинців можна визначити осіб зі спеціальною комп'ютерною освітою або тих, хто вчинив кіберзлочини. Для цих зловмисників може бути створено "чорний список", який може бути використаний для постійного моніторингу та ідентифікації кіберзлочинців.

Географічне профілювання є також важливим і дозволяє встановлювати ідентичність злочинців на основі їхнього місцезнаходження. Це досягається шляхом відстеження джерел кібератак та IP-адрес, які використовувалися або використовуються для відправлення вірусів, спаму, кібератак і т. д. Наприклад, деякі онлайн-ресурси, такі як Лабораторія Касперського, демонструють різновиди кібератак в реальному часі, які спрямовані на конкретні країни та виходять із різних країн світу. За аналогічними принципами та можливостями подібних ресурсів можна визначити потенційні країни-атакувальники, тобто ті, звідки походить більшість кібератак у світі. Також можна відслідковувати країни-жертви, тобто ті, які найбільше піддаються кібератакам. Використання цієї інформації допоможе ідентифікувати клієнтів або транзакції, які здійснюються з країн-атакувальників.

Під час створення кіберпрофілю важливо враховувати мотивацію зловмисників, існує два основних типи мотивації. Перший з них пов'язаний з усвідомленим наміром злочинця вчинити злочин. Сюди можна віднести прагнення отримати матеріальну вигоду швидко, позбутися почуття залежності чи обмеженості, цікавість і допитливість, почуття задоволення від здобуття влади, потребу у визнанні чи самоствердженні, а також бажання висловити чи стверджувати політичні чи соціальні позиції та інтереси. Зазвичай такі злочинці виявляються як хитрі та обізнані в усіх аспектах кіберзлочинів і готові піти на будь-які кроки, щоб досягти своєї мети. Цей вид зловмисників представляє небезпеку для індивідів, бізнесу та держави, і їхнє виявлення вимагає значних зусиль та ресурсів, оскільки їхні дії, зазвичай, є добре обдуманими та організованими.

Іншою мотиваційною сферою є фінансові проблеми кіберзлочинця, пов'язані з виплатою кредитів, втратою роботи, низьким рівнем доходу, наявністю численної сім'ї, хворих родичів, вирішенням проблем, пов'язаних із боргами внаслідок азартних ігор і т. д. Зазвичай такі злочинці переходять на кіберзлочинний шлях через певні негативні обставини у своєму житті. Їхні злочини не завжди дотримуються ідеального планування і можуть бути виконані з обмеженими технічними знаннями. Вони користуються простими інструментами та нерідко вдаються до простих форм кіберзлочинів, як-от соціальна інженерія або розсилка програм-вимагачів. Виявлення таких осіб зазвичай менш складне, оскільки їхні дії стандартні та відповідають передбачуваним інструкціям або шаблонам, які вони знаходять в Інтернеті.

Зрозуміло, що методи профілювання кіберзлочинців можуть відрізнятися у деяких аспектах для різних видів кіберзлочинів, але загальні підходи до його формування залишаються однаковими. Процес профілювання включає в себе три спрямовані на індивідів, зловмисне програмне забезпечення або злочини заходи.

Методика, орієнтована на особу, включає в себе аналіз дій кіберзлочинців та їх особистих характеристик. Для цього використовуються різні джерела інформації, опубліковані в засобах масової інформації і в Інтернеті, а також дані, отримані з професійних баз даних щодо кіберзлочинців. Ці матеріали більше схильні відображати типи кіберзлочинів, використовувані засоби, характеристики потенційних жертв, методи вчинення злочинів та інше. Ця інформація допомагає сформувати конкретний портрет особи, яка вчинила злочин. Звісно, цей профіль може бути унікальним в кожному випадку, але більшість кіберзлочинців, тим не менше, матимуть спільні риси.

Підхід, спрямований на зловмисне програмне забезпечення, включає в себе використання знань про аналогічні програми, які використовували або використовуються кіберзлочинцями. Формується база даних відповідних програм на основі ранішнього досвіду щодо кіберзагроз. Також до неї може включатися програмне забезпечення, яке необхідне для виявлення та протидії кіберзлочинам. Це програмне забезпечення аналізує патерни, що ідентифікують потенційні загрози. Точно ці алгоритми можуть бути використані для виявлення

інших ситуацій, якщо вони модифікуються з урахуванням відповідних шаблонів перевірки.

Третій підхід спрямований на конкретний випадок кіберзлочину і використовує ті ж методи, які використовуються в попередніх двох підходах. Це включає створення відповідної бази даних кримінальних випадків з використанням комп'ютерних технологій, де відображаються ключові характеристики цих випадків. Комбінування трьох підходів має більший вплив, оскільки одночасно враховує суб'єкта, який вчиняє кіберзлочин, інструмент, що використовується для його вчинення, і об'єкт, на який спрямований цей злочин.

Для створення кіберпрофілів важливе використання криміналістичних методів ідентифікації, які застосовуються для традиційних злочинців, включаючи кримінально-розшукові, клінічні та статистичні методи. Підхід кримінального розслідування базується на проведенні різних видів експертиз для виявлення схожих випадків у минулому. Проте цей підхід може бути не на 100% ефективним для створення профілю кіберзлочинців через швидкий розвиток технологій та методів, які використовують злочинці, ускладнюючи їх ідентифікацію. Також він потребує постійного оновлення характеристик кіберзлочинців, кіберзлочинів та їх інструментів, але це ускладнено через постійні зміни технік та інструментів, які використовуються злочинцями. У деяких випадках проведення експертизи може допомогти сформувати правдиву картину подій.

Клінічний підхід передбачає створення повної історії злочину, що дозволяє аналізувати його основні характеристики. Цей підхід частково може застосовуватися для виявлення кіберзлочинів, оскільки потребує постійного оновлення історії кіберзлочинів. Проте можуть виникнути труднощі в формуванні клінічної картини через відсутність кваліфікованих фахівців, які могли б оцінити ознаки кіберзагрози. Деякі ситуації можуть навіть потребувати залучення зовнішніх спеціалістів з необхідними знаннями та навичками у програмуванні.

Серед різних підходів, статистичний підхід вважається найбільш ефективним, оскільки він включає в себе використання спеціалізованого програмного забезпечення та методів статистики. Це дозволяє не лише збирати відповідні характеристики, але і проводити відповідні обчислення, що сприяє ідентифікації більшої кількості злочинів. У випадках обмеженої доступної інформації, використовуються непараметричні методи статистики. Коли є більше глибокої інформації, можуть бути корисні методи регресії та байєсовські мережі для профілювання. Класифікація та кластеризація використовуються для створення профілів зі стандартними ознаками та типовими уявленнями про злочинців, підозрюваних, свідків та жертв.

Використання статистичних методів у кіберпрофілюванні виявляється найбільш результативним, оскільки ці методи дозволяють аналізувати різноманітні статистичні параметри, моделювати потенційні сценарії кіберзагроз, прогнозувати ймовірність виникнення кіберзлочинів і багато іншого. Зрозуміло, що використання лише цих методів не гарантує стовідсоткову

ефективність у виявленні загроз. Проте їх поєднання з іншими підходами та методами профілювання сприяє комплексній оцінці ситуацій та розвитку передбачуваних дій, що дозволяють збільшити увагу до конкретних транзакцій, запитів або користувачів системи.

У даному дослідженні було виконане створення кіберпрофілів осіб, які здійснюють незаконні дії у сфері кредитних операцій. У банківському секторі ця проблема є вельми актуальною на сьогоднішній день, оскільки вона пов'язана зі спрощенням умов кредитування та здійсненням фінансових операцій онлайн різними групами населення за допомогою різноманітних мобільних додатків. Також існують способи незаконно здобути кредити, використовуючи чужі особисті дані, або навмисно отримати їх і не виконувати свої фінансові зобов'язання, таким чином сприяючи кібершахрайству. Для реалізації цієї задачі доцільно використовувати метод кластерного аналізу, який дозволить чітко визначити профілі тих клієнтів, у яких є ознаки потенційної злочинної діяльності відносно банку.

Було використано метод кластерного аналізу під назвою "Очікування-максимізація" для виявлення кластерів клієнтів банку, які можуть мати можливий зв'язок з кібершахрайством. Для цього була використана база даних клієнтів одного з банків, яка включає понад 300 тисяч записів. Кожен запис включає 122 атрибути, такі як тип нерухомості клієнта, наявність автомобіля, стать, кількість дітей, середній дохід та його джерело, освіту, суму кредиту, щомісячний платіж і так далі. Одним із центральних атрибутів є характеристика труднощів клієнта при виплаті кредиту. Якщо ця характеристика має значення "1", це може вказувати на ускладнення, які можуть свідчити про можливе кібершахрайство. У випадку значення "0", клієнт не викликає жодних підозр щодо кібербезпеки банку. Фрагмент вхідних даних наведено на рисунку 2.29.

Column1	Row	Description
1	SK_ID_CURR	ID of loan in our sample
2	TARGET	Target variable (1 - client with payment difficulties: he/she had late payment more than X days on at least one of the first Y installments of the loan in our sample, 0 - all other cases)
5	NAME_CONTRACT_TYPE	Identification if loan is cash or revolving
6	CODE_GENDER	Gender of the client
7	FLAG_OWN_CAR	Flag if the client owns a car
8	FLAG_OWN_REALTY	Flag if client owns a house or flat
9	CNT_CHILDREN	Number of children the client has
10	AMT_INCOME_TOTAL	Income of the client
11	AMT_CREDIT	Credit amount of the loan
12	AMT_ANNUITY	Loan annuity
13	AMT_GOODS_PRICE	For consumer loans it is the price of the goods for which the loan is given
14	NAME_TYPE_SUITE	Who was accompanying client when he was applying for the loan
15	NAME_INCOME_TYPE	Clients income type (businessman, working, maternity leave,...)
16	NAME_EDUCATION_TYPE	Level of highest education the client achieved
17	NAME_FAMILY_STATUS	Family status of the client
18	NAME_HOUSING_TYPE	What is the housing situation of the client (renting, living with parents, ...)
19	REGION_POPULATION_RELATIVE	Normalized population of region where client lives (higher number means the client lives in more populated region)
20	DAYS_BIRTH	Client's age in days at the time of application
21	DAYS_EMPLOYED	How many days before the application the person started current employment
22	DAYS_REGISTRATION	How many days before the application did client change his registration
23	DAYS_ID_PUBLISH	How many days before the application did client change the identity document with which he applied for the loan
24	OWN_CAR_AGE	Age of client's car
25	FLAG_MOBIL	Did client provide mobile phone (1=YES, 0=NO)
26	FLAG_EMP_PHONE	Did client provide work phone (1=YES, 0=NO)
27	FLAG_WORK_PHONE	Did client provide home phone (1=YES, 0=NO)
28	FLAG_CONT_MOBILE	Was mobile phone reachable (1=YES, 0=NO)

Рисунок 2.29 – Фрагмент початкових даних для формування кіберпрофілю

Джерело: розроблено авторами на основі Яровенко (2022)

Набір даних містить багато спостережень, які мають пропущену інформацію або викиди та надзвичайно високі значення. У зв'язку з цим було обрано 51 атрибут із загальної кількості 122, і проведено оцінку їхньої якості. Для виконання цього процесу використовувався програмно-аналітичний пакет "Deductor Studio Academic". Результат оцінки наведено на рисунку 2.30.

№	Столбец	Тип данных	Вид данных	Пропуски		Выбросы		Экстремальные		Кол-во уникальных	Качество данных	Резюме
				Кол-во	Действие	Кол-во	Действие	Кол-во	Действие			
6	FLAG_OWN_REALTY	ab Строковый	⋯ Дискретный							2	0,8999	Пригоден
7	CNT_CHILDREN	9.0 Вещественный	⋯ Дискретный			62	Заменять медианой	9	Заменять медианой	9	0,4115	Предобработка
8	AMT_INCOME_TOTAL	ab Строковый	⋯ Дискретный			441	Заменять наиболее ...	939	Заменять наиболее ...	416	0,5693	Предобработка
9	AMT_CREDIT	ab Строковый	⋯ Дискретный			1 906	Заменять наиболее ...	2 423	Заменять наиболее ...	2504	0,7854	Предобработка
10	AMT_ANNUITY	ab Строковый	⋯ Дискретный			2 673	Заменять наиболее ...			6119	0,8925	Предобработка
11	AMT_GOODS_PRICE	ab Строковый	⋯ Дискретный			1 832	Заменять наиболее ...	3 764	Заменять наиболее ...	426	0,6918	Предобработка
12	NAME_TYPE_SUITE	ab Строковый	⋯ Дискретный					1 479	Заменять наиболее ...	8	0,3171	Предобработка
13	NAME_INCOME_TYPE	ab Строковый	⋯ Дискретный			1 249	Заменять наиболее ...	10	Заменять наиболее ...	6	0,5800	Предобработка
14	NAME_EDUCATION_TYPE	ab Строковый	⋯ Дискретный					1 292	Заменять наиболее ...	5	0,4167	Предобработка
15	NAME_FAMILY_STATUS	ab Строковый	⋯ Дискретный			937	Заменять наиболее ...			5	0,7277	Предобработка
16	NAME_HOUSING_TYPE	ab Строковый	⋯ Дискретный			1 736	Заменять наиболее ...	1 817	Заменять наиболее ...	6	0,3284	Предобработка
17	REGION_POPULATION_RELATIVE	ab Строковый	⋯ Дискретный					3	Заменять наиболее ...	80	0,9255	Предобработка
18	DAYS_BIRTH	9.0 Вещественный	⎯ Непрерывный								0,9596	Пригоден
19	DAYS_EMPLOYED	9.0 Вещественный	⎯ Непрерывный								0,1327	Пригоден
20	DAYS_REGISTRATION	ab Строковый	⋯ Дискретный							9930	0,9792	Пригоден
21	DAYS_ID_PUBLISH	9.0 Вещественный	⎯ Непрерывный								0,9422	Пригоден
22	FLAG_MOBIL	0/1 Логический	⋯ Дискретный							1	0,0000	Непригоден
✔ 23	FLAG_EMP_PHONE	0/1 Логический	⋯ Дискретный							2	0,5307	Пригоден
24	FLAG_WORK_PHONE	0/1 Логический	⋯ Дискретный							2	0,7914	Пригоден
25	FLAG_CONT_MOBILE	0/1 Логический	⋯ Дискретный					45	Заменять наиболее ...	2	0,0191	Предобработка
26	FLAG_PHONE	0/1 Логический	⋯ Дискретный							2	0,8032	Пригоден
27	FLAG_EMAIL	0/1 Логический	⋯ Дискретный					1 374	Заменять наиболее ...	2	0,3087	Предобработка
28	OCCUPATION_TYPE	ab Строковый	⋯ Дискретный			327	Заменять наиболее ...	221	Заменять наиболее ...	19	0,7510	Предобработка
29	CNT_FAM_MEMBERS	Дата/Время	⋯ Дискретный	1	Заменять мед...	55	Ограничивать	14	Ограничивать	10	0,5593	Предобработка
30	REGION_RATING_CLIENT	9.0 Вещественный	⋯ Дискретный							3	0,6736	Пригоден
31	REGION_RATING_CLIENT_W_CITY	9.0 Вещественный	⋯ Дискретный							3	0,6660	Пригоден
32	WEEKDAY_APPR_PROCESS_START	ab Строковый	⋯ Дискретный							7	0,9718	Пригоден
33	HOUR_APPR_PROCESS_START	9.0 Вещественный	⎯ Непрерывный			33	Ограничивать				0,7937	Предобработка
34	REG_REGION_NOT_LIVE_REGION	0/1 Логический	⋯ Дискретный					433	Заменять наиболее ...	2	0,1268	Предобработка
35	REG_REGION_NOT_WORK_REGION	0/1 Логический	⋯ Дискретный					1 388	Заменять наиболее ...	2	0,3110	Предобработка
36	LIVE_REGION_NOT_WORK_REGION	0/1 Логический	⋯ Дискретный					1 056	Заменять наиболее ...	2	0,2538	Предобработка
37	REG_CITY_NOT_LIVE_CITY	0/1 Логический	⋯ Дискретный							2	0,5247	Пригоден
38	REG_CITY_NOT_WORK_CITY	0/1 Логический	⋯ Дискретный							2	0,8848	Пригоден
39	LIVE_CITY_NOT_WORK_CITY	0/1 Логический	⋯ Дискретный							2	0,7632	Пригоден
40	ORGANIZATION_TYPE	ab Строковый	⋯ Дискретный			978	Заменять наиболее ...	1 706	Заменять наиболее ...	58	0,6917	Предобработка
41	EXT_SOURCE_2	ab Строковый	⋯ Дискретный							21988	0,9900	Пригоден
42	FONDKAPREMONT_MODE	ab Строковый	⋯ Дискретный					1 548	Заменять наиболее ...	5	0,4928	Предобработка
43	HOUSETYPE_MODE	ab Строковый	⋯ Дискретный					255	Заменять наиболее ...	4	0,5332	Предобработка
44	TOTALAREA_MODE	ab Строковый	⋯ Дискретный					11 119	Заменять наиболее ...	2644	0,5123	Предобработка
45	WALLSMATERIAL_MODE	ab Строковый	⋯ Дискретный					1 562	Заменять наиболее ...	8	0,5746	Предобработка
46	EMERGENCYSTATE_MODE	ab Строковый	⋯ Дискретный					223	Заменять наиболее ...	3	0,6677	Предобработка
47	OBS_30_CNT_SOCIAL_CIRCLE	Дата/Время	⋯ Дискретный	13 097	Оставить без и...	263	Оставить без измен...			12	0,0000	Непригоден
48	DEF_30_CNT_SOCIAL_CIRCLE	Дата/Время	⋯ Дискретный	21 134	Оставить без и...	35	Оставить без измен...	9	Оставить без измен...	6	0,0000	Непригоден
49	OBS_60_CNT_SOCIAL_CIRCLE	Дата/Время	⋯ Дискретный	13 164	Оставить без и...	254	Оставить без измен...			12	0,0000	Непригоден
50	DEF_60_CNT_SOCIAL_CIRCLE	Дата/Время	⋯ Дискретный	22 030	Оставить без и...	95	Оставить без измен...	18	Оставить без измен...	5	0,0000	Непригоден

Рисунок 2.30 – Результат оцінки якості початкових даних

Джерело: розроблено авторами на основі Яровенко (2022)

З обраних даних система визначила, що 4 атрибути є непридатними. Щодо інших атрибутів, вони містять викиди та надзвичайно високі значення. Для цих атрибутів були застосовані процедури заповнення пропусків та видалення викидів і надзвичайних значень. Результат цієї обробки подано на рисунку 2.31.

Незважаючи на те, що після проведених процедур не вдалося повністю усунути всі недоліки, проте якість набору даних відчутно покращилася. Також було виявлено додаткові дані, які не придатні для аналізу і не будуть враховані в майбутньому моделюванні.

№	Столбец	Тип данных	Вид данных	Пропуски		Выбросы		Экстремальные		Кол-во уникальных	Качество данных	Резюме
				Кол-во	Действие	Кол-во	Действие	Кол-во	Действие			
1	SK_ID_CURR	9.0 Вещественный	Непрерывный								0,9999	Пригоден
2	TARGET	9.0 Вещественный	Дискретный							1	0,0000	Непригоден
3	NAME_CONTRACT_...	ab Строковый	Дискретный							1	0,0000	Непригоден
4	CODE_GENDER	ab Строковый	Дискретный							2	0,9855	Пригоден
5	FLAG_OWN_CAR	ab Строковый	Дискретный							2	0,8875	Пригоден
6	FLAG_OWN_REALTY	ab Строковый	Дискретный							2	0,8999	Пригоден
7	CNT_CHILDREN	9.0 Вещественный	Дискретный							3	0,7405	Пригоден
8	AMT_INCOME_TOTAL	ab Строковый	Дискретный			873	Заменять наиболее ...	60	Заменять наиболее ...	46	0,7961	Предобработка
9	AMT_CREDIT	ab Строковый	Дискретный			1 445	Заменять наиболее ...	10 076	Заменять наиболее ...	571	0,7492	Предобработка
10	AMT_ANNUITY	ab Строковый	Дискретный			2 019	Заменять наиболее ...	16 129	Заменять наиболее ...	3445	0,8442	Предобработка
11	AMT_GOODS_PRICE	ab Строковый	Дискретный			643	Заменять наиболее ...	5 239	Заменять наиболее ...	49	0,7051	Предобработка
12	NAME_TYPE_SUITE	ab Строковый	Дискретный							2	0,5328	Пригоден
13	NAME_INCOME_TYPE	ab Строковый	Дискретный							3	0,7805	Пригоден
14	NAME_EDUCATION_...	ab Строковый	Дискретный							2	0,6379	Пригоден
15	NAME_FAMILY_STA...	ab Строковый	Дискретный							4	0,7415	Пригоден
16	NAME_HOUSING_TY...	ab Строковый	Дискретный							1	0,0000	Непригоден
17	REGION_POPULATI...	ab Строковый	Дискретный							79	0,9280	Пригоден
18	DAYS_BIRTH	9.0 Вещественный	Непрерывный								0,9596	Пригоден
19	DAYS_EMPLOYED	9.0 Вещественный	Непрерывный								0,1327	Пригоден
20	DAYS_REGISTRATION	ab Строковый	Дискретный							9930	0,9792	Пригоден
21	DAYS_ID_PUBLISH	9.0 Вещественный	Непрерывный								0,9422	Пригоден
22	FLAG_MOBIL	0/1 Логический	Дискретный							1	0,0000	Непригоден
23	FLAG_EMP_PHONE	0/1 Логический	Дискретный							2	0,5307	Пригоден
24	FLAG_WORK_PHONE	0/1 Логический	Дискретный							2	0,7914	Пригоден
25	FLAG_CONT_MOBILE	0/1 Логический	Дискретный					45	Заменять наиболее ...	2	0,0191	Предобработка
26	FLAG_PHONE	0/1 Логический	Дискретный							2	0,8032	Пригоден
27	FLAG_EMAIL	0/1 Логический	Дискретный					1 374	Заменять наиболее ...	2	0,3087	Предобработка
28	OCCUPATION_TYPE	ab Строковый	Дискретный							13	0,8183	Пригоден
29	CNT_FAM_MEMBERS	Дата/Время	Непрерывный								0,4611	Пригоден
30	REGION_RATING_C...	9.0 Вещественный	Дискретный							3	0,6736	Пригоден
31	REGION_RATING_C...	9.0 Вещественный	Дискретный							3	0,6660	Пригоден
32	WEEKDAY_APPR_P...	ab Строковый	Дискретный							7	0,9718	Пригоден
33	HOUR_APPR_PROC...	9.0 Вещественный	Непрерывный								0,8521	Пригоден
34	REG_REGION_NOT_...	0/1 Логический	Дискретный					433	Заменять наиболее ...	2	0,1268	Предобработка
35	REG_REGION_NOT_...	0/1 Логический	Дискретный					1 388	Заменять наиболее ...	2	0,3110	Предобработка
36	LIVE_REGION_NOT_...	0/1 Логический	Дискретный					1 056	Заменять наиболее ...	2	0,2538	Предобработка
37	REG_CITY_NOT_LIV...	0/1 Логический	Дискретный							2	0,5247	Пригоден
38	REG_CITY_NOT_WO...	0/1 Логический	Дискретный							2	0,8848	Пригоден
39	LIVE_CITY_NOT_WO...	0/1 Логический	Дискретный							2	0,7632	Пригоден
40	ORGANIZATION_TYPE	ab Строковый	Дискретный			1 033	Заменять наиболее ...	726	Заменять наиболее ...	19	0,7594	Предобработка
41	EXT_SOURCE_2	ab Строковый	Дискретный							21988	0,9900	Пригоден
42	FONDKAPREMONT_...	ab Строковый	Дискретный							2	0,7367	Пригоден
43	HOUSETYPE_MODE	ab Строковый	Дискретный							2	0,9819	Пригоден
44	TOTALAREA_MODE	ab Строковый	Дискретный							1	0,0000	Непригоден
45	WALLSMATERIAL_M...	ab Строковый	Дискретный							3	0,8237	Пригоден
46	EMERGENCYSTATE...	ab Строковый	Дискретный							2	0,9920	Пригоден

Рисунок 2.31 – Кінцевий результат оцінки якості початкових даних

Джерело: розроблено авторами на основі Яровенко (2022)

Наступним етапом був проведений кластерний аналіз за допомогою методу "Очікування-максимізація", який використовувався для створення профілів потенційних кібершахраїв, які здійснюють кредитні операції. Цей ітераційний метод формування груп базується на максимальній правдоподібності або максимальних апостеріорних оцінках параметрів. Однією з переваг цього алгоритму є його здатність виявити приховані змінні, які можуть значно впливати на цільовий показник. Це корисно, оскільки аналітик або фахівець з кібербезпеки може не завжди виявити всі можливі ознаки. В результаті було створено 10 кластерів користувачів, які можна подальше проаналізувати на предмет можливого кібершахрайства у сфері кредитних операцій. Результати зв'язків між цими кластерами представлені на рисунку 2.32, де ви можете оцінити міцність кластерів, максимальну похибку розпізнання та середню похибку розпізнання.

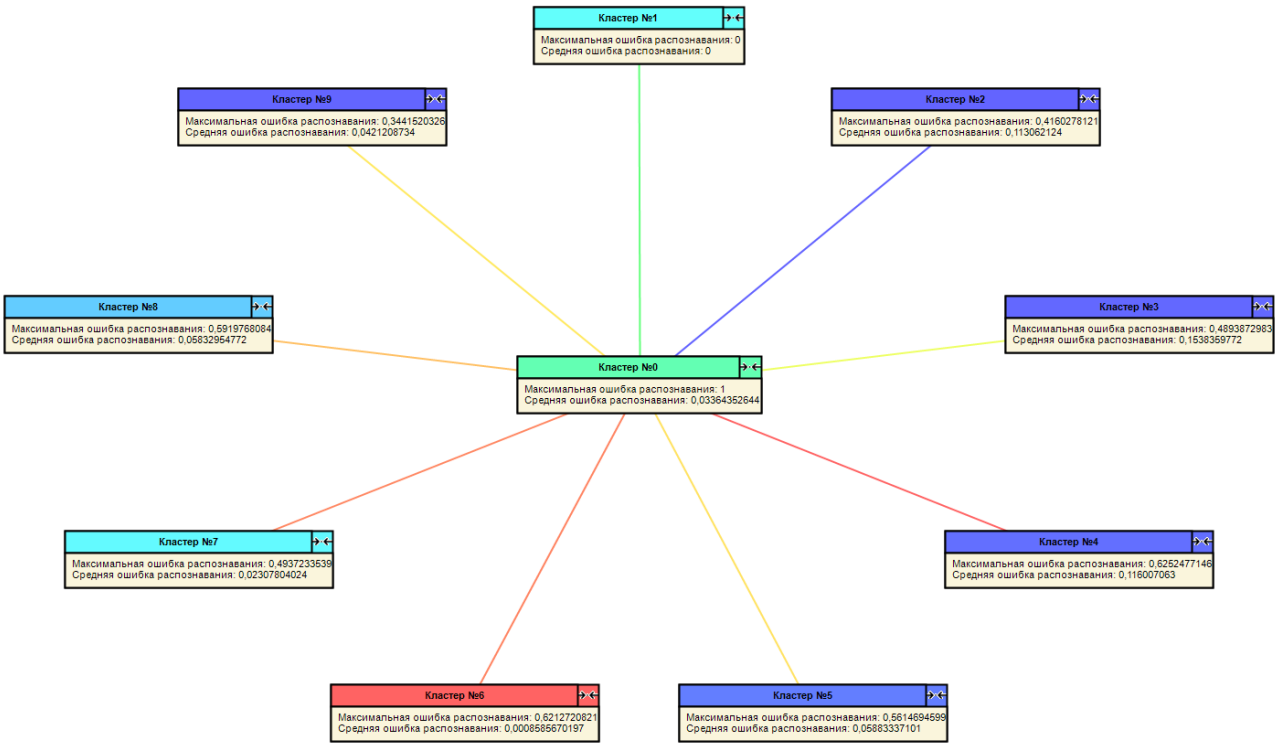


Рисунок 2.32 – Результати зв’язків між кластерами

Джерело: розроблено авторами на основі Яровенко (2022)

Кластери № 4, 3, 1, 7, та 9 виявилися найбільш впливовими. Хоча можлина була б зменшити їх кількість до 5, ми вирішили залишити поточну конфігурацію. Це дозволить нам створити більш докладні профілі злочинців, враховуючи різноманітність індивідуальних характеристик кожного кластеру. В разі отримання нової інформації ця кількість профілів сприятиме їх уточненню та більш детальній класифікації кіберзлочинців.

Рисунок 2.33 – Фрагмент профілів кіберзлочинців

Джерело: розроблено авторами на основі Яровенко (2022)

П'ять перших кластерів мають найбільшу кількість користувачів, і, отже, при ідентифіфації потенційних кіберзлочинців ймовірність їхнього віднесення до цих кластерів є найвищою порівняно з іншими випадками. Ці кластери будуть формувати основний набір характеристик, які відповідають потенційним загрозам. Рисунок 2.33 показує, що більшість випадків мають невизначений тип будинку (атрибут "HOUSETYPE_MODE"). Візуалізація наповненості кластерів користувачів за цією характеристикою наведена на рисунку 2.34. Це пов'язано з відсутністю вихідних даних і відзначенням цієї характеристики як "невизначений тип".

Але виявлені кібершахраї в 3, 1 та 7 кластерах в основному мають "Багатоквартирний будинок" як тип нерухомості. Це можна пояснити тим, що більшість клієнтів банку є власниками такого роду нерухомості, і саме ця категорія клієнтів часто звертається до банків для отримання кредитів на придбання житла. В цьому контексті важливо зауважити, що ці клієнти можуть потрапити до категорії кібершахраїв.

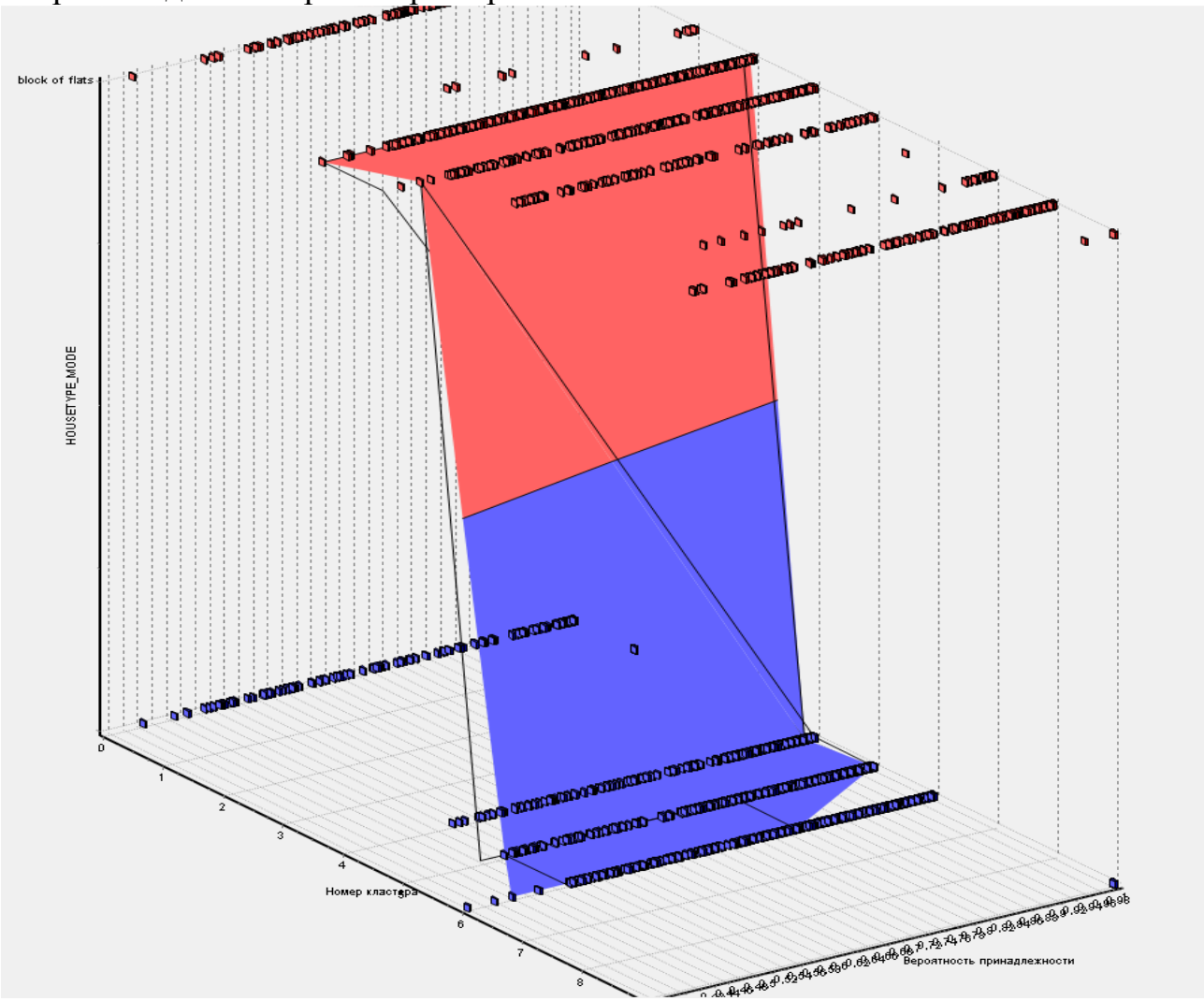


Рисунок 2.34 – Візуалізація характеристики “HOUSETYPE_MODE”

Джерело: розроблено авторами на основі Яровенко (2022)

Аналізуючи змінну "FONDKAPREMONT_MODE", можна відзначити, що якість житла, якою володіє окрема особа, має значення для 3, 1 та 7 кластерів.

Візуалізація наповненості кластерів клієнтів за цією характеристикою представлена на рисунку 2.35. Для інших кластерів ця характеристика залишається невизначеною, що може вказувати на її обмежений вплив в цих випадках. Однак потенційні зловмисники, які відповідають кластерам 3, 1 та 7, можуть мати стимул до здійснення злочину, пов'язаного з поліпшенням житлових умов або зміною типу нерухомості. Важливо зауважити, що намагання особи отримати кредит для цієї мети не означає автоматично відмову від боку банку. Замість цього, отримання інформації, що клієнт може бути потенційним зловмисником, оскільки він належить до певного кластера за цими ознаками, може призвести до проведення додаткових перевірок і аналізу за іншими критеріями.

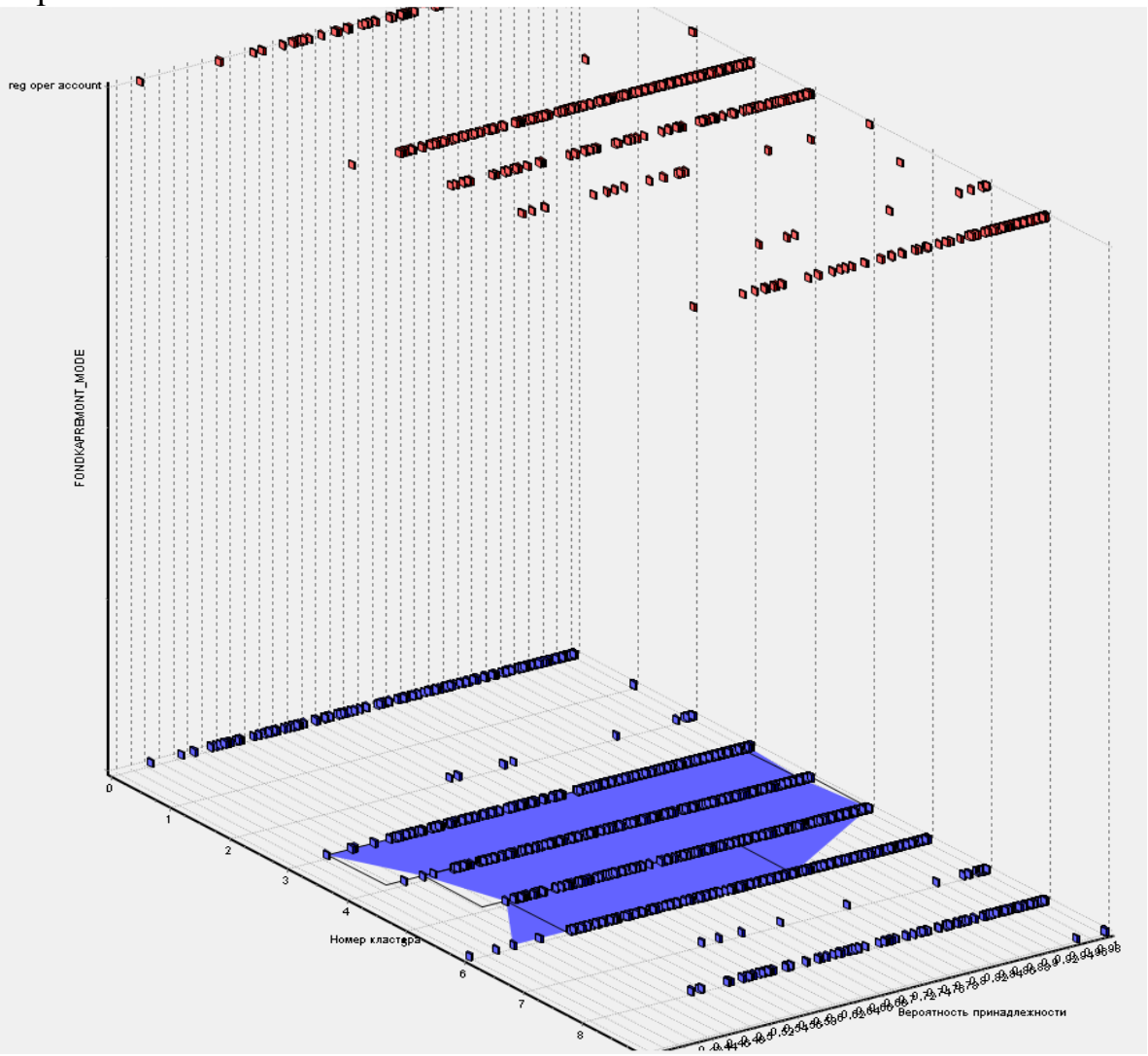


Рисунок 2.35 – Візуалізація характеристики “FONDKAPREMONT_MODE”

Джерело: розроблено авторами на основі Яровенко (2022)

Щодо наступної характеристики, такої як "ORGANIZATION_TYPE", вона вказує на вид діяльності клієнта. Графічне представлення наповненості кластерів клієнтів за цією характеристикою наведено на рисунку 2.36. Можна помітити, що 1-й кластер включає головним чином тих, чий вид діяльності ідентифікується як "XNA". Оскільки в наявності не було розшифровок у використаних даних,

важко визначити, що конкретно позначає ця абревіатура. До 4, 3 та 7 кластерів увійшли особи, чиї види діяльності визначаються як "Business Entity Type 3". Також 20,2% клієнтів у 4-му кластері є самозайнятими. Ймовірно, що ці зловмисники мають фінансові труднощі, пов'язані з їх видом діяльності, які можуть потребувати додаткових інвестицій, розширення або погашення боргів. Тому вони можуть схилятися до злочинних схем, таких як незаконне одержання кредиту або невідшкодування його.

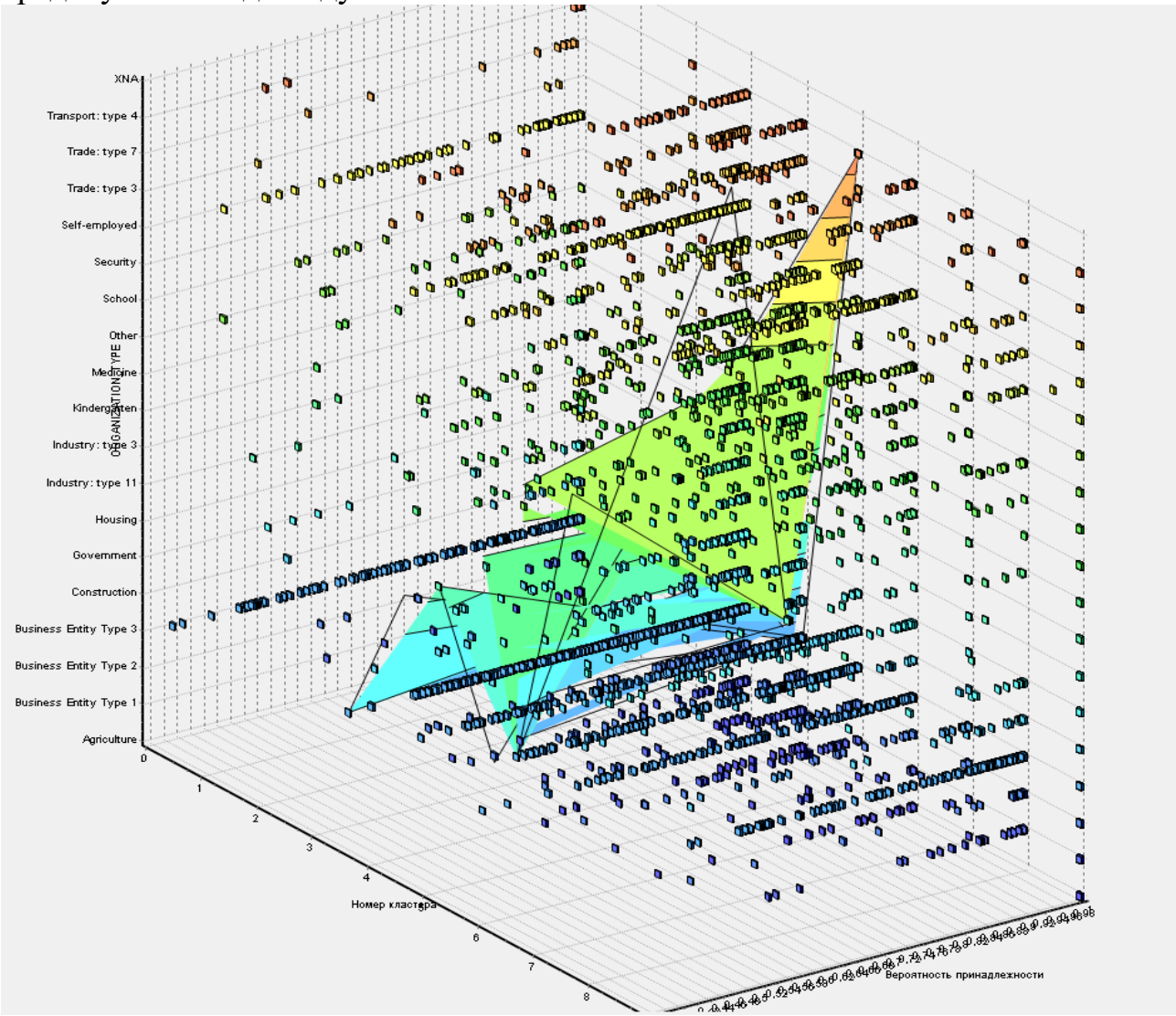


Рисунок 2.36 – Візуалізація характеристики “ORGANIZATION_TYPE”

Джерело: розроблено авторами на основі Яровенко (2022)

При формуванні профілю важливим аспектом є сімейний статус, який відображено в "NAME_FAMILY_STATUS". На рисунку 2.37 наведено графічне представлення наповненості кластерів клієнтів за цією характеристикою. За значеннями кластерів видно, що більшість клієнтів банку є одруженими або заміжніми. Ми вважаємо, що саме сімейні особи можуть звертатися до кіберзлочинності з різних мотивів, таких як нездатність утримувати сім'ю, присутність хворого члена сім'ї або бажання задовольнити свої потреби, які вимагають значних фінансових ресурсів.

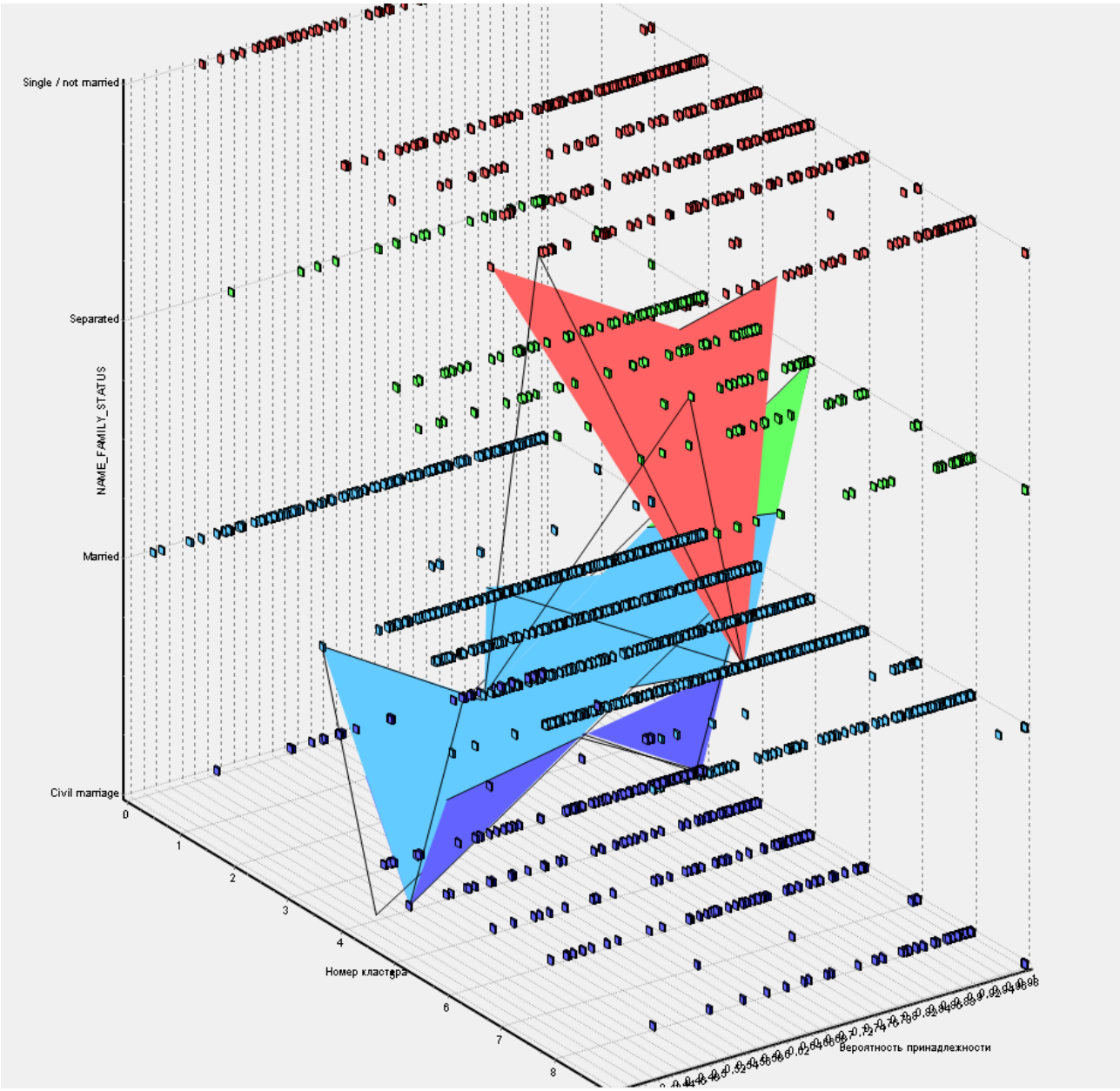


Рисунок 2.37 – Візуалізація характеристики “NAME_FAMILY_STATUS”

Джерело: розроблено авторами на основі Яровенко (2022)

Дуже цікавою виявилася характеристика, яка стосується рівня освіти клієнтів. На рисунку 2.38 надано графічне подання розподілу клієнтів по кластерах за цією характеристикою. Виявлено, що кіберзлочинцями можуть бути як ті, хто має лише базову освіту (завершили середню школу), так і ті, хто має вищу освіту. Основна частина зловмисників відноситься до першої категорії, яка завершила середню школу. Ймовірно, ці особи не досягли визначених життєвих досягнень і можуть шукати швидкий шлях до самореалізації через простий вид кібершахрайства, такий як шахрайство з кредитними операціями. Такі злочинці часто діють за типовими сценаріями і їх легше виявити. Проте варто відзначити, що приблизно 10-20% клієнтів мають вищу освіту, і кожен кластер містить кілька таких потенційних злочинців. Ця категорія осіб може бути досить мотивованою, і їм може бути властиве злочинність заради самовдосконалення або задоволення гострих почуттів. Виявлення таких кандидатів ускладнене, оскільки вони не

тільки мають вищу освіту, але й мають стабільну роботу, що може сприяти побудові позитивної кредитної історії.

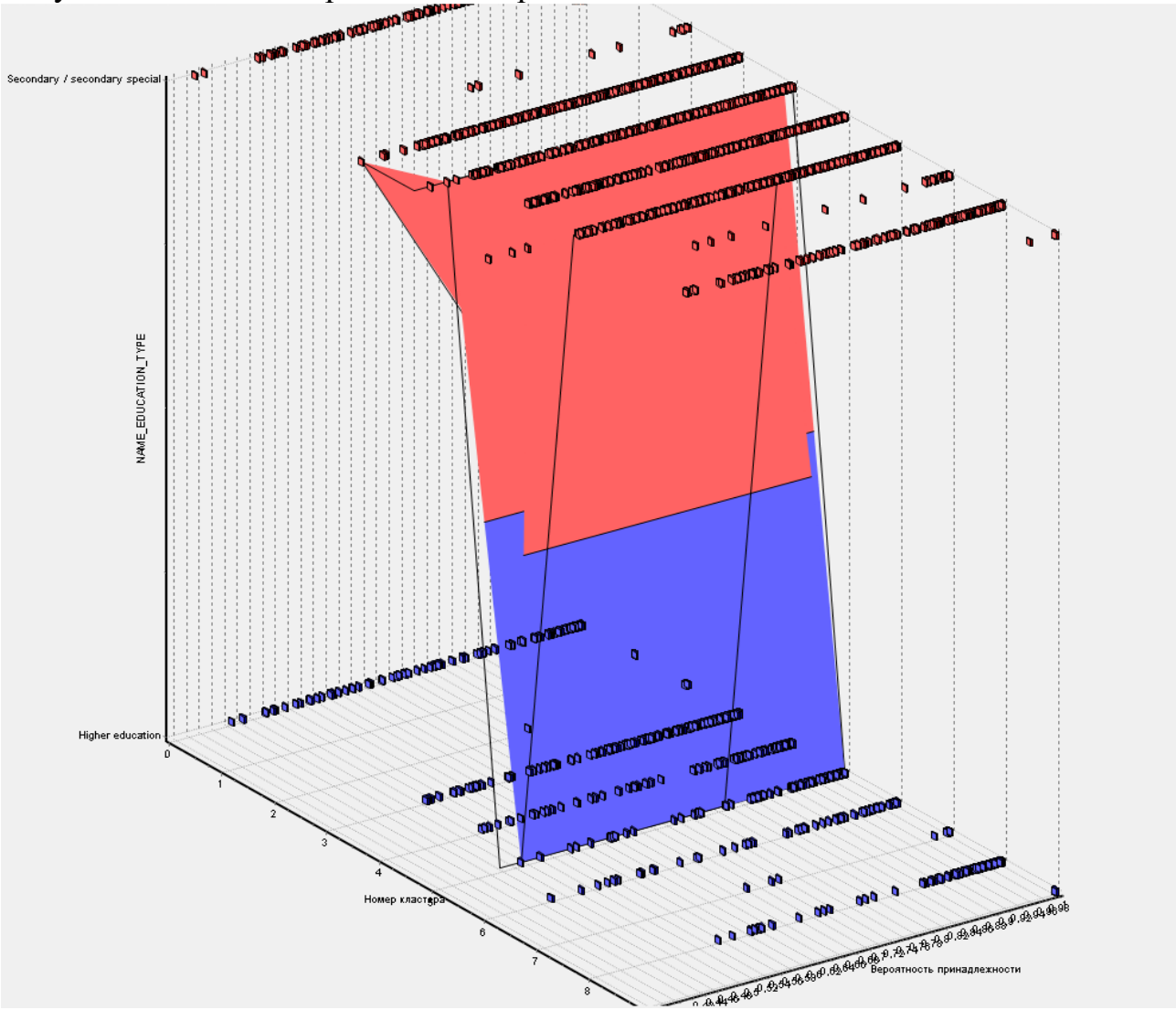


Рисунок 2.38 – Візуалізація характеристики “NAME_EDUCATION_TYPE”

Джерело: розроблено авторами на основі Яровенко (2022)

Щодо джерела доходу, представленої як "NAME_INCOME_TYPE," виявлення наповненості кластерів клієнтів можна побачити на рисунку 2.39. Здавалося б, більшість зловмисників отримує дохід від роботи або участі в комерційних об’єднаннях. Однак особливу увагу привертає кластер №1, де зосереджені клієнти, які отримують пенсії. Враховуючи попередні ознаки, виявляється, що цей кластер включає в себе зловмисників, які перебувають на пенсії, мають базову освіту, сімейний статус, і, можливо, стикаються з житловими труднощами. Отже, цей кластер може бути високоризиковим щодо видання кредиту і його подальшого повернення. Навіть якщо клієнт не має явних намірів щодо кібершахрайства, існують різні чинники, які можуть стати перешкодою відшкодування боргу перед банком.

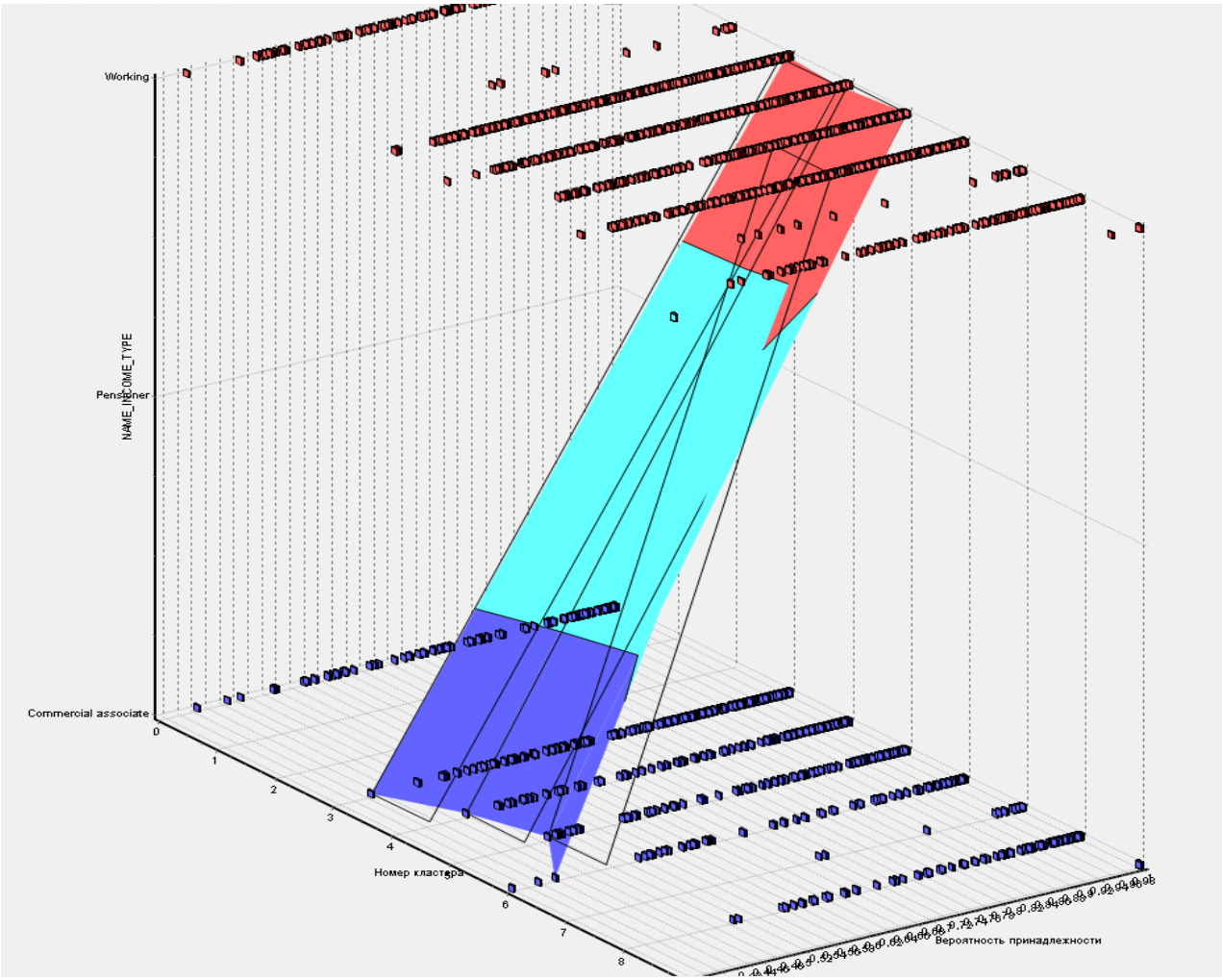


Рисунок 2.39 – Візуалізація характеристики “NAME_INCOME_TYPE”

Джерело: розроблено авторами на основі Яровенко (2022)

Наступною розглянутою характеристикою є "WEEKDAY_APPR_PROCESS_START," і графічне зображення наповненості кластерів клієнтів представлено на рисунку 2.40. Виявлено, що більшість клієнтів звертаються за кредитом у вівторок, а найменша активність припадає на вихідні дні. Здається, ця характеристика може бути менш інформативною для формування кіберпрофілю в контексті таких злочинів, як кібератаки або соціальна інженерія. Що стосується злочинів, пов'язаних із кредитним шахрайством, ця характеристика може бути корисною лише для оцінки завантаженості співробітників банку у питаннях обробки кредитних заявок. Іншими словами, ця інформація може стимулювати впровадження додаткових організаційних заходів для поліпшення уваги щодо прийняття правильних рішень щодо видання кредитів.

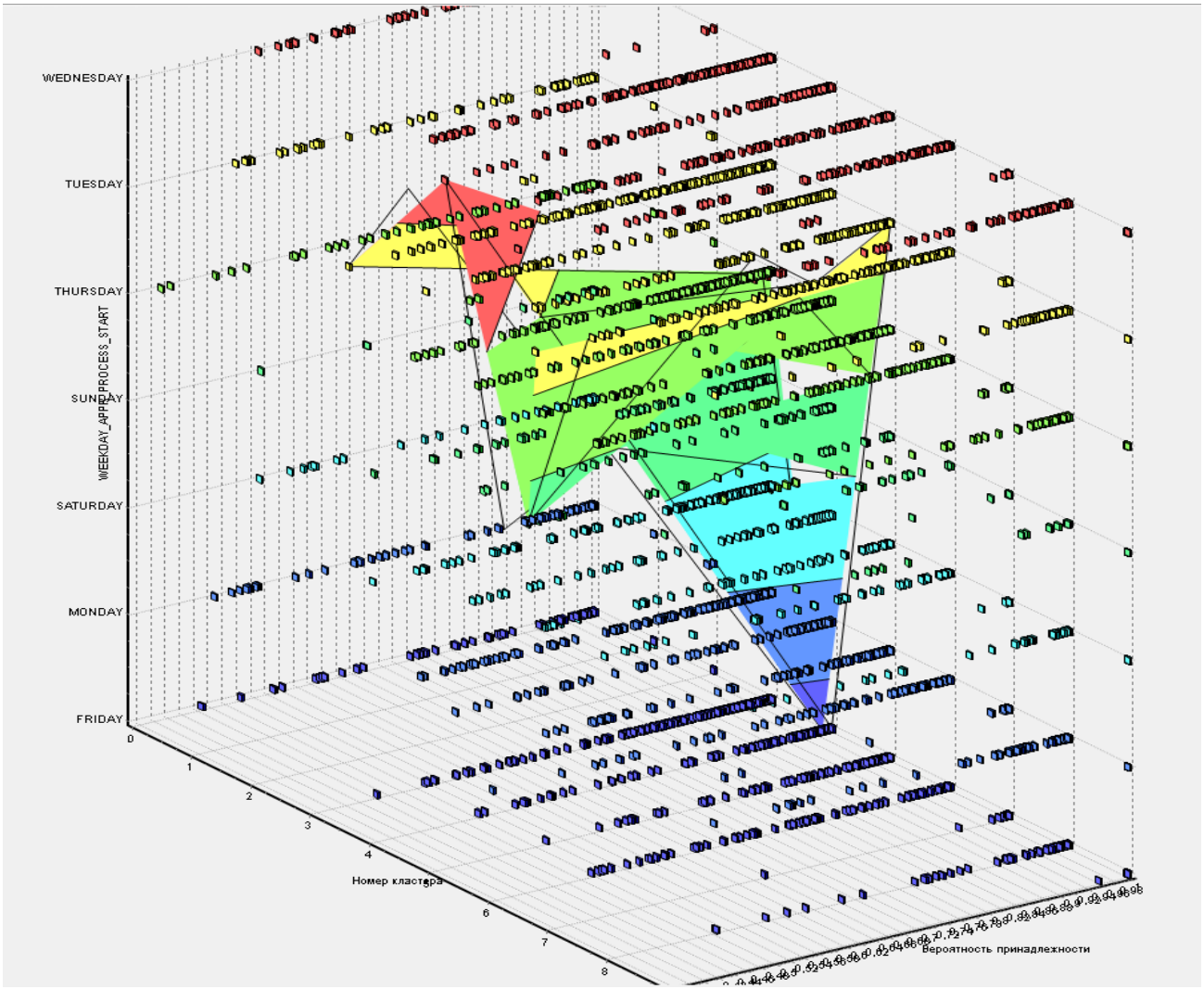


Рисунок 2.40 – Візуалізація характеристики “WEEKDAY_APPR_PROCESS_START”

Джерело: розроблено авторами на основі Яровенко (2022)

Для різних сценаріїв та типів злочинів можна адаптувати характеристики так, щоб вони відповідали конкретному випадку. Проте запропонований у даній роботі метод профілювання кіберзлочинів є також ефективним і для боротьби з кіберзлочинністю у громадян, підприємств та державних установ поряд із використанням програмного забезпечення, математичних та технічних інструментів. При розробці цих інструментів критично важливо враховувати різні характеристики, такі як поведінкові, географічні, психологічні та соціальні аспекти. Формування профілів на основі цих характеристик вимагає застосування різних методів, таких як криміналістичні, слідчі, клінічні та статистичні, для виявлення кіберзагроз з різних точок зору їх виникнення.

2.3 Формування стратегічних засад забезпечення стійкості фінансового кіберпростору

2.3.1 Стратегія ребілдингу архітектоніки системи держфінмоніторингу

Державна служба фінансового моніторингу України (Держфінмон) є центральним органом виконавчої влади, який відповідає за забезпечення реалізації політики державного фінансового моніторингу в Україні. Її діяльність регулюється законодавством України, зокрема Законом "Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення" та іншими нормативними актами.

Функції Держфінмон України включають наступне:

– Збір, обробка і аналіз інформації. Держфінмон збирає інформацію про фінансові та інші транзакції, які можуть бути пов'язані з легалізацією доходів, одержаних злочинним шляхом, фінансуванням тероризму та іншими злочинними діями. Ця інформація надходить від фінансових установ, юридичних осіб, інших суб'єктів та відповідних державних органів.

– Виявлення сумнівних операцій. Держфінмон аналізує отриману інформацію, виявляє сумнівні та потенційно злочинні фінансові операції та транзакції.

– Забезпечення відповідності. Відповідно до законодавства, Держфінмон встановлює вимоги до фінансових установ і суб'єктів щодо здійснення фінансового моніторингу та звітності. Він сприяє дотриманню визначених норм та стандартів у сфері фінансового моніторингу.

– Співпраця з іншими органами. Держфінмон співпрацює з іншими органами державної влади, правоохоронними органами та міжнародними організаціями для обміну інформацією та координації заходів з моніторингу та боротьби з фінансовими злочинами.

– Застосування заходів контролю та санкцій. Держфінмон має право вживати заходів контролю та санкцій відповідно до законодавства в разі виявлення порушень в сфері фінансового моніторингу.

– Освіта та навчання. Держфінмон проводить роботу з підвищення обізнаності та навчання фінансових установ, юридичних осіб та інших суб'єктів у сфері фінансового моніторингу та виявлення фінансових злочинів.

Держфінмон України грає важливу роль у забезпеченні фінансової безпеки та боротьбі з фінансовими злочинами в Україні, зокрема у запобіганні легалізації доходів, одержаних злочинним шляхом, та фінансуванні тероризму.

Можна виділити кілька загальних тенденцій та проблем, які можуть залишатися актуальними:

– Технічна інфраструктура та інновації. Вдосконалення технічної бази та використання сучасних технологій для ефективного аналізу великих обсягів фінансової інформації може залишатися однією з найбільш важливих проблем.

Для боротьби зі складними схемами відмивання грошей та фінансуванням тероризму потрібні ефективні інструменти аналізу та моніторингу.

– Підвищення професійної кваліфікації персоналу. Співпраця з міжнародними партнерами, аналіз нових методик та навчання персоналу є важливими для підвищення ефективності роботи Держфінмону.

– Співпраця з іншими країнами. У сучасному глобальному фінансовому середовищі важлива міжнародна співпраця у сфері обміну інформацією щодо фінансових транзакцій та виявлення сумнівних операцій.

– Оптимізація процедур і стандартів. Вдосконалення внутрішніх процедур та стандартів фінансового моніторингу для забезпечення високої якості виявлення та аналізу сумнівних операцій.

– Забезпечення незалежності. Гарантування незалежності Держфінмону від політичних впливів і забезпечення його безперешкодної роботи для ефективної боротьби з фінансовими злочинами.

Перебудова структури Держфінмону може бути необхідною для покращення ефективності та ефективної боротьби з фінансовими злочинами. Ось деякі аспекти, які можуть потребувати уваги при перебудові структури Держфінмону:

– Зміцнення технічної інфраструктури. Для ефективного фінансового моніторингу та аналізу великих обсягів фінансової інформації може бути необхідним покращення технічної бази та використання сучасних технологій. Це включає в себе оновлення апаратного та програмного забезпечення, розвиток біг-дата аналітики, застосування штучного інтелекту та інших інноваційних рішень.

– Навчання та розвиток персоналу. Перепідготовка та підвищення кваліфікації персоналу є ключовим аспектом. Персонал Держфінмону повинен бути добре підготовленим для виявлення сумнівних операцій та аналізу фінансової інформації. Навчання з актуальних методів та стратегій фінансового моніторингу є важливим.

– Законодавчі та регуляторні зміни. Перебудова може включати оновлення законодавства та регуляторних норм, щоб забезпечити відповідність міжнародним стандартам фінансового моніторингу та боротьби зі злочинністю. Це може включати в себе розширення повноважень Держфінмону та вдосконалення процедур.

– Співпраця та координація. Зміцнення співпраці з іншими державними органами, правоохоронними органами та міжнародними партнерами може бути важливою частиною перебудови. Важливо забезпечити ефективну координацію заходів для виявлення та боротьби з фінансовими злочинами.

– Збільшення незалежності. Забезпечення незалежності Держфінмону від політичних впливів є важливим аспектом. Державна служба фінансового моніторингу повинна мати можливість діяти об'єктивно та без впливу ззовні.

– Залучення громадськості та стейкхолдерів. Важливо враховувати думку громадськості та інших стейкхолдерів у процесі перебудови та

впровадження змін в Держфінмоні. Широка підтримка може сприяти успішному впровадженню реформ.

Перебудова структури Держфінмону повинна бути цілеспрямованою та спрямованою на зміцнення функцій фінансового моніторингу та підвищення ефективності боротьби з фінансовими злочинами.

Зміцнення технічної інфраструктури для системи Держфінмону є критично важливим для ефективної боротьби з фінансовими злочинами. Ось детальна характеристика можливих напрямків зміцнення технічної інфраструктури:

– Розвиток бази даних. Система Держфінмону повинна мати потужну та надійну базу даних, яка дозволить збирати, зберігати та оновлювати фінансову інформацію. Це включає в себе інтеграцію з різними джерелами даних, включаючи фінансові установи, регулятори, інші державні органи та міжнародні джерела.

– Біг-дейта аналітика. За допомогою технологій аналізу великих обсягів даних (біг-дейта), Держфінмон може ефективніше виявляти сумнівні та злочинні фінансові операції. Інструменти для обробки та аналізу біг-дейта допомагають виявляти шаблони та зв'язки між транзакціями.

– Штучний інтелект (AI) та машинне навчання. Використання AI і машинного навчання дозволяє автоматизувати процес виявлення сумнівних операцій. Системи можуть навчитися розпізнавати аномалії та сигнали, які можуть свідчити про фінансові злочини.

– Кіберзахист. Забезпечення високого рівня кіберзахисту є надзвичайно важливим для запобігання несанкціонованому доступу до фінансової інформації та захисту від кібератак. Це включає в себе захист від хакерських атак, витоків даних та інших кіберзагроз.

– Системи визначення осіб (AML) та визначення бенефіціарів (KYC). Системи AML та KYC дозволяють визначати та перевіряти клієнтів та їх фінансові транзакції для виявлення потенційно сумнівних операцій. Інтеграція та вдосконалення цих систем є важливою частиною технічної інфраструктури.

– Засоби обміну інформацією. Система повинна мати засоби обміну інформацією з іншими державними органами, правоохоронними органами та міжнародними партнерами для ефективного обміну даними та координації дій.

– Захист даних та конфіденційності. Забезпечення захисту фінансових даних та конфіденційності є важливою складовою технічної інфраструктури. Система повинна дотримуватися високих стандартів безпеки даних та забезпечувати конфіденційність інформації.

– Моніторинг та звітність. Розробка систем моніторингу та звітності допомагає вести контроль над фінансовими операціями та створювати звіти для внутрішнього та зовнішнього використання.

Зміцнення технічної інфраструктури сприяє покращенню якості фінансового моніторингу та боротьбі з фінансовими злочинами.

Навчання та розвиток персоналу є ключовими аспектами для удосконалення системи Держфінмону та її поєднання з системою кібербезпеки.

Ось детальна характеристика можливих напрямків навчання та розвитку персоналу:

– Навчання з фінансового моніторингу. Персонал Держфінмону повинен проходити навчання з основ фінансового моніторингу, включаючи виявлення сумнівних та злочинних фінансових операцій, використання інструментів AML (визначення осіб) та KYC (визначення бенефіціарів), аналіз банківських та фінансових транзакцій.

– Школи та тренінги. Організація шкіл та тренінгів є важливою частиною навчання персоналу. Це може включати в себе участь у міжнародних тренінгах та семінарах, де спеціалісти можуть вивчати найкращі практики з фінансового моніторингу та кібербезпеки.

– Розвиток навичок кібербезпеки. З огляду на поєднання Держфінмону з системою кібербезпеки, персонал повинен проходити навчання з кіберзахисту. Це включає в себе навчання з виявлення та захисту від кібератак, використання кіберзасобів та інших аспектів кібербезпеки.

– Машинне навчання та штучний інтелект. Вивчення машинного навчання та штучного інтелекту є важливим для розвитку аналітичних навичок персоналу. Інтеграція цих технологій у фінансовий моніторинг та кібербезпеку вимагає розуміння їхніх принципів та застосування.

– Знання законодавства. Персонал повинен бути добре ознайомлений із законодавством, яке регулює фінансовий моніторинг та кібербезпеку. Це включає в себе знання про міжнародні та внутрішні правила та стандарти.

– Міжнародна співпраця. Розуміння принципів та практики міжнародної співпраці у сферах фінансового моніторингу та кібербезпеки є важливим для персоналу. Вони повинні бути здатні співпрацювати з міжнародними партнерами та іншими країнами.

– Моніторинг та оцінка результатів. По закінченні навчання слід проводити моніторинг та оцінку результатів, щоб переконатися, що персонал володіє необхідними навичками та здатностями для виконання завдань з фінансового моніторингу та кібербезпеки.

Навчання та розвиток персоналу є невід'ємною частиною удосконалення системи Держфінмону та її поєднання з системою кібербезпеки. Воно допомагає персоналу адаптуватися до сучасних викликів та забезпечувати високу ефективність роботи.

Законодавчі та регуляторні зміни в системі Держфінмону, які поєднують функції фінансового моніторингу та кіберзахисту, можуть бути важливими для забезпечення ефективності та цілісності системи. Ось детальна характеристика можливих напрямків цих змін:

– Розширення повноважень Держфінмону. Законодавчі зміни можуть передбачати розширення повноважень Держфінмону для виявлення та запобігання кіберзлочинам, зокрема, фінансуванню кібертероризму та інших кіберзлочинів. Це включає в себе право проводити аналіз фінансових транзакцій, пов'язаних з кібератаками.

– Оновлення регуляторного середовища. Зміни можуть включати в себе оновлення регуляторних норм та стандартів для врахування кіберзахисту в контексті фінансового моніторингу. Важливо встановити вимоги щодо захисту фінансових інформаційних систем та обміну даними з іншими структурами.

– Обов'язкова звітність щодо кіберзахисту. Законодавство може встановити обов'язок для фінансових установ та інших суб'єктів сповіщати Держфінмон про інциденти в галузі кіберзахисту, які можуть впливати на фінансову стабільність.

– Заохочення співпраці. Законодавство може надавати стимули для співпраці між різними суб'єктами, включаючи фінансові установи, кіберзахисні компанії та правоохоронні органи. Зміни можуть сприяти обміну інформацією та спільним діям для запобігання кіберзлочинам.

– Захист особистих даних. Законодавчі зміни повинні враховувати правила та стандарти щодо захисту особистих даних у контексті кіберзахисту. Це важливо для забезпечення конфіденційності та приватності клієнтів.

– Відповідальність за недотримання правил. Законодавство може передбачати відповідальність для суб'єктів, які не дотримуються правил кіберзахисту та не повідомляють про інциденти. Це сприяє підвищенню відповідальності та стимулює дотримання норм.

– Забезпечення незалежності та недоторканості Держфінмону. Законодавчі зміни можуть встановлювати правовий статус та незалежність Держфінмону, щоб він міг виконувати свої функції об'єктивно та незалежно від політичних впливів.

– Міжнародна співпраця. Законодавство повинно надавати правові основи для міжнародної співпраці в галузі кіберзахисту та фінансового моніторингу, включаючи обмін інформацією з іншими країнами.

Законодавчі та регуляторні зміни, які поєднують функції фінансового моніторингу та кіберзахисту, можуть створити надійну та ефективну систему для виявлення та запобігання кіберзлочинам у фінансовому секторі.

Співпраця та координація між Держфінмоном та органами кібербезпеки є критично важливими для забезпечення ефективної боротьби з кіберзагрозами у фінансовому секторі. Ось детальна характеристика можливих напрямків співпраці та координації:

– Обмін інформацією. Держфінмон та органи кібербезпеки повинні встановити механізми для обміну інформацією про потенційні кіберзагрози та інциденти. Це дозволяє обом сторонам отримувати оперативну інформацію про можливі кіберзагрози та реагувати на них.

– Спільні вправи та симуляції. Органи кібербезпеки та Держфінмон можуть проводити спільні вправи та симуляції для перевірки готовності та реагування на кібератаки. Це допомагає покращити спільну координацію та сприяє ефективному вирішенню кризових ситуацій.

– Спільні команди реагування. Створення спільних команд реагування на кіберзагрози дозволяє об'єднати експертів з обох сторін для вивчення та вирішення кіберінцидентів.

– Визначення ролей та відповідальності. Для ефективної координації важливо визначити ролі та відповідальність кожної сторони в разі кібератаки. Це включає в себе розподіл завдань та визначення того, хто відповідає за певні аспекти реагування.

– Обмін аналітичною інформацією. Держфінмон та органи кібербезпеки повинні спільно аналізувати дані та інформацію щодо кіберзагроз для виявлення патернів та зв'язків між кібератаками та фінансовими операціями.

– Спільні рекомендації та заходи. На основі аналізу можна розробляти спільні рекомендації та заходи для зменшення ризику кіберзагроз та підвищення кібербезпеки в фінансовому секторі.

– Моніторинг та вдосконалення. Спільна моніторингова система дозволяє відслідковувати кіберзагрози та оцінювати ефективність заходів кіберзахисту. На основі цих даних можна внести вдосконалення у стратегії та тактики.

– Міжнародна співпраця. Співпраця з міжнародними організаціями та іншими країнами також є важливою складовою співпраці. Обмін інформацією та координація на міжнародному рівні допомагає виявляти та вирішувати кіберзагрози, які можуть мати глобальний вплив.

Співпраця та координація між Держфінмоном та органами кібербезпеки допомагає забезпечити ефективний захист фінансового сектору від кіберзагроз та підвищити рівень безпеки фінансових операцій.

Збільшення незалежності Держфінмону та системи кіберзахисту є важливим кроком для забезпечення ефективності та недоторканості їх функцій. Ось детальна характеристика можливих напрямків збільшення незалежності:

– Правовий статус. Забезпечення правового статусу Держфінмону та системи кіберзахисту як незалежних організацій, що не підпорядковуються іншим структурам, дозволяє їм виконувати свої функції без впливу зовнішніх структур або політичних інтересів.

– Фінансування. Забезпечення стабільного та незалежного фінансування Держфінмону та системи кіберзахисту допомагає уникнути втручання з боку сторонніх інтересів. Фінансування повинно бути достатнім для виконання завдань та забезпечення ефективності.

– Визначення процедур апеляції. Встановлення процедур для подання апеляцій щодо рішень та дій Держфінмону та системи кіберзахисту допомагає забезпечити об'єктивність та недоторканість прийнятих рішень.

– Захист від політичних тиску. Законодавчі заходи можуть передбачати захист від політичного тиску на роботу Держфінмону та системи кіберзахисту. Це може включати в себе встановлення чітких правил для звільнення керівників та співробітників у випадку недостойної поведінки.

– Кадровий резерв. Створення кадрового резерву з фахівців, які мають необхідні знання та навички в області фінансового моніторингу та кіберзахисту, допомагає забезпечити незалежність від зовнішніх впливів у випадку відставки чи звільнення керівництва.

– Моніторинг та звітність. Установлення системи моніторингу та звітності, яка допомагає відстежувати та доповідати про роботу Держфінмону та системи кіберзахисту, дозволяє стежити за їхньою діяльністю та виявляти будь-які спроби втручання.

– Публічна підтримка. Залучення громадськості та стейкхолдерів до питань фінансового моніторингу та кіберзахисту сприяє створенню широкої підтримки для незалежних організацій. Громадськість може відстоювати незалежність та вимагати відповідності високим стандартам.

– Міжнародна співпраця. Співпраця з міжнародними партнерами та організаціями також допомагає зберегти незалежність та відстоювати загальноприйняті стандарти та практики.

Збільшення незалежності Держфінмону та системи кіберзахисту допомагає забезпечити їхню ефективну діяльність та захист від зовнішніх впливів.

Залучення громадськості та стейкхолдерів в процесі перебудови Держфінмону та системи фінансового моніторингу є важливим для забезпечення прозорості, відповідності стандартам та отримання широкої підтримки громадськості. Ось детальна характеристика можливих напрямків залучення:

– Публічні консультації. Організування публічних консультацій, де громадськість, представники бізнесу, академічних груп та інші стейкхолдери можуть висловити свої погляди, запити та рекомендації щодо реформи фінансового моніторингу.

– Створення робочих груп. Формування робочих груп, в яких представники громадськості та стейкхолдери можуть спільно працювати з представниками Держфінмону для розробки нових стратегій та політик.

– Публікація звітів та інформації. Забезпечення публічного доступу до інформації про роботу Держфінмону та результати моніторингу допомагає громадськості розуміти та оцінювати діяльність органу.

– Участь у наглядових радах. Залучення представників громадськості та стейкхолдерів до наглядових рад і комітетів, які надають рекомендації та наглядають за діяльністю Держфінмону.

– Сприяння усвідомленню. Організація освітніх заходів та інформаційних кампаній для громадськості та бізнесу, щоб вони краще розуміли важливість фінансового моніторингу та його ролі у запобіганні фінансування тероризму та іншої злочинності.

– Моніторинг ініціатив. Залучення стейкхолдерів до моніторингу та оцінки ефективності реформ у фінансовому моніторингу для забезпечення відповідності стандартам та потребам громадськості.

– Залучення до розробки політик. Представники громадськості та стейкхолдери можуть бути запрошені до участі у розробці та обговоренні нових законодавчих актів та політик у сфері фінансового моніторингу.

– Створення механізмів зворотного зв'язку. Установлення механізмів для прийому звернень, запитів та скарг від громадськості та стейкхолдерів щодо діяльності Держфінмону.

Залучення громадськості та стейкхолдерів сприяє створенню більш прозорої, відкритої та відповідальної системи фінансового моніторингу, яка враховує різноманітні інтереси та потреби.

Поєднання функцій Держфінмону з функціями кібербезпеки може бути досягнуто через концепцію конвергенції, що передбачає інтеграцію та співпрацю між цими двома сферами. Ось кілька кроків для поєднання цих функцій:

– Створення інтегрованої команди. Сформуйте команду, яка об'єднає фахівців з обох напрямків - фінансового моніторингу та кібербезпеки. Ця команда повинна бути відповідальною за розробку та виконання стратегії конвергенції.

– Згуртування інформації. Об'єднайте інформацію та дані, що стосуються фінансового моніторингу та кібербезпеки. Важливо мати одну централізовану систему для збору, аналізу та спільного використання даних.

– Спільні процедури та протоколи. Розробіть спільні процедури та протоколи для виявлення та реагування на можливі кіберзагрози, які можуть впливати на фінансову сферу. Визначте ролі та відповідальність кожного члена команди.

– Обмін інформацією. Забезпечте систему обміну інформацією між фінансовим моніторингом і кібербезпекою. Це дозволяє вчасно реагувати на кіберзагрози, які можуть бути пов'язані з фінансовими операціями.

– Захист фінансових систем. Посиліть заходи кібербезпеки в фінансових системах, включаючи захист від кібератак, антивірусні програми та моніторинг безпеки мережі.

– Спільні навчальні програми. Організуйте навчальні програми та тренінги для персоналу, які охоплюють аспекти як фінансового моніторингу, так і кібербезпеки.

– Спільні проекти та дослідження. Проводьте спільні дослідження та проекти, щоб вдосконалювати практики та технології в галузі фінансового моніторингу та кібербезпеки.

– Забезпечення законодавчої підтримки. Розробіть та підтримуйте відповідну законодавчу базу, яка дозволяє обмін інформацією та спільну роботу між фінансовим моніторингом і кібербезпекою.

Поєднання функцій Держфінмону з функціями кібербезпеки допомагає створити більш інтегровану та ефективну систему для виявлення та запобігання кіберзагрозам у фінансовому секторі.

Зважаючи на складність та динамічність фінансових та кіберзагроз сучасного світу, необхідність перебудови системи Держфінмону України стає невідкладним завданням. Висока ступінь залежності сучасного суспільства від інформаційних технологій та фінансових послуг робить фінансовий сектор особливо вразливим перед різними формами кіберзагроз. З цього погляду, впровадження концепції конвергенції між Держфінмоном та кібербезпекою стає важливим механізмом для забезпечення інтегрованого та ефективного підходу до виявлення, аналізу та запобігання фінансовим злочинам, пов'язаним з кібератаками.

Закордонні практики та міжнародні стандарти визначають напрями для розвитку органів фінансового моніторингу, надаючи їм методології та інструменти для боротьби з фінансовою злочинністю. Залучення кращих практик з інших країн може значно покращити роботу Держфінмону та зробити його діяльність більш прозорою та ефективною.

Для досягнення успіху у цій перебудові, необхідно також зосередити увагу на розвитку технічної інфраструктури, підвищенні кваліфікації персоналу, залученні громадськості та стейкхолдерів, а також забезпечити належну законодавчу підтримку. Це дозволить створити сучасну та надійну систему фінансового моніторингу, здатну вчасно реагувати на змінюючіться умови та виклики в сфері кібербезпеки.

У підсумку, перебудова Держфінмону з урахуванням закордонних практик та його конвергенція з кібербезпекою є стратегічним кроком для забезпечення стабільності та безпеки фінансових систем України. Ця ініціатива допоможе зробити фінансовий сектор більш витривалим перед кіберзагрозами та забезпечить виконання міжнародних стандартів у сфері фінансового моніторингу та кібербезпеки.

2.3.2 Розробка соціо-економічних профілів країн-жертв кіберзлочинів

Наслідки Четвертої промислової революції призвели до активного впровадження комп’ютерних технологій в усі сфери життєдіяльності людини. Розробка Розумних заводів, потужних кіберфізичних систем, Інтернету речей та послуг сприяли та продовжують сприяти активному економічному та соціальному розвитку багатьох країн світу. З іншого боку, масова комп’ютеризація та цифровізація вплинули на появу кіберзлочинності, яка за останнє десятиліття набула великих масштабів в розрізі країн та світу. Масові кіберзлочини в наш час здійснюються не тільки заради отримання фінансових вигід для окремих осіб, але й задля ненасильницького впливу на конкретні групи людей, компанії, уряди, цілі держави. Ознаки масовості та впливу на життєво важливі об’єкти інфраструктури країни для порушення їх функціонування або виведення з активного стану можуть ідентифікувати кібератаки як кібервійна. Хоча Smith (2013) і заперечує подібне ототожнення. Але Lucas (2016) вважає здійснення масових кібератак однією з головних ознак кібервійн. Не дивлячись на розбіжності у поглядах на ідентифікацію даного явища достовірним фактом є те, що найбільш потужні у світовому кіберпросторі країни світу, такі як США, Китай, Великобританія, Росія, Нідерланди, Франція, Німеччина, Канада, Японія та Австралія, застосовують його інструменти для виконання інколи зовсім немирних цілей (Voo et al., 2022).

Так, у 2016 році Росія втрутилася у проведення президентських виборів в США, що було підтверджено Департаментом внутрішньої безпеки та Офісом директора національної розвідки США (U.S. Department of Homeland Security, 2016). У 2017 році була здійснена масштабна кібератака із використанням шкідливих програм-вимагачів Petya (NotPetya) та WannaCry, які були націлені на різні компанії України, але потім вірус поширився на інші країни світу, в

результаті чого постраждали великі компанії, такі як американська фармацевтична корпорація Merck, датська судноплавна компанія Maersk, Національна служба охорони здоров'я Великобританії, німецька логістична компанія DHL, австралійська шоколадна фабрика Cadbury та багато інших (Perlroth, 2017). У 2019 році Об'єднані Арабські Емірати здійснили серію кібератак на своїх політичних опонентів, які приймали участь у проєкті, присвяченому організації заходів для стеження за бойовиками та терористами (Bing & Schectman, 2019). У 2020 році Індія здійснила серію масштабних кібератак у бік державних служб Пакистану, про що заявила газета Tribune (2020). Через вразливості у програмному забезпеченні Microsoft китайський підрозділ кібершпигунів зламав 30,000 американських організацій, що значно вплинуло на їх роботу (Krebs, 2021). У 2022 році Україна стала об'єктом військової агресії з боку Росії. Цьому передувала масова серія DoS-атак та атак програм-вимагачів, які були вчинені на український уряд 13-14 січня 2022 року (Deutsche Welle, 2022). Можна навести багато інших прикладів кіберзлочинів, але, не дивлячись на різницю в їх цілях та засобах досягнення, їх вплив на події та процеси в різних країнах є вагомий.

Чому одні країни стають частіше жертвами кіберзлочинів, а інші не представляють жодного інтересу для масових кібератак, шпигунства, тероризму чи інших форм кібервійни? Які фактори сприяють зниженню зацікавленості кіберзлочинців та підвищують захисні резерви для протидії даного явища? Дане дослідження спрямоване на отримання відповідей на ці питання. З цією метою сформуємо декілька гіпотез, для доведення або відхилення яких будуть проведені аналітичні розрахунки, які дозволять сформувати профайли країн-жертв кіберзлочинів на базі найважливіших показників соціально-економічного розвитку. Першою гіпотезою є те, що країни, які є найпотужнішими країнами світу та які є ініціаторами кіберзлочинів також виступають жертвами більше, ніж ті, які мають слабкий вплив на світовій арені. Іншою гіпотезою є те, що рівень соціально-економічного розвитку країн може бути опосередкованою мотивацією кіберзлочинців для масових кібератак. Доведення запропонованих тверджень потребують застосування різних аналітичних методів. Для вирішення першого питання доцільно утворити групи країн в залежності від впливу різної кількості спрямованих на них кібератак. Формування висновків за другою гіпотезою можливі тільки за умови утворення профайлів на основі ключових індикаторів, які характеризують соціально-економічний розвиток країн.

Для проведення дослідження було обрано два набори даних. Один із них використовувався для формування кластерів країн в залежності від рівня виявлених кіберзлочинів, спрямованих на них. Джерелом даних є ресурс Лабораторії Касперського (Kaspersky, 2023). Другий набір даних було сформовано із індикаторів, які характеризують соціально-економічний рівень розвитку країн з урахуванням їх впливу на макро- та глобальні процеси. Це дозволило провести аналіз потенційної привабливості для кібершахраїв та виявити ті напрямки, які потребують уваги з боку міжнародних організації та уряду для протидії кіберзлочинності.

Перший набір даних було сформовано для 93 країн світу, який представляє собою обсяги трьох видів кіберзлочинів за місяць за період з 21.04.23 по 20.05.23. До першого виду було обрано кількість шкідливих програм та вірусів, знайдених із використанням антивірусів “Mail Anti-Virus” (MAV). Другим видом кіберзлочину було обрано мережеві кібератаки, які були виявлені системою “Intrusion Detection Scan” (IDS). Вразливості у програмному забезпеченні, комп’ютерах та мережах за часту сприяють кіберзлочинцям проводити більш активні кібератаки та порушувати безпеку різних видів користувачів. Такі загрози виникають завдяки недосконалому програмуванню та неправильній конфігурації маршрутизаторів, серверів додатків, веб-серверів, брандмауерів та інших технічних та програмних засобів. Для їх аналізу було обрано кількість вразливостей у інформаційних системах (“Vulnerability” – VUL), які виявляються за допомогою програм-сканерів.

Для виявлення характеристик, за якими можна ідентифікувати привабливість країни для кіберзлочинців, було обрано ряд індикаторів соціально-економічного розвитку за 2022 рік для 93 країн світу. В першу чергу було обрано National Cyber Security Index (NCSI), який дозволяє оцінити рівень країни протидіяти кіберзагрозам (E-Governance Academy, 2023). Високий ступінь національної кібербезпеки дозволяє формувати потужну базу захисту на основі правового, інформаційного, технічного, програмного, організаційного та інших видів забезпечення системи безпеки. Це повинно сприяти зниженню привабливості країни для масових кібератак. Оскільки кіберзлочини в наш час використовуються для розповсюдження кібертероризму, то вибір індикатора Global Terrorism Index (GTI) дозволить виявити вплив країни на рівень глобального тероризму в цілому (Institute for Economics and Peace, 2022). Тобто країни із найвищим рівнем тероризму можуть бути найбільшими жертвами масових хакерських атак або їх ініціаторами, тоді як країни з найнижчим впливом навпаки не стануть їх ціллю. Важливим для формування профайлу щодо потенційної привабливості для кіберзлочинців є розуміння обставин щодо стану злочинності всередині країни, що вимірює Crime Index, CI (Numbeo, 2023). Він дозволяє оцінити внутрішню ситуацію формування умов сприятливих для розвитку та підтримки різного роду злочинів для конкретної країни. Оскільки сьогодні зростає популярність Darknet і більшість кримінальних дій відбувається із використанням комп’ютерних технологій, то аналіз даного індикатора дозволить оцінити як внутрішнє середовище сприяє формуванню умов для підтримки кіберзлочинності, що може перетворювати країну не тільки на її жертву, але й на активного кібертерориста. На імідж країни в кіберпросторі може впливати й рівень корупції, яка формує відповідну площину для легалізації коштів, незаконного перерозподілу грошових потоків, здійснення порушень у законодавстві, тощо. Для аналізу даної характеристики було обрано Corruption Perceptions Index (CPI) (Transparency International, 2023).

На формування соціально-економічного профілю країни впливає рівень його економічної свободи, який дозволяє вимірювати взаємовідносини між різними сферами економіки: державними фінансами, бізнесом, податками,

інвестиційною та податковою сферами, торгівлею, чесністю уряду та ефективністю судової системи, тощо. Як правило, економічна складова є драйвером розвитку науково-технічного прогресу, що впливає на створення відповідного кіберсередовища окремої країни. Тому для аналізу у даній площині було вибрано Index of Economic Freedom, IEF (The Heritage Foundation, 2023). Окрім економічного благополуччя важливими є задоволеність населення від якості сфери здоров'я, освіти, мистецтва, культури, навколишнього середовища, можливостей забезпечення працею та психологічної підтримки. Оцінювання цих аспектів можливе за допомогою Happiness Index, HI (World Happiness Report, 2023). Найбільш щасливі країни у порівнянні із менш щасливими можуть приваблювати кіберзлочинців саме для отримання фінансових вигід від такого роду злочинів. Life Expectancy at Birth (LE) є індикатором, який характеризує рівень соціально-економічного розвитку країн. Найвищі його значення відповідають економічно розвиненим країнам, найнижчі – тим, що є найменш розвиненими (The World Bank, 2023). Останньою обраною характеристикою є рівень демократії, який дозволяє оцінити рівень громадянських та політичних свобод, що викликають повагу з боку уряду країни. Для цього використовується Democracy Index (DI) (Economist Intelligence, 2023). Наявність або відсутність таких прав та свобод серйозно впливає на формування несприятливого середовища для стійкого соціально-економічного розвитку країни, що також може викликати певну зацікавленість для кіберзлочинців. Перелічені індикатори було обрано для 93 країн світу за 2022 рік.

Таким чином, сформовано два набори даних для проведення аналізу профілів груп країн, які виступають жертвами внаслідок здійснення кібератак через поштові сервіси, мережі та вразливості інформаційних систем.

Методологія дослідження соціально-економічних профайлів країн, які є жертвами кіберзлочинів здійснювалася в три етапи. Реалізація першого пов'язана із проведенням попередньої обробки даних, визначенням наявності чи відсутності мультиколінеарності між трьома видами кіберзлочинів та у проведенні стандартизації значень спостережень. Другий етап пов'язаний із кластеризацією країн, яка проводиться, виходячи з кількісного значення тих видів кіберзлочинів, які не є мультиколінеарними. Також тут передбачена перевірка узгодженості кластерів за допомогою Silhouette методу. Третій етап необхідний для виявлення соціально-економічних закономірностей, властивих для визначених груп країн, який реалізується за допомогою асоціативного аналізу.

Перший етап дослідження полягав у здійсненні попередньої обробки вхідних даних. Оскільки вони збиралися вручну, то необхідність у обробці пропущених значень була відсутньою. Також дані не потребували дослідження на аномальність, оскільки у нашому випадку наявність таких спостережень свідчить про надмірність кібератак у бік даної країни.

Для реалізації кластерного аналізу обов'язково провести перевірку на мультиколінеарність та здійснити стандартизацію даних. Стандартизація дозволяє прибрати середнє значення та збільшити масштаб до значення

дисперсії. Дану процедуру було проведено за формулою (2.24) (Yarovenko et al., 2023):

$$x_{ij}^{scaled} = \frac{x_{ij} - \overline{x_j}}{\sigma_j}, \tag{2.24}$$

де x_{ij}^{scaled} – стандартизоване значення j–th виду кіберзлочину в розрізі i–th країни;

x_{ij} – фактичне значення j–th виду кіберзлочину в розрізі i–ї країни;

$\overline{x_j}$ – середнє значення вибірки для j–th виду кіберзлочину;

σ_j – стандартне відхилення вибірки для j–th виду кіберзлочину (Yarovenko et al., 2023).

Для перевірки даних на мультиколінеарність застосовувався алгоритм Farrar–Glauber, який передбачає розрахунок Chi-squared за формулою (2.25) (Yarovenko et al., 2023):

$$\mathrm{X}^2 = -\left((n-1) - \frac{2m+5}{6}\right) \times ln|R|, \tag{2.25}$$

де X^2 – розраховане значення Chi-squared;

n – кількість спостережень в масиві змінних, яке дорівнює 93 країні;

m – кількість пояснювальних змінних, яке дорівнює 3 видам кіберзлочинів;

$|R|$ – визначник матриці, яка формується з попарних коефіцієнтів кореляції, тобто (Yarovenko et al., 2023):

$$R = \begin{pmatrix} 1 & r_{12} & r_{13} \\ r_{21} & 1 & r_{23} \\ r_{31} & r_{32} & 1 \end{pmatrix}, \tag{2.26}$$

де r_{kj} – значення коефіцієнтів кореляції між парами пояснювальних змінних, які відповідають досліджуваним видам кіберзлочинів ($k = 1 \div 3$; $j = 1 \div 3$), яке розраховується за формулою (2.27) (Yarovenko et al., 2023):

$$r_{kj} = \frac{\sum_{i=1}^{n}\left(\left(x_i^k - \overline{x^k}\right)\left(x_i^j - \overline{x^j}\right)\right)}{\sqrt{\sum_{i=1}^{n}\left(x_i^k - \overline{x^k}\right)^2 \sum_{i=1}^{n}\left(x_i^j - \overline{x^j}\right)^2}}. \tag{2.27}$$

Розраховане значення Chi-squared порівнюється із критичним при $\frac{1}{2}m(m-1)$ – ступенів вільності та відповідному рівню значущості α. Якщо $\mathrm{X}^2 > \mathrm{X}_{cr}^2$, то в масиві змінних існує мультиколінеарність і перевірку потрібно продовжити далі, в іншому випадку мультиколінеарність відсутня і перевірка не проводиться.

Для подальшого дослідження обчислюється критерій Фішера за формулою (2.28), який дозволяє визначити корельованість окремого фактору з іншими (Yarovenko et al., 2023):

$$F_k = (a_{kk} - 1) \times \frac{(n-m)}{(m-1)}, \quad (2.28)$$

де F_k –значення критерія Фішера, розраховане окремо для кожної з трьох змінних;

a_{kk} – діагональний елемент матриці, оберненої до матриці R.

Розраховане значення критерія Фішера порівнюється із критичним $F_{cr}(\alpha, k_1, k_2)$, де α – відповідний рівень значущості, $k_1 = n - m$ та $k_2 = m - 1$. Якщо $F_k > F_{cr}$, то відповідна змінна корелює з іншими. В протилежному, вона не корелює з іншими (Yarovenko et al., 2023).

Далі розраховуються частинні коефіцієнти кореляції за формулою (2.29), які показують тісноту зв'язку між двома змінними без врахування впливу інших змінних (Yarovenko et al., 2023):

$$r_{kj}^* = \frac{-a_{kj}}{\sqrt{a_{kk} a_{jj}}}, \quad (2.29)$$

де r_{kj}^* – значення частинних коефіцієнтів кореляції між парами пояснювальних змінних, які відповідають досліджуваним видам кіберзлочинів ($k = 1 \div 3$; $j = 1 \div 3$);

a_{kj}, a_{jj} – відповідні елементи матриці, оберненої до матриці R (Yarovenko et al., 2023).

Якщо розраховані значення наближаються до 1 або -1, то це свідчитеме про наявність тісного кореляційного зв'язку між змінними. Для отримання уточненого висновку можна скористатися критичними значеннями $r_{cr}(\alpha, v)$, отриманими з таблиці Fisher–Yates, де α – відповідний рівень значущості, $v = n - l - 2$, де l – число виключених величин у випадку частинної кореляції, n – кількість спостережень.

На останньому кроці розраховується критерій Стьюдента за формулою (2.30) для перевірки статистичної значущості частинних коефіцієнтів кореляції (Yarovenko et al., 2023):

$$t_{kj} = \frac{r_{kj}^* \sqrt{n-m}}{\sqrt{1 - {r_{kj}^*}^2}}. \quad (2.30)$$

Отримані значення критерія Стьюдента порівнюють із його критичним значенням $t_{cr}(\alpha, k)$, де α – відповідний рівень значущості, $k = n - m$. Якщо

$|t_{kj}| > t_{cr}$, то кореляційна залежність між змінними є статистично значущою, в іншому випадку залежність не є статистично значущою (Yarovenko et al., 2023).

На другому етапі дослідження було здійснено кластерний аналіз за допомогою методу k-means та перевірку узгодженості кластерів за допомогою Silhouette техніки. K-means clustering є одним з методів Data Mining, який дозволяє проводити розбиття набору даних на певну кількість груп (кластерів), за умови, що кожне спостереження є близьким до відповідного кластерного центроїду (середнього значення). Тобто ціллю кластерного аналізу є мінімізація дисперсії всередині кластеру та знаходження оптимальної відстані спостереження до середини групи, що можна представити у вигляді формули (2.31) (Yarovenko et al., 2023):

$$\arg\min_{C} \sum_{i=1}^{k} \sum_{x_p \in C_i} \left|\left|x_p - \mu_i\right|\right|^2 = \arg\min_{C} \sum_{i=1}^{k} |C_i|\, VarC_i, \tag{2.31}$$

де $(x_1, x_2, \dots, x_p)$ – набір змінних, кожен з яких представляє собою d – мірний вектор з n – спостережень в кожному;

μ_i – центроїд i-th кластеру, який визначається за формулою (2.32) (Yarovenko et al., 2023):

$$\mu_i = \frac{1}{|C_i|} \sum_{p \in C_i} x_p, \tag{2.32}$$

де $C = \{C_1, C_2, \dots, C_k\}$ – набори змінних, які відповідають i-th кластеру при $i = 1 \div k$. При цьому належність спостережень i-th кластеру зазначається як формула (2.33) (Yarovenko et al., 2023):

$$\mathrm{C}_i = \{p | if\ x_p\ belongs\ to\ the\ i^{th}\ cluster\}. \tag{2.33}$$

Silhouette є методом перевірки узгодженості даних у кластерах за допомогою візуалізації, який було запропоновано Rousseeuw (1987). Дана техніка передбачає визначення коефіцієнту silhouette для всіх зразків з урахуванням середньої відстані всередені кластеру та середньої відстані до найближчого кластера за формулою (2.34) (Yarovenko et al., 2023):

$$\begin{cases} s(i) = \dfrac{b(i) - a(i)}{max\{a(i), b(i)\}}, if\ |C_I| > 1, \\ s(i) = 0, if\ |C_I| = 1 \end{cases} \tag{2.34}$$

де $s(i)$ – значення силуету для і-го спостереження з набору даних;

$a(i)$ – середня відстань між i-th та іншими спостереженнями у кластері, яка розраховується за формулою (2.35);

$b(i)$ – середня відстань від i-th спостереженням у кластері до інших спостережень інших кластерів, яка розраховується за формулою (2.36);

$|C_I|$– множина спостережень одного кластера (Yarovenko et al., 2023):

$$a(i) = \frac{1}{|C_I| - 1} \sum_{j \in C_I, i \neq j} d(i,j), \tag{2.35}$$

$$b(i) = \min_{J \neq I} \frac{1}{|C_J|} \sum_{j \in C_J} d(i,j), \tag{2.36}$$

де $d(i,j)$ – відстань від i-th спостереження до j-th (Yarovenko et al., 2023).

Для ідентифікації результатів необхідно, щоб $-1 \leq s(i) \leq 1$. Якщо значення silhouette наближатиметься до 1, то це свідчитиме про групування даних належним чином. Якщо його значення буде близьким до 0, то дані знаходяться на межі двох кластерів і їх важко віднести до певного кластеру. Якщо silhouette наближатиметься до -1, до дані належать іншому кластеру.

Третій етап дослідження потребує попередньої обробки даних, які відповідають соціально-економічним факторам. Спочатку їх потрібно нормалізувати за формулою (2.37), якщо показник є стимулятором, та формулою (2.38), якщо показник є дестимулятором (Yarovenko et al., 2023):

$$x'_{ij} = \frac{x_{ij} - x_j^{min}}{x_j^{max} - x_j^{min}}, \tag{2.37}$$

$$x'_{ij} = \frac{x_j^{max} - x_j}{x_j^{max} - x_j^{min}}, \tag{2.38}$$

де x'_{ij} – нормалізоване значення i-th спостереження для j-th змінної;

x_j^{min} та x_j^{max} – відповідно, мінімальне та максимальне значення для j-th змінної (Yarovenko et al., 2023).

Для реалізації асоціативного аналізу є потреба у заміні даних на рейтингові групи. Це пов’язані із невеликою кількістю спостережень та великою варіацією їх значень. Для цього скористуємося формулою (2.39) (Yarovenko et al., 2023):

$$x_{ij}^* = \begin{cases} x_{ij} = 1, if\ 0 < x_{ij} \leq 0.25 \\ x_{ij} = 2, if\ 0.25 < x_{ij} \leq 0.50 \\ x_{ij} = 3, if\ 0.5 < x_{ij} \leq 0.75 \\ x_{ij} = 4, if\ 0.75 < x_{ij} \leq 1 \end{cases}, \tag{2.39}$$

де x_{ij}^{*} – рейтингове значення i-th спостереження для j-th змінної;

1 – рейтингове значення, яке відповідає низькому значенню показника, що входить в перші 25%;

2 – рейтингове значення, яке відповідає нижче середньому значенню показника, що входить до другого квартилю значень вибірки;

3 – рейтингове значення, яке відповідає вище середньому значенню показника, що входить до третього квартилю значень вибірки;

4 – рейтингове значення, яке відповідає високому значенню показника, що входить до четвертого квартилю значень вибірки (Yarovenko et al., 2023).

Даний етап дослідження полягає у проведенні асоціативного аналізу, який дозволить виявити правила причин з'єднання аналізованих індикаторів для певного кластеру країн. Це сприятиме формуванню профайлу країн-жертв кіберзлочинів на основі факторів їх соціально-економічного розвитку, що допоможе розуміти мотивацію злочинців щодо здійснення цілеспрямованих кібератак. Для реалізації даного виду аналізу використовується алгоритм Apriori, який базується на виявленні частотних множин даних в наборі, що дозволить сформувати перелік типових факторів для кластерів країн. Також його побудова на асоціації та кореляції сприятиме виявленню причинно-наслідкових зв'язків в рамках окремої групи країн. Для виявлення асоціативних правил визначаються наступні показники за формулою (2.40) (Yarovenko et al., 2023):

$$supp(X \Longrightarrow Y) = \frac{F(X,Y)}{N},$$

$$conf(X \Longrightarrow Y) = \frac{F(X,Y)}{F(X)}, \qquad (2.40)$$

$$lift(X \Longrightarrow Y) = \frac{S(X \Rightarrow Y)}{S(X) \times S(Y)},$$

де $supp\ (support)$ – показник, який характеризує частоту появи набору елементів X та Y;

$conf\ (confidence)$ – показник, який дозволяє визначити відсоток елементів, які задовольняють умові елементу X, які також задовольняють й умові елементу Y;

$lift$ – показник, який демонструє рівень зацікавленості в елементі Y за умови існування зацікавленості в елементі X;

якщо $lift(X \Rightarrow Y) = 1$ – кореляція в наборі даних відсутня; якщо $lift(X \Rightarrow Y) > 1$ – кореляція позитивна, тобто ймовірність сумісної реалізації елементів X та Y є дуже високою;

якщо $lift(X \Rightarrow Y) < 1$ – кореляція від'ємна, тобто сумісна реалізація елементів X та Y є мало ймовірною (Yarovenko et al., 2023).

Оскільки розрахунки асоціативного аналізу відбувалися у аналітичному пакеті STATISTICA, то позначення показника $lift$ відбувалося як $correlation$.

Розрахунки першого етапу методології щодо стандартизації даних та перевірки їх на наявність мультиколінеарності за допомогою тесту Фарара-Глобера відбувалися із використанням програмного забезпечення MS Excel. Результати тесту представлені в таблиці 2.12, де можна побачити, що в масиві даних, сформованому на основі трьох видів кіберзлочинів, присутня мультиколінеарність, оскільки $X^2 > X^2_{cr}$. Подальша перевірка із використанням критерії Фішера, часткової кореляції та Стьюдента виявила, що змінна, яка відповідає кількості шкідливих програм та вірусів, розповсюджених через поштові сервіси, не є мультиколінеарною з іншими. Щодо фактору кількості мережевих атак, то у поєднанні із попередньою змінною він не є мультиколінеарним ($r_{MAV,IDS} < r_{cr}, \quad t_{MAV,IDS} < t_{cr}$). Третя змінна, яка характеризує кількість виявлених атак на вразливості системи, є колінеарною з іншими ($r_{IDS,VUL} > r_{cr}, \quad t_{IDS,VUL} > t_{cr}, \quad r_{MAV,VUL} > r_{cr}, \quad t_{MAV,VUL} > t_{cr}$). Для усунення мультиколінеарності з масиву змінних найкращим способом є метод головних компонент, але у нашому випадку його застосування не призвело до отримання набору даних, який б задовольняв всім умовам. Тому для проведення кластеризації було прийнято рішення усунути змінну VUL та здійснити кластеризацію з урахуванням тільки двох змінних.

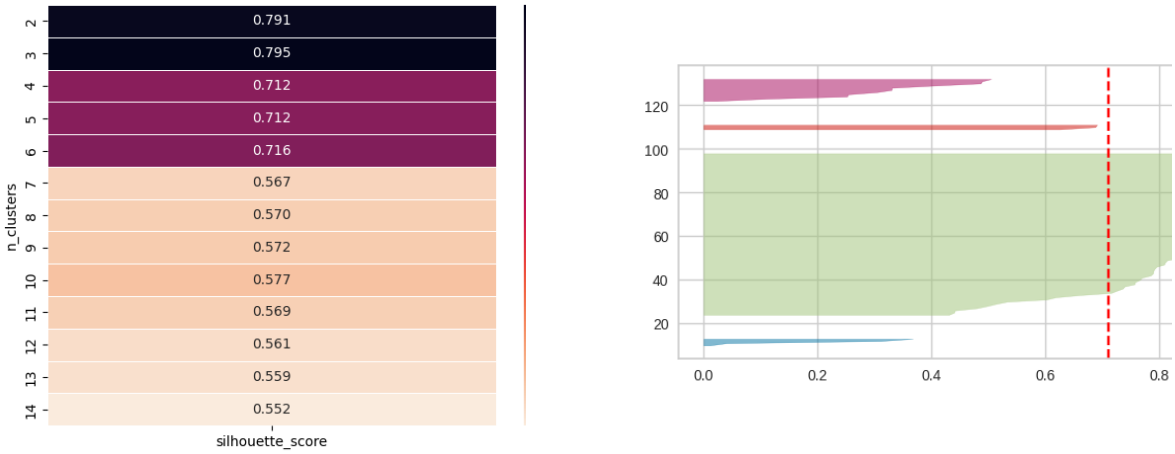
Таблиця 2.12 – Результати тесту Фаррара–Глобера

Розрахунковий критерій	Розрахункове значення	Знак нерівності	Критичний критерій	Критичне значення	Результати перевірки
X^2	81.6434	>	X^2_{cr}	7.8147	Присутня мультиколінеарність
F_{MAV}	16.8229	<	F_{cr}	19.4846	Немультиколінеарний
F_{IDS}	39.5230	>			Мультиколінеарний
F_{VUL}	42.7960	>			Мультиколінеарний
$r_{MAV,IDS}$	0.2040	<	r_{cr}	0.2050	Немультиколінеарний
$r_{MAV,VUL}$	0.2781	>			Мультиколінеарний
$r_{IDS,VUL}$	0.5702	>			Мультиколінеарний
$t_{MAV,IDS}$	1.9767	<	t_{cr}	1.9867	Статистично значущий
$t_{MAV,VUL}$	2.7466	>			Статистично незначущий
$t_{IDS,VUL}$	6.5848	>			Статистично незначущий

Джерело: розроблено авторами на основі Yarovenko et al. (2023)

Проведення кластерного аналізу та здійснення перевірки узгодженості кластерів за допомогою Silhouette методу проводилося із використанням мови програмування Python. Оскільки кластеризація дозволила отримати нерівномірні розміри кластерів, то виникла необхідність у проведенні даної процедури в

декілька етапів за прикладом ієрархічної кластеризації. Результати першого етапу представлені на рисунку 2.41.

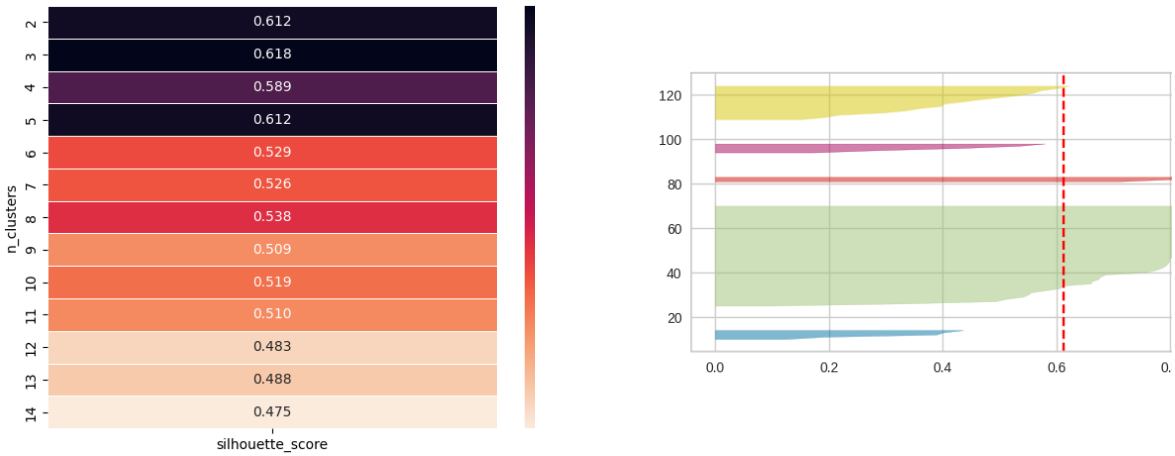


a) b)

Рисунок 2.41 – Результати першого етапу кластеризації: a) Silhouette score; b) Silhouette plot

Джерело: розроблено авторами на основі Yarovenko et al. (2023)

Найвищі Silhouette score відповідають ситуації розбиття даних на 3 кластери (Рисунок 2.41a). Але за цієї умови було також отримано й частку неправильної класифікації, тобто деякі країни (Німеччина), віднесені до кластеру, насправді до нього не належать. Для зменшення частки неправильної класифікації було прийнято рішення здійснити кластерний аналіз для 4 груп. Рисунок 2.41b підтверджує правильність такого розбиття. Але також можна побачити, що аналіз виділив кластер, який містить 80.65% усіх даних. Це обумовлено нерівномірним розподілом початкових даних, що викликано, нерівномірністю здійснення кібератак на країни. При цьому ті, які були атаковані найбільше, не потрапили до даного кластеру. Тому було проведено наступний етап кластеризації для тих країн, що увійшли до найбільшого кластеру. Результати другого етапу представлені на рисунку 2.42.



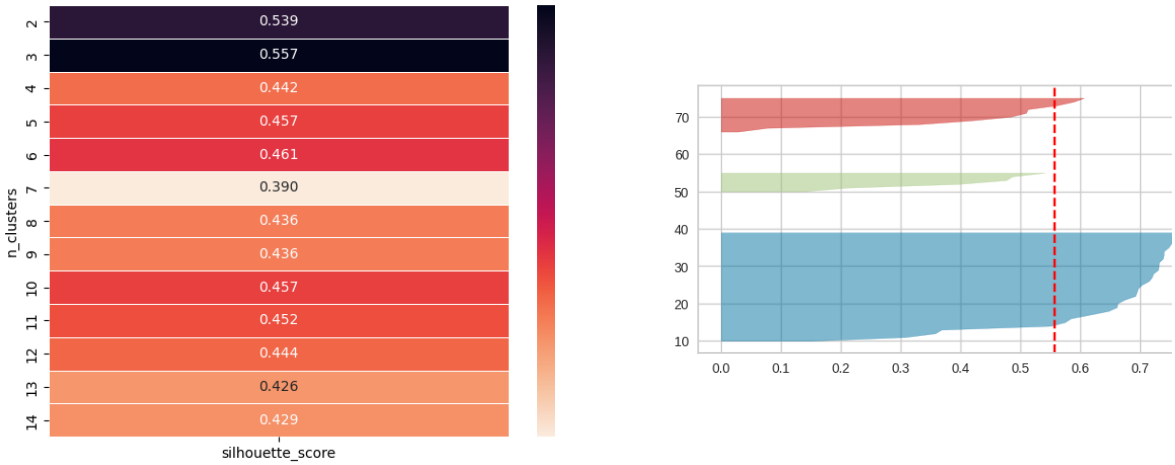
a) b)

Рисунок 2.42 – Результати другого етапу кластеризації: a) Silhouette score; b) Silhouette plot

Джерело: розроблено авторами на основі Yarovenko et al. (2023)

Хоча найвищі Silhouette score відповідають трикластерному розбиттю даних, але для даної ситуації також було отримано й частку неправильної класифікації. Дана процедура віднесла Сербію до іншого кластеру, про що свідчить від'ємне значення Silhouette score (-0.1090). Використання п'ятьох кластерів дозволяє уникнути неправильно класифікованих об'єктів, що підтверджує Рисунок 2.42b, що говорить про доцільність застосування саме цього виду розподілу. Не дивлячись на кількість кластерів, отримано висновок, що один з них містить 61.33% даних вибірки. Тобто існує потреба у подальшому розбитті вибірки, отриманої на другому етапі.

Результати третього кроку кластеризації для країн, які увійшли до найбільшого кластеру, представлені на рисунку 2.43. Отримані Silhouette score є значними для трикластерного розподілу (Рисунок 2.43a). При цьому всі країни були класифіковано правильно (Рисунок 2.43b). Але й на даному кроці також було сформовано кластер, який містить 65.22% всіх спостережень вибірки, узятої для даного етапу, що свідчить про продовження процедури кластеризації даних для найбільшої групи країн.

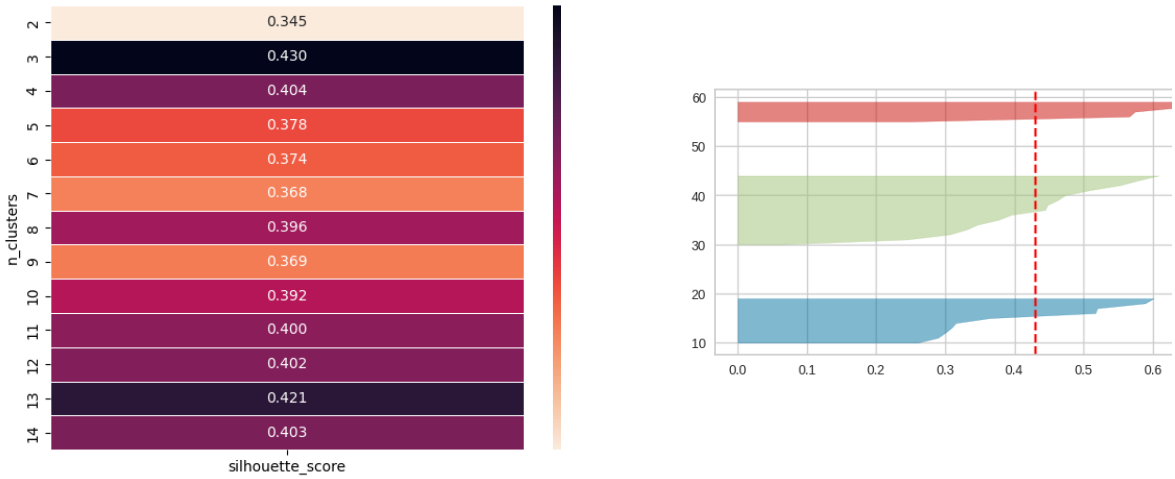


a) b)

Рисунок 2.43 – Результати третього етапу кластеризації: a) Silhouette score; b) Silhouette plot

Джерело: розроблено авторами на основі Yarovenko et al. (2023)

Результати четвертого останнього етапу кластеризації представлено на рисунку 2.44. Найвище значення Silhouette score відповідає трикластерному розподілу (Рисунок 2.44a). Візуалізація Silhouette підтверджує правильність отриманих результатів із відсутністю частки неправильної класифікації об'єктів (Рисунок 2.44b). Хоча тут присутній один кластер, який складається з 50% вибірки, але це значення відповідає 16% генеральної сукупності, що є прийнятним для аналізу даних. Недоцільність подальшої кластеризації також підтверджує зниження Silhouette score, що відбувається від етапу до етапу.



a) b)

Рисунок 2.44 – Результати четвертого етапу кластеризації: a) Silhouette score; b) Silhouette plot

Джерело: розроблено авторами на основі Yarovenko et al. (2023)

На рисунку 2.45 представлена карта країн, розподілених за визначеними кластерами, а в Таблиці 2.13 наведені усереднені за кластером значення по кожній групі кіберзлочинів. Тут також враховано й той вид, який було усунуто із процесу кластеризації. Найбільш атакованими є країни кластерів 1.3, 1.2 та 1.1. Найменш атакованими є країни, які належать до груп 4.1, 4.2 та 4.3.

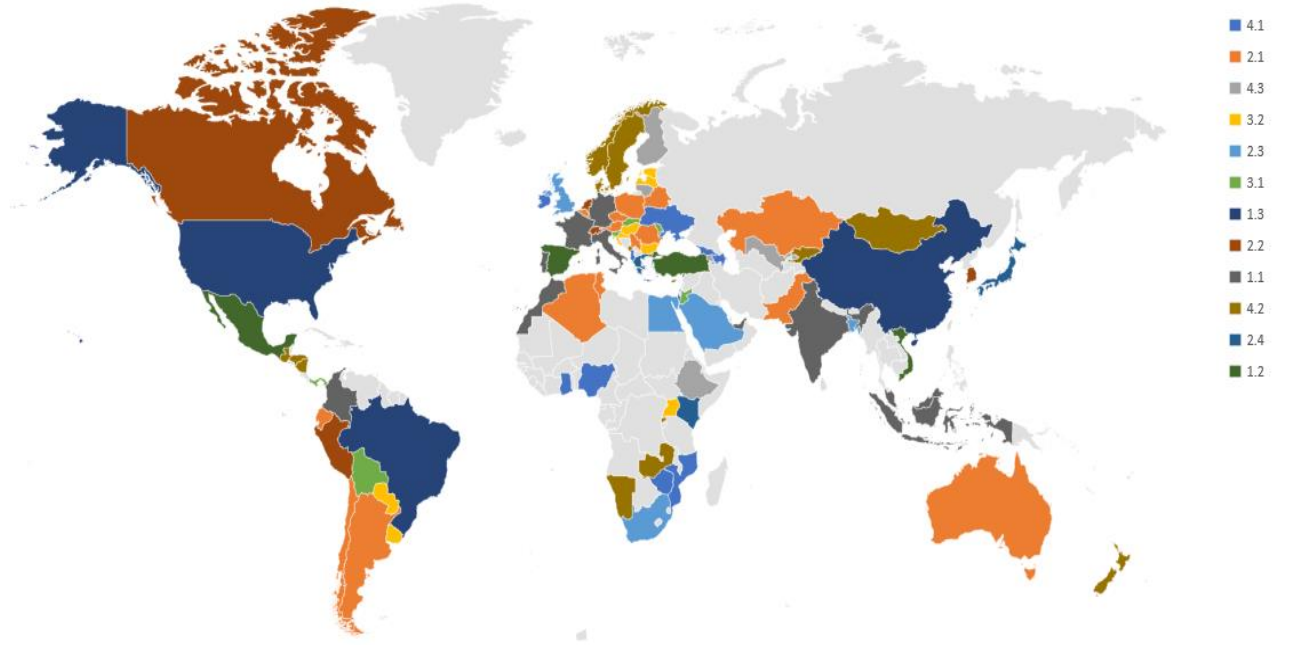


Рисунок 2.45 – Карта країн, поділених на кластери в залежності від виявлених кіберзлочинів

Джерело: розроблено авторами на основі Yarovenko et al. (2023)

Таблиця 2.13 – Результати кластерного аналізу

Кластер	Країни	Середнє значення MAV	Середнє значення IDS	Середнє значення VUL
1.1	Франція, Німеччина, Індія, Італія, Колумбія, Індонезія, Іран, Малайзія, Марокко, Португалія, Об'єднані Арабські Емірати	226463.27	3191437.27	54251.55
1.2	Мексика, В'єтнам, Туреччина, Іспанія	709347.25	5406983.75	60429.00
1.3	США, Китай, Бразилія	241351.33	16181266.33	136751.33
2.1	Алжир, Австралія, Австрія, Польща, Аргентина, Білорусь, Бельгія, Чехія, Еквадор, Казахстан, Румунія, Туніс, Чилі, Пакистан, Сербія, Сінгапур	51759.31	775175.06	12641.88
2.2	Нідерланди, Канада, Швейцарія, Південна Корея, Перу	37788.00	1751951.40	23692.20
2.3	Бангладеш, Єгипет, Південна Африка, Саудівська Аравія, Велика Британія	107084.20	1188240.80	22990.40
2.4	Японія, Греція, Кенія	132841.67	256754.33	38421.00
3.1	Панама, Болівія, Йорданія, Молдова, Словаччина, Словенія	16229.17	346157.33	1560.67
3.2	Бахрейн, Болгарія, Хорватія, Естонія, Угорщина, Парагвай, Уганда, Уругвай, Танзанія, Латвія	29107.20	167196.00	1904.50
4.1	Албанія, Азербайджан, Грузія, Гана, Ірландія, Зімбабве, Ізраїль, Мозамбік, Нігерія, Україна	9014.10	65207.00	1973.40
4.2	Кіпр, Гватемала, Гондурас, Киргизстан, Люксембург, Монголія, Чорногорія, Нова Зеландія, Нікарагуа, Норвегія, Руанда, Замбія, Данія, Намібія, Швеція	2873.93	69052.33	1702.13
4.3	Вірменія, Ефіопія, Фінляндія, Литва, Узбекистан	6430.40	190978.20	936.40

Джерело: розроблено авторами на основі Yarovenko et al. (2023)

Для доведення або відхилення висунутої першої гіпотези скористуємося статичними даними Power Index, який визначається на базі 50 факторів, що поєднуються за військовим, економічним та культурним потенціалом (Wisevoter, 2023). За даним рейтингом тільки 25 країн світу відносяться до найбільш потужних. При цьому 12 з них відносяться до країн, що є найбільш атакованими, тобто є країнами кластерів 1.3 (США, Китай та Бразилія), 1.2 (Іспанія, Туреччина та В’єтнам) та 1.1 (Франція, Німеччина, Італія, Індія, Індонезія та Іран). Тобто країни, які є найбільш атакованими, є також найбільш потужними країнами світу. При цьому, до топ-10 країн, які здійснюють кібератаки у бік інших, відносяться Китай (18.83%), США (17.05%), Бразилія (5.63%), Індія (5.33%), Німеччина (5.10%), В’єтнам (4.23%), Тайланд (2.51%), Росія (2.46%), Індонезія (2.41%), Нідерланди (2.20%) (DavidPur, 2022). Сім країн з даного переліку – це країни кластерів 1.1, 1.2 та 1.3. Інформація щодо Тайланду та Росії відсутні у обраній для даного дослідження вибірці. Щодо Нідерландів, то дана країна не попала до кластерів із країнами-найбільшими жертвами кіберзлочинів, але також її не було віднесено й до кластерів з найменшими.

Таким чином, можна сказати, що перша гіпотеза, висунута на початку дослідження, підтверджується для таких країн, як США, Китай, Бразилія, Іспанія, В’єтнам, Франція, Німеччина, Італія, Індія, Індонезія, Іран, та Туреччина, які з одного боку, є найбільш потужними країнами у світі та є найбільшими джерелами кібератак у світі. З іншого боку, вони також належать до кластерів країн, які є найбільшими жертвами кібератак. І хоча багато фахівців заперечують наявність кібервійн, то отриманий висновок може свідчити про наявність прихованих та неприхованих кібервійн, які здійснюють потужні країни світу, оскільки мають найбільший військовий потенціал у світі. Причинами цього, на нашу думку, є створення протистояння таких країн та сприяння ними зниження впливу інших на світовому рівні, нанесення шкоди їх економічному, соціальному, політичному секторам, та формування негативного іміджу на міжнародній політичній арені.

Для прийняття чи відхилення другої гіпотези необхідно проаналізувати соціально-економічні профайли кластерів країн, сформованих в залежно від рівня виявлених кіберзлочинів. Для цього було проведено асоціативний аналіз із використанням аналітичного пакету STATISTICA. Його результати представлені на рисунках 2.46-2.47.

Кластер 1.1 містить країни, які сильно відрізняються за своїм соціально-економічним розвитком. Саме тому результати асоціативного аналізу, представлені на рисунку 2.46a, показують тільки дві спільні характеристики, за якими ці країни можуть належати до даної групи. Це Index of Economic Freedom та Happiness Index. При цьому рівень економічної свободи вище середнього (IEF = 3) є однією з причин щастя на вище середньому рівні (HI = 3). Даний зв'язок є взаємообумовленим. Сумісна підтримка спостережень для цього кластеру дорівнює 45.45%, рівень достовірності коливається від 71.42% до 100%, а ймовірність того, що країни будуть знаходитися в одному кластері, дорівнює 0.85. Тобто, для ряду країн кластеру 1.1 є характерним те, що частка з них є дуже потужними, входять до топ-країн, що є ініціаторами кібератак та мають взаємообумовлений зв'язок між рівнем економічної свободи та щастя.

Рисунок 2.46b демонструє результати асоціативного аналізу кластеру 1.2, країни якого є найбільшими жертвами кібератак. Встановлено, що суттєвими характеристиками є ті, яким відповідають таким індикаторам, як National Cyber Security Index, Crime Index, Corruption Perceptions Index, Global Terrorism Index, Happiness Index та Life Expectancy at Birth. Результати містять 182 асоціативних правила, для яких сумісна підтримка спостережень дорівнює 50%, рівень достовірності коливається від 66.67% до 100%, а ймовірність знаходження країн з обраними характеристиками дорівнює 0.67-1.00. Тобто, країни кластеру 1.2 це країни з низьким рівнем тероризму, вище середнього рівнем розвитку національної кібербезпеки, очікуваної тривалості життя, щастя, корупції та злочинності в країні. З одного боку, для них характерним є комбінація соціально-економічного розвитку та присутність злочинності, корупції, що може сформувати певний імідж для кіберзлочинців, як країн-цілей кібершахрайств з метою отримання фінансово-економічних вигід.

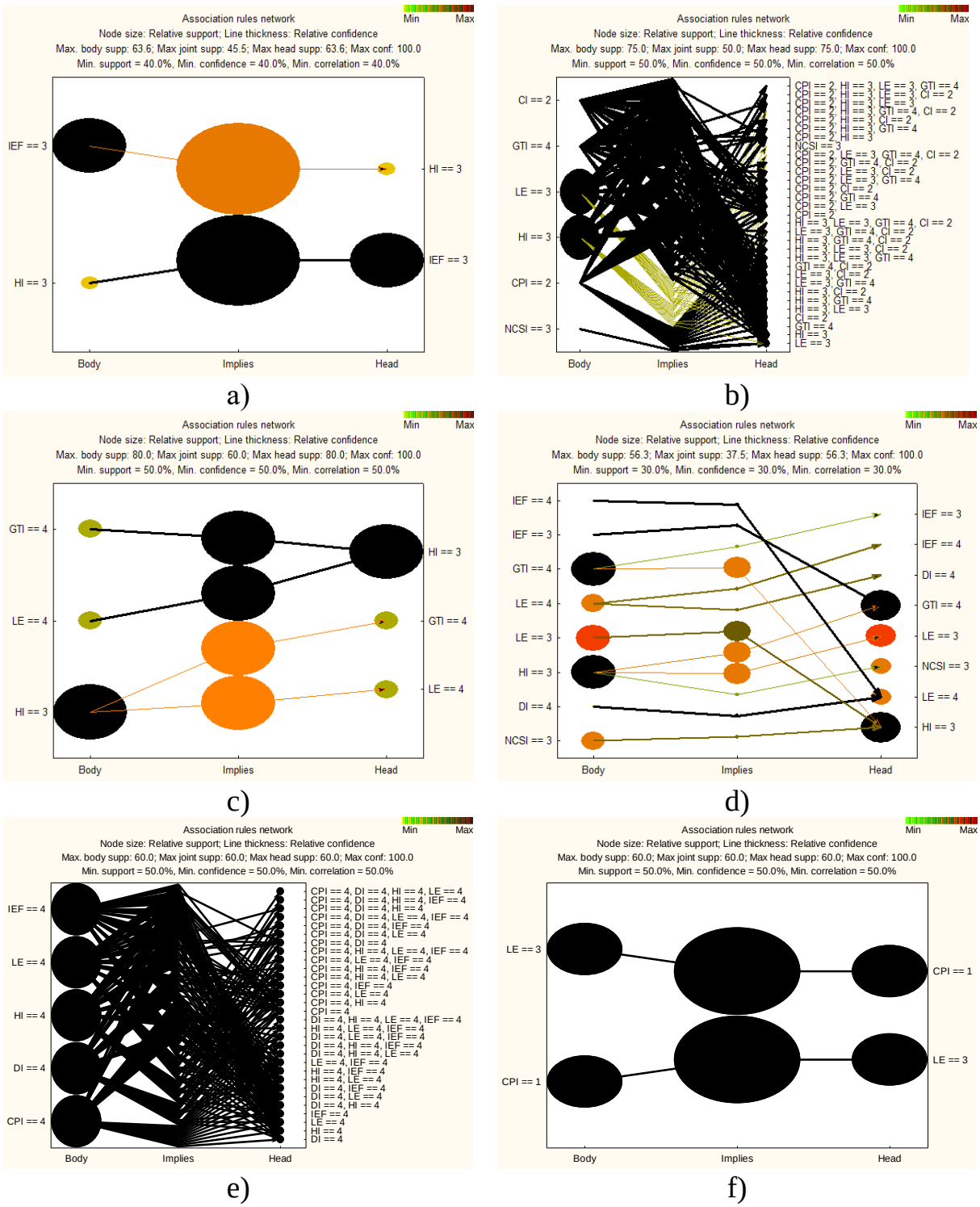


Рисунок 2.46 – Результати асоціативного аналізу для кластерів: a) 1.1; b) 1.2; c) 1.3; d) 2.1; e) 2.2; f) 2.3

Джерело: розроблено авторами на основі Yarovenko et al. (2023)

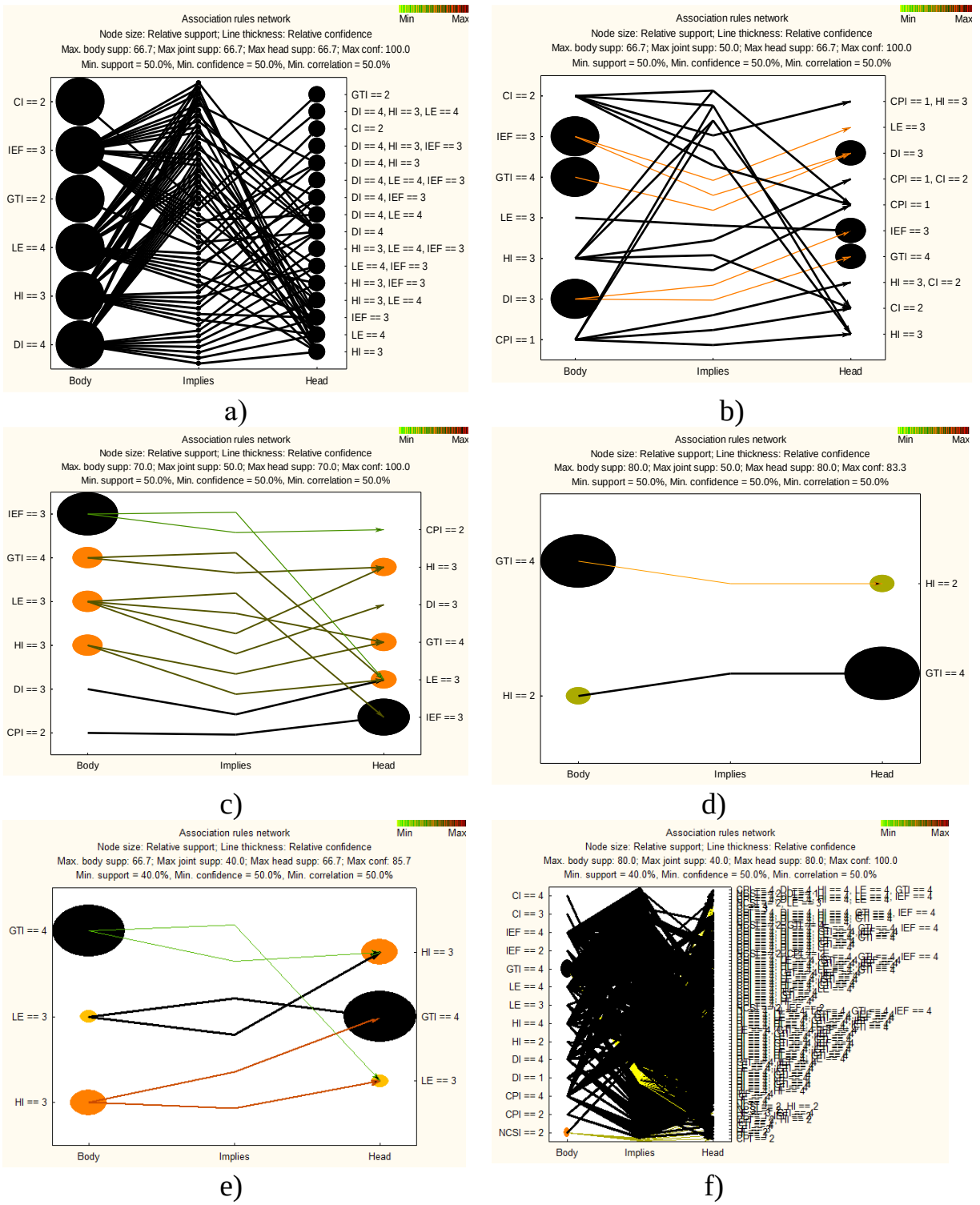


Рисунок 2.47 – Результати асоціативного аналізу для кластерів: a) 2.4; b) 3.1; c) 3.2; d) 4.1; e) 4.2; f) 4.3

Джерело: розроблено авторами на основі Yarovenko et al. (2023)

Асоціативний аналіз кластеру 1.3 країн – найбільших жертв кібератак, дозволив виявити суттєві характеристики цієї групи, яким відповідають Global Terrorism Index, Happiness Index та Life Expectancy at Birth (Рисунок 2.46c). При цьому всі три виступають один для одного й причиною, й наслідком. Наприклад, низький рівень впливу країни на глобальний рівень тероризму (GTI = 4) є однією з причин щастя на вище середньому рівні (HI = 3), який з іншого боку є причиною

для високого рівня очікуваної тривалості життя (LE = 4). Сумісна підтримка спостережень, для яких одночасно є вірним причина та наслідок дорівнює 60%. При цьому рівень достовірності для всіх спостережень коливається від 75% до 100%, а ймовірність того, що країни з обраними характеристиками будуть знаходитися в одному кластері, є досить високою і дорівнює 0.87. Тобто, в більшості випадків країни кластеру 1.3 є країни з низьким рівнем тероризму, високим рівнем очікуваної тривалості життя та рівнем щастя вище середнього. Інші характеристики для цих країн сильно відрізняються.

Кластери 2.1, 2.2 та 2.3 характеризуються також високим рівнем кібератак, але у порівнянні із країнами груп 1.1, 1.2 та 1.3, вони атакуються значно менше (Таблиця 2.13). Рисунок 2.46d демонструє асоціативні правила для кластеру 2.1, які визначили суттєві характеристики, яким відповідають National Cyber Security Index, Democracy Index, Happiness Index, Life Expectancy at Birth, Global Terrorism Index, та Index of Economic Freedom. Хоча значення сумісної підтримки спостережень коливається від 31.25% до 37.50%, але рівень достовірності знаходиться від 55.56% до 100% та кореляції від 66.67% до 84.52%. Тобто, третина країн кластеру 2.1 це країни з високим рівнем демократії, низьким рівнем впливу на глобальний тероризм, вище середнього рівнем щастя та кібербезпеки, високим та вище середнього рівнями економічної свободи та очікуваною тривалістю життя. На жаль, для формування профайлів інших країн з даного кластеру необхідно розширити перелік обраних для аналізу характеристик. Також можна припустити, що на це можуть впливати фактори, які виявити аналітичним шляхом дуже складно, або взагалі відсутність скритих мотивів кіберзлочинців.

Рисунок 2.46e показує, що для країн кластеру 2.2 є характерними високий рівень економічної свободи, очікуваної тривалості життя, демократії суспільства, щастя та низький рівень корупції. При цьому рівень підтримки дорівнює 60% для всіх асоціативних правил, рівень достовірності та кореляції – 100%. Тобто 60% країн даного кластеру відносяться до країн з високим рівнем соціально-економічного розвитку, що може стати метою кіберзлочинів. Для країн з групи 2.3 асоціативні правила дозволили виявити такі характеристики як Corruption Perceptions Index та Life Expectancy at Birth (Рисунок 2.46f). При цьому характерним для країн даного кластеру є високий рівень корупційної складової. Рівень підтримки для даної групи країн дорівнює 60%, рівень достовірності та кореляції – 100%. Слід сказати, що фактор високого рівня корупції може бути індикатором для формування іміджу країни, привабливого для кіберзлочинців.

Країни, які належать до кластерів 2.4, 3.1 та 3.2, також виступають жертвами кібератак, але у порівнянні із попередніми групами, вони становилися їх цілями значно менше (Таблиця 2.13). Асоціативні правила для групи 2.4 представлені на рисунку 2.47a та демонструють такі суттєві характеристики, як Crime Index, Democracy Index, Happiness Index, Life Expectancy at Birth, Global Terrorism Index, та Index of Economic Freedom. Це є справедливим для 66.67% країн (Греція та Японія) при рівнях достовірності та кореляції 100%. Слід відмітити, що ця група характеризується високим та вище середнього рівнями

розвитку економіки, щастя, тривалості життя та демократичних свобод. Також у даній групі є країни з рейтингом “2” (Греція та Кенія) для впливу на глобальний рівень тероризму та злочинності. Тобто кластер поєднав країни за полярними характеристиками – позитивним соціально-економічним розвитком та проблемами злочинного характеру.

Рисунок 2.47b демонструє характеристики для країн кластеру 3.1, до яких було віднесено низький рівень впливу на глобальний тероризм, вище середнього рівні щастя, демократії, економічної свободи, очікуваної тривалості життя, злочинності, а також високий рівень корупції. Визначені правила виконуються для 50% країн із достовірністю та кореляцією від 75% до 100%. Для країн кластеру 3.2 є характерним вище середнього рівні демократії, економічного розвитку, тривалості життя та щастя, корупції та низький вплив на глобальний рівень тероризму (Рисунок 2.47c). Це забезпечується із 50% підтримкою, достовірністю від 71.43% до 100.00% та кореляцією від 77.15% до 91.29%. Виходячи із отриманих міркувань для країн 3.1 та 3.2 кластерів рівень корупції може бути ключовим фактором для здійснення кіберзлочинів, але його вплив не може бути досить суттєвим.

Кластерами, до яких відносяться країни із найменшим рівнем кіберзлочинів, є кластери 4.1, 4.2 та 4.3 (Таблиця 2.13). Рисунок 2.47d показує, що для кластера 4.1 було виявлено тільки два правила, які характеризують причинно-наслідкові зв’язки між Global Terrorism Index та Happiness Index. При чому розмір кола, який відповідає Global Terrorism Index є великим, що свідчить про високий рівень підтримки для причини та для наслідку з боку даної характеристики, ніж для Happiness Index. Сумісна підтримка спостережень в цьому випадку дорівнює 50%, рівень достовірності коливається від 62.5% до 83.3%, а ймовірність знаходження в одному кластері дорівнює 0.72. Отримані показники є суттєвими. Тобто країни даного кластеру мають низький рівень впливу на глобальний тероризм, що відповідно робить їх не привабливими для масових кібератак. Рисунок 2.47e відображає результати асоціативного аналізу для кластеру 4.2. Виявлено, що характеристиками країн даної групи виступають Global Terrorism Index, Life Expectancy at Birth та Happiness Index. Сумісна підтримка асоціацій дорівнює 40% при досить високих значеннях рівня достовірності від 60% до 85.71%, а також ймовірності від 0.67 до 0.80. Для країн даного кластеру, так як і попередньої групи, характерним є низький вплив на рівень глобального тероризму (GTI = 4), але також суттєвим є сильний зв'язок між причиною очікуваної тривалості життя та іншими показниками (LE = 3 $\Rightarrow$ GTI = 4; LE = 3 $\Rightarrow$ HI = 3). Асоціативний аналіз для країн кластеру 4.3 виявив 642 асоціативних правила між характеристиками, яким відповідають вісім аналізованих індикаторів (Рисунок 2.47f). При цьому сумісна підтримка асоціацій дорівнює 40% при досить високих значеннях рівня достовірності від 50% до 100%, а також ймовірності від 0.58 до 1.00. Тобто дану групу складають країни, які можуть мати різну комбінацію соціально-економічних характеристик. Так, сюди входять країни із високим рівнем демократичних та економічних вільностей для населення, щастя, очікуваної тривалості життя, низьким рівнем

корупції та впливу на глобальний тероризм. Інша група, це країни із низьким рівнем демократії, впливом на глобальний тероризм та нижче середнього рівнем кібербезпеки, щастя та економічної свободи. Тобто, групи країн, які мають у своєму профайлі перелічені комбінації соціально-економічних характеристик в найменшій мірі є привабливими для масових кібератак та війн з боку інших країн.

Таким чином, виявлені характеристики профайлів кластерів країн із найбільшим та найменшим рівнем кібератак можуть підтвердити другу гіпотезу щодо опосередкованого впливу соціально-економічного розвитку країн на їх привабливість для кіберзлочинців. Про це говорить той факт, що знайдені асоціативні правила у більшості випадків характерні для країн із високим та вище середнього рейтингом соціально-економічного розвитку. Для інших країн закономірності не були встановлені або виявлено вплив окремих з них, таких як рівень корупції, злочинності, впливу на глобальний тероризм. Це свідчить про існування невиявлених в процесі дослідження факторів, що потребує подальших досліджень для їх ідентифікації.

В умовах сьогодення проблема кіберзлочинності є невід'ємною складовою науково-технічного прогресу, вирішення якої потребує багатьох зусиль з боку світових організацій, урядів країн і просто зацікавлених осіб. Але вона також становиться зручним інструментом для маніпулювання та досягнення політичних, фінансових, військово-стратегічних, психологічних та інших цілей як з боку окремих груп осіб, так й державних представників. Масова кіберзлочинність призводить до значних фінансових втрат, дестабілізації політичних, соціальних та економічних процесів, тому дане питання за часту ставиться на повістки дня такими міжнародними організаціями, як Економічна і Соціальна Рада ООН, Рада Європи, Міжнародна організація по боротьбі з кібертероризмом "ІМПАКТ", Міжнародний союз електрозв'язку та Управління ООН з наркотиків і злочинності та інші. В рамках такого співробітництва здійснюється розробка комплексу наукових, правових та організаційних заходів, які дозволяють формувати стратегії щодо регулювання та захисту поведінки користувачів у кіберпросторі. Це актуально в умовах здійснення кібервійн окремими країнами для зменшення наслідків їх агресії у бік інших. Тому запропоноване дослідження буде цікавим аналітичним підрозділам міжнародних організацій з метою виявлення потенційних жертв кіберзлочинів та розробці спеціальних заходів протидії та відповідальності у випадках цілеспрямованих кібератак, які призвели до катастрофічних наслідків.

В рамках даного дослідження було висунуто гіпотезу, що потужні за Power Index країни одночасно є ініціаторами кіберзлочинів у бік інших країн та є жертвами кіберагресій у більшій мірі, ніж країни зі слабким впливом на світовому рівні. Дана гіпотеза була підтверджена повністю на основі проведеного кластерного аналізу та порівняння його результатів із доступними статистичними даними. Виявлено, що найбільш потужні країни в світі, а саме США, Китай, Бразилія, Іспанія, В'єтнам, Франція, Німеччина, Італія, Індія, Індонезія, Іран, та Туреччина, піддаються кіберзлочинам більше, ніж інші. При

цьому вони також є джерелами активних кібератак у бік інших. Висновки цього дослідження можуть стати підґрунтям для розробки відповідних стратегій стримування таких країн у випадках їх активних дій. Ці знання будуть корисними для формування попереджувального комплексу дій, націленого на відслідковування потоків різного роду транзакцій саме з тих країн, які є джерелами кібератак та належать до критичних групам. Накопичення ретроспективних даних за більш тривалий період часу та їх використання для розширення запропонованої методики дослідження дозволить сформувати більш ймовірні структури кластерів країн – жертв кіберзлочинів та країн – кіберхижаків.

Соціально-економічні профайли кластерів країн, визначені за обсягами виявлених кібератак, що здійснювалися через поштові сервіси та мережу, було сформовано на основі проведення асоціативного аналізу. Його результати дозволили виявити ті характеристики, які є властивими для більшості країн визначених груп. При чому було виділено як їх комбінації, так й окремі з них, що може стати ключовим фактором у розумінні мотивів кіберзлочинів у світовому масштабі. Аналіз профайлів груп країн, які атакуються в меншій мірі, засвідчив, що важливим аспектом відсутності мотивації для кіберзлочинців є низький вплив даних країн на глобальний рівень тероризму. Також сюди увійшли країни як з високим рівнем соціально-економічного розвитку, так й менш розвинені. Аналіз профайлів кластерів країн – найбільших жертв кібератак показав, що за більшістю характеристик сюди увійшли країни з високим та вище середнього рейтингом соціально-економічного розвитку, більшість з яких є потужними та тими, які є джерелом масових кібератак. Щодо інших кластерів важливим є аспект впливу високого рівня корупції, що може бути індикатором для таргетованих кібератак для отримання фінансових вигід. Отримані результати дозволили підтвердити висунуту гіпотезу, що рівень соціально-економічного розвитку країн може бути опосередкованою мотивацією кіберзлочинців для масових кібератак, а саме на це може впливати рівень корупції, злочинності та впливу на глобальний тероризм. Висновки даного аналізу можуть допомогти в удосконаленні стратегії боротьби із кіберзлочинністю, як на рівні окремої країни, так і світу в цілому, з урахуванням ключових індикаторів, які впливають на мотивацію кіберзлочинців.

ВИСНОВКИ

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

Однією із головних причин появи фінансових шахрайств є зростаюча у геометричній прогресії кількість пристроїв з конфіденційними фінансовими даними, що підключаються до мережі Internet, а також розширення кіберпростору, наслідком чого є : 1) онлайн атаки на програмне та апаратне забезпечення серверів, мережевих пристроїв, одиночних кінцевих користувачів, за допомогою шкідливих програм – віруси, трояни, шпигунське програмне забезпечення, з метою крадіжки конфіденційної інформації, перевірок шахраями рівня захисту об’єкту, отримання контролю над комп’ютерним обладнанням об’єкту нападу; 2) ботнети Internet of Things – технологія, що дозволяє через мережу Internet чи подібну мережу встановлювати віддалені з’єднання між інтелектуальними пристроями; 3) фішингова загроза для фінансових платежів – через підроблені сайти виступає причиною шахрайських операцій, компрометації особистих та корпоративних даних, розповсюдження небезпечного програмного забезпечення; 4) розповсюдження спамів через розгалужені платформи соціальних мереж; 5) порушення даних, вразливість від непрямих атак, через недоліки безпеки у веб-інфраструктурі, веб-додатках, веб-завантаженнях; 6) прогалини у практичних навичках працівників кібербезпеки, недостатність фахівців з кіберзахисту; 7) хмарна небезпека інформаційних ресурсів – через повсюдний доступ до мережі, об’єднання ресурсів для спільного використання, контроль та управління даними постачальниками хмарних послуг, зростає ризик кібератак на ці ресурси.

При оцінці взаємозв’язків між детермінантами процесу протидії легалізації доходів, отриманих незаконним шляхом, було визначено, що при зростанні рівня діджиталізації на 1% рівень розвитку регулювання ринку фінансових послуг буде зростати на 0,30%; позитивний вплив підвищення рівня діджиталізації на 1% здійснює на рівень розвитку правоохоронної системи, яка буде зростати відповідно на 0,93%; спостерігається обернений вплив діджиталізації на судову систему, рівень розвитку якої буде зменшуватись на 0,09% при 1%-ому зростанні рівня діджиталізації; прямо пропорційний вплив виявлено в розрізі залежності правоохоронної та судової систем, тобто при зростанні рівня розвитку

правоохоронної системи на 1% рівень розвитку судової системи буде збільшуватись на 0,81%;

Концепція конвергенції систем фінансового моніторингу і кібербезпеки відображає сучасну реальність, в якій фінансова злочинність і кіберзагрози стають взаємопов'язаними і важливими викликами для суспільства. Поєднання зусиль у галузі фінансового моніторингу та кібербезпеки може призвести до більш ефективного виявлення та запобігання таким загрозам. Цей підхід визнає, що обидві системи спільно працюють для досягнення загальної мети - захисту фінансових ресурсів і кіберпростору від зловживань та атак. Використання інноваційних технологій та аналізу даних може підвищити ефективність цих систем і зробити їх більш адаптивними до змінюючихся загроз. Важливо наголосити на необхідності співпраці і обміну інформацією між країнами та секторами, оскільки кіберзлочинність і фінансова злочинність не мають кордонів. Міжнародний підхід до цього питання стає дедалі важливішим. Забезпечення захисту особистих даних і приватності користувачів - це ще один важливий аспект при впровадженні концепції конвергенції. Необхідно знайти баланс між забезпеченням безпеки та захистом приватності. Все це вказує на важливість системного підходу до вирішення проблем фінансової злочинності і кіберзагроз. Об'єднуючи зусилля та застосовуючи передові технології, ми можемо створити більш безпечне та стійке цифрове середовище для сучасного світу.

На основі аналізу біфуркацій, були створені графічні подання "зрілості системи", "точок рівноваги" і "релаксаційних коливань втрати стійкості" у сфері захисту від фінансових та кібер загроз. Ця методика дозволила побудувати комплексний показник конвергенції системи на основі методу Сундаровського згортки. Також були ідентифіковані ключові фактори впливу на цей індекс кібербезпеки з використанням методу сигма-обмеженої параметризації та Парето-оптимізації. Побудовані залежності між інтегральним індексом кібербезпеки та суттєвими впливовими факторами шляхом застосування нелінійної регресії з поступовим виключенням змінних. Здійснено аналіз стабільності системи захисту від фінансових та кібер загроз з використанням біфуркаційного аналізу та створені графічні подання "зрілості системи", "точок рівноваги" і "релаксаційних коливань втрати стійкості" для цієї системи. Також доведено доцільність опису динаміки системи, яка перебуває в нерівноважному стані, з використанням фазових діаграм "нестійкий фокус" та "нестійкий вузол" в залежності від різних проекцій "зрілості" і "релаксаційних коливань втрати стійкості".

Було проведено оцінку потенційної зближеності систем кібербезпеки та боротьби з легалізацією кримінальних прибутків і фінансуванням тероризму. Ця оцінка ґрунтувалася на визначенні інтегральних показників та використанні функції Харрінгтона-Менчера. Це дозволило виявити можливі сценарії взаємодії між системами кібербезпеки та протидії фінансовим злочинам у країнах з різним рівнем економічного розвитку, залежно від загального рівня кібербезпеки,

ефективності протидії легалізації кримінальних прибутків і загального рівня зближеності між ними.

Були запропоновані методи ідентифікації кіберзлочинців, використовуючи методи аналізу даних, такі як об'єднана регресія, LASSO, RIDGE, Elastic Net регресія, класифікаційне дерево та нейронна мережа. Цей підхід дозволив виявити, що найбільш ефективними є методи класифікаційного дерева та нейронної мережі, які забезпечують можливість ідентифікації кіберзлочинців з високим рівнем довіри, досягаючи 90% точності.

За допомогою методу визначення центра мас, були розроблені чотириполюсні барицентричні моделі для досягнення збалансованого розвитку національної економіки. Ці моделі об'єднують композитні індикатори економічного, соціального та політичного розвитку країни, а також рівень захисту від фінансових шахрайств і кібербезпеки. За допомогою цих моделей було проведено розрахунки, враховуючи три аспекти: значення складових цілей (використовуючи середнє геометричне), рівень парного балансу (як суму протилежних пар чотирикутних кутів) і відстань між фактичним та нормативним центрами мас для всіх чотирьох цілей. Аналіз результатів дозволив ідентифікувати країни з найбільш ефективними стратегічними цілями, країни з незбалансованими цільовими парними величинами і розподілити країни за відстанями між їх центрами мас.

Стратегія ребілдингу архітектоніки системи держфінмоніторингу є критичним етапом у вдосконаленні державних фінансових систем і забезпеченні їхньої ефективної роботи. Вона надає можливість системі адаптуватися до змін в економіці та зростаючих фінансових ризиків. Запропонована в роботі стратегія сприятиме підвищенню точності та ефективності системи за рахунок застосування передових технологій і інструментів, що дозволить покращити виявлення фінансових аномалій та мінімізувати ризики. Забезпечення високого рівня кібербезпеки є необхідним аспектом стратегії, оскільки фінансова система піддається загрозам з кіберпростору. Захист фінансових даних та особистої інформації користувачів стає пріоритетним завданням. Реалізація стратегії полегшить організацію співпраці з іншими країнами та організаціями, оскільки фінансові операції та атаки можуть мати міжнародний характер. Міжнародний підхід сприяє більш успішній боротьбі з фінансовою злочинністю. Система повинна залишатися гнучкою і готовою до змін в фінансовому середовищі, і регулярне оновлення та адаптація є важливими елементами стратегії. Завдяки цій стратегії, можливо досягти покращення надійності та ефективності фінансових систем, забезпечити високий рівень безпеки та прозорості, а також відповісти на сучасні виклики фінансового світу.

Аналіз соціально-економічних профайлів кластерів країн, які стали жертвами кібератак через поштові сервіси та мережі, базувався на асоціативному аналізі. Його результати виявили спільні характеристики, які властиві більшості країн у кожному з визначених кластерів. Також було виявлено комбінації та окремі характеристики, які можуть відігравати ключову роль у розумінні мотивації кіберзлочинців на глобальному рівні. Аналіз профайлів країн, які рідко

стають жертвами кібератак, підтвердив, що низький вплив цих країн на глобальний рівень тероризму може бути важливим аспектом відсутності мотивації для кіберзлочинців. В цей кластер включені як країни з високим рівнем соціально-економічного розвитку, так і менш розвинені. Аналіз профайлів країн, що є найбільшими жертвами кібератак, показав, що більшість з них мають високий рівень соціально-економічного розвитку і є потужними центрами кібератак. Деякі інші кластери демонструють вплив високого рівня корупції, що може бути фактором для таргетованих кібератак з метою фінансового зиску. Отримані результати підтверджують гіпотезу, що рівень соціально-економічного розвитку країн може впливати на мотивацію кіберзлочинців для масових кібератак, і враховувати такі ключові індикатори може сприяти удосконаленню стратегії боротьби з кіберзлочинністю на рівні окремих країн і в світовому контексті.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

Acwalks (2021). *Відмивання грошей*. URL: https://acwalks.com.ua/knowledgebase/vidmyvannia-hroshey/ (дата звернення: 01.12.2021).

Addo A., Senyo PK. Digitalization and government corruption in developing countries: towards a framework and research agenda. *Academy of Management Proceedings*, 2020. №1. DOI: 10.5465/AMBPP.2020.16765abstract

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. 12(1). URL: https://doi.org/10.4018/IJBIR.20210101.oa5

Akinbowale O. E., Klingelhöfer H. E., Zerihun M. F. Analysis of cyber-crime effects on the banking sector using the balanced score card: A survey of literature. *Journal of Financial Crime*. 2020, vol. 27(3). P. 945-958. DOI: https://doi.org/10.1108/JFC-03-2020-0037.

Albulescu, C., Tamasila, M., & Taucean, I. (2016). SE, tax policies, institutional weakness and financial stability in selected OECD countries. Economics Bulletin, 36(3), 1868-1875. Retrieved from http://www.accessecon.com/Pubs/EB/2016/Volume36/EB-16-V36-I3- P182.pdf

Alhogail A., Alsabih A. Applying machine learning and natural language processing to detect phishing email. *Computers and Security*. 2021. 110. URL: https://doi.org/10.1016/j.cose.2021.102414

Alshamasi S., Menai M. Ensemble-based clustering for writing style change detection in multi-authored textual documents. *Paper presented at the CEUR Workshop Proceedings.* 2022, art. no. 3180. P. 2357-2374.

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. 9(3).

Andreou P. C., Anyfantaki S. Financial literacy and its influence on internet banking behavior. *European Management Journal*. 2021. 39(5). URL: https://doi.org/10.1016/j.emj.2020.12.001

Arcuri M. C., Gai L., Ielasi F., Ventisette E. Cyber attacks on hospitality sector: stock market reaction. *Journal of Hospitality and Tourism Technology*. 2020. 11(2). URL: https://doi.org/10.1108/JHTT-05-2019-0080

ATKearney &VISA (2017). Digital Payments and the Global Informal Economy. URL: https://www.kearney.com/industry/financial-services/digital-payments-and-the-global-informal-economy

BBC. *Ukraine cyber-attack: Russia to blame for hack, says Kyiv*. URL: https://www.bbc.com/news/world-europe-59992531 (дата звернення: 31.05.2022).

Berdiev, A. N., & Saunoris, J. W. (2016). Financial development and the shadow economy: A panel VAR analysis. *Economic Modelling*, *57*, 197–207. https://doi.org/10.1016/j.econmod.2016.03.028

Berdyugin A. A., Revenkov P. V. Cyberattack risk assessment in electronic banking technologies (the case of software implementation). *Finance: Theory and Practice*. 2020. 24(6). URL: https://doi.org/10.26794/2587-5671-2020-24-6-51-60

Bernasco, W., Ruiter, S., & Block, R. (2017). 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*, *54*(2), 244–275. https://doi.org/10.1177/0022427816680681

Bing C., Schectman J. (2019). *Inside the UAE's secret hacking team of American mercenaries.* URL: https://www.reuters.com/investigates/special-report/usa-spying-raven/ (дата звернення: 01.05.2023).

Blackburn, K., Bose, N., & Capasso, S. (2012). Tax evasion, the underground economy and financial development. *Journal of Economic Behavior and Organization*, *83*(2), 243–253. https://doi.org/10.1016/j.jebo.2012.05.019

Boitan, I. A., & Ștefoni, S. E. (2023). Digitalization and the Shadow Economy: Impact Assessment and Policy Implications for EU Countries. *Eastern European Economics*, *61*(2), 152–180. https://doi.org/10.1080/00128775.2022.2102508

Camoletto, S., Corazza, L., Pizzi, S., & Santini, E. (2022). Corporate social responsibility due diligence among european companies: The results of an interventionist research project with accountability and political implications. *Corporate Social Responsibility and Environmental Management, 29*(5), 1122-1133. doi:10.1002/csr.2258

Canhoto A.I. Leveraging machine learning in the global fight against money laundering and terrorism financing: An affordances perspective. *Journal of Business Research*, 2021. №131. P. 441-452. DOI: 10.1016/j.jbusres.2020.10.012

Carlton M., Levy Y., Ramim M. Mitigating cyber attacks through the measurement of non-IT professionals' cybersecurity skills. *Information and Computer Security*. 2019. 27(1). https://doi.org/10.1108/ICS-11-2016-0088

Chen Z., Van Khoa L.D., Teoh E.N., Nazir A., Karuppiah E.K., Lam K.S. Machine learning techniques for anti-money laundering (AML) solutions in suspicious transaction detection: a review. *Knowledge and Information Systems*. 2018, №57(2). P. 245–285. DOI: https://doi.org/10.1007/s10115-017-1144-z.

Chen, D., Wawrzynski, P., & Lv, Z. (2021). Cyber security in smart cities: A review of deep learning-based applications and case studies. *Sustainable Cities and Society*, *66*. https://doi.org/10.1016/j.scs.2020.102655

CyberPeace Institute. *UKRAINE: Timeline of Cyberattacks on critical infrastructure and civilian objects*. URL: https://cyberpeaceinstitute.org/ukraine-timeline-of-cyberattacks/ (дата звернення: 31.05.2022).

DavidPur N. (2022). *Which Countries are Most Dangerous? Cyber Attack Origin – by Country*. URL: https://blog.cyberproof.com/blog/which-countries-are-most-dangerous (дата звернення: 01.05.2023).

Dawson M. Applying a holistic cybersecurity framework for global IT organizations. *Business Information Review*. 2018, № 35(2). P. 60–67. DOI: https://doi.org/10.1177/0266382118773624.

de Castro Halis D. Digitalization and Dissent in Legal Cultures. Chinese and Other Perspectives. Naveiñ Reet: *Nordic Journal of Law and Social Research (NNJLSR)*, 2019. №9. P. 127-152. URL: https://tidsskrift.dk/nnjlsr/issue/download/8857/1189#page=129

Deloitte, (2019). *The connected defense: Elevating the fight against financial crime. Using 4IR technologies to prevent and detect the growing ecosystem of financial crime*. URL: https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/financial-services/deloitte-nl-fsi-elevating-the-fight-against-financial-crime.pdf (дата звернення: 31.05.2022).

Deutsche Welle (2022). *Ukrainian websites hacked in 'global attack'*. URL: https://www.dw.com/en/ukraine-government-websites-hacked-in-global-attack/a-60421475 (дата звернення: 01.05.2023).

Deva, S. (2023). Mandatory human rights due diligence laws in europe: A mirage for rightsholders? *Leiden Journal of International Law*, doi:10.1017/S0922156522000802

Dileep M.R., Navaneeth A.V., Abhishek M. A novel approach for credit card fraud detection using decision tree and random forest algorithms. In *Proceedings of the 3rd International Conference on Intelligent Communication Technologies and Virtual Mobile Networks, ICICV 2021*. 2021. P. 1025–10284. DOI: https://doi.org/10.1109/ICICV50876.2021.9388431.

Dionysios S. Demetis. *Technology and Anti-Money Laundering: A Systems Theory and Risk-Based Approach*. Edward Elgar Publishing, Incorporated, 2010. P. 188.

Dobrowolski Z., Sułkowski Ł. Implementing a Sustainable Model for Anti-Money Laundering in the United Nations Development Goals. *Sustainability*, 2020. №12(1):244. DOI: 10.3390/su12010244

Dotsenko Tetiana, Berezhna Darina. TRENDS IN DUE DILIGENCE MODELING TO COMBAT FINANCIAL CYBER FRAUD // Cybersecurity Challenges Facing the Financial Services Industry: matherial of the International virtual conference, Sumy, Ukraine, June, 2 2023. Sumy: Sumy State University, 2023. P. 120-123. https://ek.biem.sumdu.edu.ua/wp-content/uploads/wpforo/default_attachments/1685651966-trends-in-due-diligence-modeling-to-counter-financial-cyber-fraud.pdf

Dotsenko Tetiana, Yarovenko Hanna, Berezhna Darina. (2023). Due diligence in the aspect of countering financial cyber fraud: modeling trends. Economic Herald of State Higher Educational Institution «Ukrainian State University of Chemical Technology», 1, 20-30. http://dx.doi.org/10.32434/2415-3974-2022-17-1-20-30

Dupuis D., Gleason K. Money laundering with cryptocurrency: open doors and the regulatory dialectic. *Journal of Financial Crime*, 2020. №28(1), P. 60-74. DOI: 10.1108/JFC-06-2020-0113

Economist Intelligence (2023). *Democracy Index.* URL: https://www.eiu.com/n/campaigns/democracy-index-2022/?utm_source=google&utm_medium=paid-search&utm_campaign=democracy-index-2022&gclid=CjwKCAjwgqejBhBAEiwAuWHioAEruOQA25JyHg-61MBEiYNJp9hvu3Pf91E_tWO2W0nauZ6on003ORoC6UsQAvD_BwE (дата звернення: 01.05.2023).

E-Governance Academy (2023). *National Cyber Security Index.* URL: https://ncsi.ega.ee/ncsi-index/ (дата звернення: 01.05.2023).

Elbel, J., Bose O'Reilly, S., & Hrzic, R. (2023). A european union corporate due diligence act for whom? considerations about the impact of a european union due diligence act on artisanal and small-scale cobalt miners in the democratic republic of congo. *Resources Policy, 81* doi:10.1016/j.resourpol.2022.103241

ENISA THREAT LANDSCAPE 2021. European Union Agency for Cybersecurity. URL: https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends

Ethereum Fraud Detection Dataset. Kaggle. URL: https://www.kaggle.com/datasets/vagifa/ethereum-frauddetection-dataset

EuRepoc Data. European Repository of Cyber Incidents. URL: https://eurepoc.eu/databases

Euronews. *Ukraine's defence ministry and two banks targeted in cyberattack*. URL: https://www.euronews.com/my-europe/2022/02/15/ukraine-s-defence-ministry-and-two-banks-targeted-in-cyberattack (дата звернення: 31.05.2022).

Europeans' attitudes towards cyber security. Special Eurobarometer 499. European Commision. 2020. URL: https://europa.eu/eurobarometer/surveys/detail/2249

Eurostat. Cloud computing - statistics on the use by enterprises. URL: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Cloud_computing_-_statistics_on_the_use_by_enterprises

Eurostat. Use of Internet of Things in enterprises. URL: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Use_of_Internet_of_Things_in_enterprises#Enterprises_using_IoT

Fedotova G. V., Gontar A. A., Titov V. A., Kurbanov A. K., Kuzmina E. V. Increasing the economic security of information banking systems. In book: *Ubiquitous Computing and the Internet of Things: Prerequisites for the Development of ICT*. 2019. P. 1153-1161. DOI: https://doi.org/10.1007/978-3-030-13397-9_118.

Ferwerda J., Kleemans E.R. Estimating Money Laundering Risks: An Application to Business Sectors in the Netherlands. *Eur J Crim Policy Res*, 2019. №25. P. 45-62. DOI: 10.1007/s10610-018-9391-4

FinCEN, (2009). *Mortgage Loan Fraud Connections with Other Financial Crime: An Evaluation of Suspicious Activity Reports Filed By Money Services Businesses, Securities and Futures Firms, Insurance Companies and Casinos*. URL: https://www.fincen.gov/sites/default/files/shared/ mortgage_fraud.pdf (дата звернення: 31.05.2022).

Gagliani G. Cybersecurity, Technological Neutrality, and International Trade Law. *Journal of International Economic Law*. 2020, № 23(3). P. 723–745. DOI: https://doi.org/10.1093/jiel/jgaa006.

Gao S., Xu D., Wang H., Green, P. Knowledge-based anti-money laundering: a software agent bank application. Journal of Knowledge Management. 2009, №13(2). P. 63-75. DOI: https://doi.org/10.1108/13673270910942709

Grand View Research. Cloud Computing. URL: https://www.grandviewresearch.com/industry-analysis/cloud-computing-industry#

Guanipa, H. J., & Chimá, J. T. (2023). Integrality human rights-rights of nature: Towards corporate due diligence and sustainable energy transition. [Integralidad derechos humanos-derechos de la naturaleza: hacia la debida diligencia empresarial y la transición energética sostenible] *Revista Derecho Del Estado*, (54), 307-344. doi:10.18601/01229893.n54.10

Haberman, C. P., & Ratcliffe, J. H. (2015). Testing for Temporally Differentiated Relationships among Potentially Criminogenic Places and Census Block Street Robbery Counts. *Criminology*, *53*(3), 457–483. https://doi.org/10.1111/1745-9125.12076

Haruna, E. U., & Alhassan, U. (2022). Does digitalization limit the proliferation of the shadow economy in African countries? An in-depth panel analysis. *African Development Review*, *34*(S1), S34–S62. https://doi.org/10.1111/1467-8268.12653

Horban H., Kandyba I., Dvoretskyi M., Boiko A. Principles of searching for a variety of types of associative rules in OLAP-cubes. *CEUR Workshop Proceedings*. 2021. 2845. P.181-192.

https://www.emarketer.com/content/global-social-network-users-2020.

Yarovenko H. Evaluating the threat to national information security. *Problems and Perspectives in Managemen*. 2020, № 18(3), P. 195–210. DOI: https://doi.org/10.21511/ppm.18(3).2020.17.

Yarovenko H., Kolotilina O., Svitlychna A. Assessment Of The Convergence Level Of The Cyber Security System And Counteraction Of Money Laundering *The Journal of V. N. Karazin Kharkiv National University. Series: International Relations. Economics. Country Studies. Tourism*. 2021. №14. P. 119–130. (in Ukrainian). DOI: https://doi.org/10.26565/2310-9513-2021-14-12.

Yarovenko H., Lopatka A., Vasilyeva T., Vida I. Socio-economic profiles of countries - cybercrime victims. *Economics and Sociology*. 2023, №16(2). P. 167-194. DOI: https://doi.org/10.14254/2071-789X.2023/16-2/11

IBM. What is a cyberattack? URL: https://www.ibm.com/topics/cyber-attack

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

Yevseiev, S., Rzayev, K., Mammadova, T., Samedov, F., & Romashchenko, N. (2018). КЛАСИФІКАТОР КІБЕРЗАГРОЗ ІНФОРМАЦІЙНИХ РЕСУРСІВ

АВТОМАТИЗОВАНИХ БАНКІВСЬКИХ СИСТЕМ. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, *2*(2), 47–67. https://doi.org/10.28925/2663-4023.2018.2.4767

Ying, W., Jia, S., & Du, W. (2018). Digital enablement of blockchain: Evidence from HNA group. International Journal of Information Management, 39, 1-4. https://doi.org /10.1016/j. ijinfomgt.2017.10.004

Institute for Economics and Peace (2022). *Global Terrorism Index 2022*. URL: https://reliefweb.int/report/world/global-terrorism-index-2022 (дата звернення: 01.05.2023).

Internet Crime Report. *Federal Bureau of Investigation*. URL: https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

ISO. Information technology — Cybersecurity — Overview and concepts ISO/IEC TS 27100:2020. URL: https://www.iso.org/obp/ui/#iso:std:iso-iec:ts:27100:ed-1:v1:en

Jouini, M., Rabai, L. B. A., & Aissa, A. B. (2014). Classification of security threats in information systems. In *Procedia Computer Science* (Vol. 32, pp. 489–496). Elsevier B.V. https://doi.org/10.1016/j.procs.2014.05.452

Kanimozhi V., Prem Jacob T. Artificial intelligence based network intrusion detection with hyper-parameter optimization tuning on the realistic cyber dataset CSE-CIC-IDS2018 using cloud computing. Paper presented at the *Proceedings of the 2019 IEEE International Conference on Communication and Signal Processing*, *ICCSP*. 2019. P. 33-36. DOI: https://doi.org/10.1109/ICCSP.2019.8698029.

Karpunina E.K., Mikhailov A.M., Bondareva N.A., Lyubimenko O.A., Fedotova E.V. Blockchain Technologies as a Reflection of Modern Reality: Diversity of Opportunities Versus Security Risks. *Studies in Systems, Decision and Control*. 2021, № 314. P. 3–14. DOI: https://doi.org/10.1007/978-3-030-56433-9_1.

Kaspersky (2023). *Cyberthreat real-time map.* URL: https://cybermap.kaspersky.com/ (дата звернення: 01.05.2023).

Khattak, M. A., Ali, M., Azmi, W., & Rizvi, S. A. R. (2023). Digital transformation, diversification and stability: What do we know about banks? *Economic Analysis and Policy*, *78*, 122–132. https://doi.org/10.1016/j.eap.2023.03.004

Kobushko I., Tiutiunyk I., Kobushko I., Starinskyi M., Zavalna, Z. The triadic approach to cash management: Communication, advocacy, and legal aspects. *Estudios De Economia Aplicada*, 2021. №39(7). DOI: 10.25115/eea.v39i7.5071

Krebs B. (2021). *At Least 30,000 U.S. Organizations Newly Hacked Via Holes in Microsoft's Email Software*. URL: https://krebsonsecurity.com/2021/03/at-least-30000-u-s-organizations-newly-hacked-via-holes-in-microsofts-email-software/ (дата звернення: 01.05.2023).

Krebsonsecurity. *Report: Recent 10x Increase in Cyberattacks on Ukraine*. URL: https://krebsonsecurity.com/2022/03/report-recent-10x-increase-in-cyberattacks-on-ukraine/ (дата звернення: 31.05.2022).

Kuzmenko O., Yarovenko H., Perkhun L. Assessing the maturity of the current global system for combating financial and cyber fraud. Statistics in Transition New

Seriesthis. 2023, №24(1). P. 229–258. DOI: https://doi.org/10.59170/stattrans-2023-013

Lebid O.U. (2015). Some aspects of cognitive modeling in public administration. *Public administration: improvement and development. 11. URL: http://www.dy.nayka.com.ua/?op=1&z=922*

Lekha K. C., Prakasam S. Data mining techniques in detecting and predicting cyber crimes in banking sector. Paper presented at *the 2017 International Conference on Energy, Communication, Data Analytics and Soft Computing, ICECDS*. 2017. P. 1639–1643. DOI: https://doi.org/10.1109/ICECDS.2017.8389725.

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, *7*, 8176–8186. https://doi.org/10.1016/j.egyr.2021.08.126

Lieonov S., Zolkover A., Bozhenko V. Shadow economy channels and their impact on macroeconomic stability. Причорноморські економічні студії. 2019. Вип. 44. С. 98-101

Liesa, C. R. F. (2022). Business due diligence and human rights: Towards a spanish law. [La debida diligencia de las empresas y los Derechos Humanos: hacia una ley española] *Cuadernos De Derecho Transnacional*, *14*(2), 427-455. doi:10.20318/cdt.2022.7190

Litwin, D. (2023). Business impacts on economic inequality: An agenda for defining related human rights impacts and economic inequality due diligence. *Business and Human Rights Journal*, *8*(1), 90-96. doi:10.1017/bhj.2022.27

Lowry, P. B., Zhang, J., Wang, C., & Siponen, M. (2016). 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. *Information Systems Research*, *27*(4), 962–986. https://doi.org/10.1287/isre.2016.0671

Lucas G. *Ethics and Cyber Warfare: The Quest for Responsible Security in the Age of Digital Warfare*. Oxford University Press, 2016.

Medina, L., & Schneider, F. G. (2021). Shedding Light on the Shadow Economy: A Global Database and the Interaction with the Official One. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3502028

Mekterović I., Karan M., Pintar D., Brkić L. Credit card fraud detection in card-not-present transactions: Where to invest? *Applied Sciences (Switzerland)*. 2021, №11(151). Article number 6766. DOI: https://doi.org/10.3390/app11156766

Mishra S.P., Kumari P. Analysis of techniques for credit card fraud detection: A data mining perspective. *Advances in Intelligent Systems and Computing*. 2020, №1030. P. 89–98. DOI: https://doi.org/10.1007/978-981-13-9330-3_9

Morgan S. (2019). *Cybersecurity Almanac: 100 Facts, Figures, Predictions And Statistics*. URL: https://cybersecurityventures.com/cybersecurity-almanac-2019/ (дата звернення: 01.12.2021).

Motsch, W., David, A., Sivalingam, K., Wagner, A., & Ruskowski, M. (2020). Approach for dynamic price-based demand side management in cyber-physical

production systems. In *Procedia Manufacturing* (Vol. 51, pp. 1748–1754). Elsevier B.V. https://doi.org/10.1016/j.promfg.2020.10.243

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. 9(4). URL: https://doi.org/10.1515/joim-2017-0025

Mulyana Y. Digitalization of the court in the settlement of cases. *International Journal of Latin Notary*, 2021. №1(2). P. 36-42. URL: https://i-latinnotary.notariat.unpas.ac.id/index.php/jurnal/article/view/6

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

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. 96. URL: https://doi.org/10.1016/j.future.2019.02.013

Nuha M., Mahmud S., Sattar A. A case study and fraud rate prediction in e-banking systems using machine learning and data mining. Soft *Computing Techniques and Applications*. 2021. P. 71-83. DOI: https://doi.org/10.1007/978-981-15-7394-1_6.

Numbeo (2023). *Crime Index by Country 2022.* URL: https://www.numbeo.com/crime/rankings_by_country.jsp?title=2022 (дата звернення: 01.05.2023).

Onete C. B., Vargas V. M., Chita S. D. Study on the implications of personal data exposure on the social media platforms. *Transformations in Business and Economics.* 2020. 19(2).

Pazarbasioglu, C.; Mora, A.G.; Uttamchandani, M.; Natarajan, H.; Feyen, E.; Saal, M. Digital Financial Services; World Bank: Washington, DC, USA, 2020.

Perlroth N., Scott M, Frenkel S. (2017). *Cyberattack Hits Ukraine Then Spreads Internationally.* URL: https://www.nytimes.com/2017/06/27/technology/ransomware-hackers.html (дата звернення: 01.05.2023).

Prieto Curiel, R. (2023). Weekly Crime Concentration. *Journal of Quantitative Criminology*, *39*(1), 97–124. https://doi.org/10.1007/s10940-021-09533-6

PwC, (2018). *Building a united front on financial crimes*. URL: https://www.pwc.com/gx/en/financial-services/pdf/united-front-financial-crimes-2018-pwc.pdf (дата звернення: 31.05.2022).

Rousseeuw P.J. Silhouettes: a Graphical Aid to the Interpretation and Validation of Cluster Analysis. *Computational and Applied Mathematics.* 1987, № 20. P. 53–65. DOI: https://doi.org/10.1016/0377-0427(87)90125-7.

Said Kh., Karimi D. K. Impact de la Digitalisation sur la Performance Bancaire dans la Prévention et la Lutte contre le Blanchiment de Capitaux. *African Scientific Journal*, 2022. №3(12). P. 461-476. DOI: 10.5281/zenodo.6874059

Salehi A., Ghazanfari M., Fathian M. Data mining techniques for anti money laundering. *International Journal of Applied Engineering Research*, 2017. №12(20). P. 10084–10094. DOI: 10.5120/ijca2016910953

Savchuk T. O., Pryimak N. V., Slyusarenko N. V., Smolarz A., Smailova S., Amirgaliyev Y. Improved method of searching the associative rules while developing the software. *International Journal of Electronics and Telecommunications*. 2020. 66(3), 425-430. doi:10.24425-ijet.2020.131895/715.

Schneider F. Shadow Economies in 145 Countries All Over the World : What Do We Really Know? Center for Research in Economics, Management and the Arts (CREMA). Working Papers No 2005-13. Basel, 2005. 54 p. URL: http://www.crema-research.ch/papers/2005-13pdf

Schneider, F. (2022). New COVID-related results for estimating the shadow economy in the global economy in 2021 and 2022. *International Economics and Economic Policy*, *19*(2), 299–313. https://doi.org/10.1007/s10368-022-00537-6

Sedano, T. G. (2022). Due diligence and criminal policy models in the fight against contemporary forms of slavery. [Diligencia debida y modelos de política criminal en la lucha contra las formas contemporáneas de esclavitud] *Eunomia.Revista En Cultura De La Legalidad*, (22), 210-229. doi:10.20318/eunomia.2022.6813

Syed, A. A., Ahmed, F., Kamal, M. A., & Trinidad Segovia, J. E. (2021). Assessing the role of digital finance on shadow economy and financial instability: An empirical analysis of selected South Asian countries. *Mathematics*, *9*(23). https://doi.org/10.3390/math9233018

Silalahi, P. (2022). Analysis of the Effect of ICT, Tax and Corruption on Shadow Economy in G20 Countries. *JURNAL EKONOMI DAN KEBIJAKAN PEMBANGUNAN*, *11*(2), 132–145. https://doi.org/10.29244/jekp.11.2.2022.132-145

Singh, S. K., Jeong, Y. S., & Park, J. H. (2020). A deep learning-based IoT-oriented infrastructure for secure smart City. *Sustainable Cities and Society*, *60*. https://doi.org/10.1016/j.scs.2020.102252

Syniavska O., Dekhtyar N., Deyneka O., Zhukova T., Syniavska O. Modeling the process of counteracting fraud in e-banking. Paper presented at *the CEUR Workshop Proceedings*. 2019, vol. 2422. P. 100–110.

Smith E.T. Cyber warfare: a misrepresentation of the true cyber threat. *American Intelligence Journal.* 2013, №31(1). P. 82-85.

The Heritage Foundation (2023). *2023 Index of Economic Freedom*. URL: https://www.heritage.org/index/download (дата звернення: 01.05.2023).

The Mobile Economy 2020. GSM Association URL: https://www.gsma.com/mobileeconomy/wp-content/uploads/2020/03/GSMA_MobileEconomy2020_Global.pdf

The World Bank (2023). *Life expectancy at birth, total (years).* URL: https://data.worldbank.org/indicator/SP.DYN.LE00.IN (дата звернення: 01.05.2023).

Transparency International (2023). *Corruption_Perceptions_Index.* URL: https://www.transparency.org/en/cpi/2021?gclid=CjwKCAjw67ajBhAVEiwA2

g_jEPyd355cvDdhD7SdWVteYeer5WvV3BZFHMo-Ox6p3vXSGk9wKi4p4BoCRJgQAvD_BwE (дата звернення: 01.05.2023).

Tribune (2020). *Major cyber attack by Indian intelligence identified: ISPR*. URL: https://tribune.com.pk/story/2259193/major-cyber-attack-by-indian-intelligence-identified-ispr (дата звернення: 01.05.2023).

Tweneboah-Koduah S., Atsu F., Prasad R. Reaction of stock volatility to data breach: An event study. *Journal of Cyber Security and Mobility*. 2020. 9(3). https://doi.org/10.13052/JCSM2245-1439.931

U.S. Department of Homeland Security (2016). *Joint Statement from the Department Of Homeland Security and Office of the Director of National Intelligence on Election Security*. URL: https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national (дата звернення: 01.05.2023).

Uma, M., & Padmavathi, G. (2013). A survey on various cyber attacks and their classification. *International Journal of Network Security*, *15*(5), 390–396.

Villiers, C. (2022). New directions in the european union's regulatory framework for corporate reporting, due diligence and accountability: The challenge of complexity. *European Journal of Risk Regulation, 13*(4), 548-566. doi:10.1017/err.2022.25

Vinayakumar R., Alazab M., Soman K. P., Poornachandran P., Al-Nemrat A., Venkatraman S. Deep learning approach for intelligent intrusion detection system. *IEEE Access*. 2019, № 7. P. 41525–41550. DOI: https://doi.org/10.1109/ACCESS.2019.2895334.

Vives, X. Digital disruption in banking (2019). Annual Rewiew of Financial Economics. URL: https://blog.iese.edu/xvives/files/2020/01/Digital-Disruption-in-Banking_Nov.2019.pdf

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers and Security*, *38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

Voo J., Hemani I., Cassidy D. (2022). *National Cyber Power Index 2022*. URL: https://www.belfercenter.org/sites/default/files/files/publication/CyberProject_National%20Cyber%20Power%20Index%202022_v3_220922.pdf (дата звернення: 01.05.2023).

Vovk V., Zhezherun Y., Bilovodska O., Babenko V., Biriukova A. Financial Monitoring in the Bank as a Market Instrument in the Conditions of Innovative Development and Digitalization of Economy: Management and Legal Aspects of the Risk-Based Approach. *IJIEPR*, 2020. №31(4). P. 559-570. URL: http://ijiepr.iust.ac.ir/article-1-1141-en.html

Wang R., Liu G. Ensemble Method for Credit Card Fraud Detection. In *Proceedings - 2021 4th International Conference on Intelligent Autonomous Systems, ICoIAS 2021*. 2021. P. 246–252. DOI: https://doi.org/10.1109/ICoIAS53694.2021.00051.

Wisevoter (2023). *Most Powerful Countries in the World.* URL: https://wisevoter.com/country-rankings/most-powerful-countries-in-the-world/ (дата звернення: 01.05.2023).

World Happiness Report (2023). *World Happiness Report 2022.* URL: https://worldhappiness.report/ed/2022/ (дата звернення: 01.05.2023).

World Robotics Report 2020. International Federation of Robotics. URL: https://ifr.org/downloads/press2018/Presentation_WR_2020.pdf

Wronka C. Money laundering through cryptocurrencies – analysis of the phenomenon and appropriate prevention measures. *Journal of Money Laundering Control*, 2022. №25(1). P.79-94. DOI: 10.1108/JMLC-02-2021-0017

X-Force Threat Intelligence Index 2021. *IBM Security*. URL: https://www.ibm.com/downloads/cas/M1X3B7QG

Zhou Y., Song X., Zhou M. Supply Chain Fraud Prediction Based on XGBoost Method. In *2021 IEEE 2nd International Conference on Big Data, Artificial Intelligence and Internet of Things Engineering, ICBAIE 2021*. 2021. P. 539–542. DOI: https://doi.org/10.1109/ICBAIE52039.2021.9389949.

Боженко В.В., Кушнерьов О. С., Кільдей А.Д. Детермінанти поширення кіберзлочинності у сфері фінансових послуг. *Економічний форум*. 2021. № 4. С. 116-121.

Діордіца І. В. Поняття та зміст кіберзлочинності // Глобальна організація союзницького лідерства : сайт. URL: http://goal-int.org/ponyattya-ta-zmist-kiberzlochinnosti

Довгань О. Д., Доронін І. М. Ескалація кіберзагроз національним інтересам України та правові аспекти кіберзахисту: монографія; НАПрН України, НДІІП. Київ : Видавничий дім «АртЕк», 2017. 107 с.

Дюк В., Самойленко А. Data Mining: учебный курс (+CD). СПб: Изд. Питер, 2001. 368 с.

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

Козирєва В.П., Гаврилішин А.П. Кіберправопорушення як загроза економічній безпеці України. Юридичний вісник.2020. № 1 (54). С. 148-155.

Кримінальний кодекс України *Закон* від 05.04.2001 № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text

Кузьменко О.В. Data-Mining для протидії кібершахрайствам та легалізації кримінальних доходів в умовах цифровізації фінансового сектору економіки України. Формалізація та оцінка якісних і кількісних параметрів визначення передумов та детермінантів здійснення злочинної діяльності у фінансовому секторі економіки України : звіт про НДР (проміжний) / кер. О. В. Кузьменко. Суми : СумДУ, 2021. 197 с.

Кузьменко О.В., Яровенко Г.М., Радько В.В. Попередній аналіз процесу конвергенції систем кібербезпеки та фінансового моніторингу країн.

Економіка та суспільство. 2021, № 32. DOI: https://doi.org/10.32782/2524-0072/2021-32-37.

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

Ланде Д. В., Субач І. Ю., Бояринова Ю. Є. Основи теорії і практики інтелектуального аналізу даних у сфері кібербезпеки : навчальний посібник. Київ : КПІ ім. Ігоря Сікорського, 2018. 300 с.

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

Мокін В.Б. Метод проектування когнітивної карти для оптимізації профорієнтаційної діяльності ЗВО / В.Б. Мокін, О.В. Бурдейна, К.О.Коваль, А.Р. Ящолт. Вісник Вінницького політехнічного інституту. 2018. № 3. С. 89-99.

Національний банк України (2021). Карта ризиків фінансового сектору України.URL: https://bank.gov.ua/admin_uploads/article/Risk_map_2021.pdf?v=4

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.

Перелік категорій кіберінцидентів. Державна служба спеціального зв'язку та захисту інформації України. URL: https://www.cip.gov.ua/ua/news/perelik-kategorii-kiberincidentiv

Перелік категорій кіберінцидентів. Державна служба спеціального зв'язку та захисту інформації України. URL: https://www.cip.gov.ua/ua/news/perelik-kategorii-kiberincidentiv

Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

Цивільний кодекс України від 16.01.2003 № 435-IV. URL: https://zakon.rada.gov.ua/laws/show/435-15#Text

Яровенко Г.М. Розробка кіберпрофілів сучасних фінансових кіберзлочинів / Національна безпека через конвергенцію систем фінансового моніторингу та кібербезпеки: інтелектуальне моделювання механізмів регулювання фінансового ринку. Модернізація інструментарію протидії легалізації кримінальних доходів та кібершахрайствам : звіт про НДР (проміжний) / кер. Г. М. Яровенко. Суми : СумДУ, 2022. С. 101-118.

Яровенко Г.М., Колотіліна О.В. Алгоритми розпізнавання поведінки кібершахраїв / Національна безпека через конвергенцію систем фінансового моніторингу та кібербезпеки: інтелектуальне моделювання механізмів регулювання фінансового ринку. Модернізація інструментарію

протидії легалізації кримінальних доходів та кібершахрайствам : звіт про НДР (проміжний) / кер. Г. М. Яровенко. Суми : СумДУ, 2022. С. 119-137.

Яровенко Г.М., Колотіліна О.В., Світлична А.О. Сценарії взаємодії систем кібербезпеки та протидії фінансовим злочинам для країн з різним рівнем економічного розвитку / Національна безпека через конвергенцію систем фінансового моніторингу та кібербезпеки: інтелектуальне моделювання механізмів регулювання фінансового ринку. Обґрунтування концепції конвергенції системи фінансового моніторингу та кібершахрайств : звіт про НДР (проміжний) / кер. Г. М. Яровенко. Суми : СумДУ, 2021. С. 136-152.

Яровенко Г.М., Кузьменко О.В., Лєонов С.В. Побудова фазових портретів «зрілості», «станів рівноваги» та «релаксаційних коливань втрати стійкості» системи протидії фінансовим та кібершахрайствам / Національна безпека через конвергенцію систем фінансового моніторингу та кібербезпеки: інтелектуальне моделювання механізмів регулювання фінансового ринку. Обґрунтування концепції конвергенції системи фінансового моніторингу та кібершахрайств : звіт про НДР (проміжний) / кер. Г. М. Яровенко. Суми : СумДУ, 2021. С. 40-62.

Електронне наукове видання

УДОСКОНАЛЕННЯ СИСТЕМИ ЗАПОБІГАННЯ ТА ПРОТИДІЇ ФІНАНСОВИМ КІБЕРШАХРАЙСТВАМ: ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ТА ПРАКТИЧНІ АСПЕКТИ

Монографія

За загальною редакцією

доктора економічних наук, професора А.О. Бойка,

докторки економічних наук, доцентки Г.М. Яровенко

Художнє оформлення обкладинки В. В. Боженко
Редактори: Н. З. Клочко, С. М. Симоненко
Комп'ютерне верстання В. В. Боженко, Г.М.Яровенко

Формат. Ум. друк. арк.. Обл.-вид. арк..

Видавець і виготовлювач
Сумський державний університет,
вул. Римського-Корсакова, 2, м. Суми, 40007
Свідоцтво суб'єкта видавничої справи ДК № 3062 від 17.12.200