МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Сумський державний університет

Навчально-науковий інститут бізнесу, економіки та менеджменту

Кафедра економічної кібернетики

«До захисту допущено»
Завідувач кафедри
_____ Віталія КОЙБІЧУК
(підпис) (Ім'я та ПРІЗВИЩЕ)
____ _____ 2024 р.

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня магістр

зі спеціальності 051 Економіка ,
(код та назва)
освітньо-професійної програми «Економічна кібернетика»
(освітньо-професійної / освітньо-наукової) (назва програми)
на тему: Вплив діджиталізації на розвиток фінансових злочинів: економічні та безпекові ефекти.

Здобувачки групи ЕК.м-31 ПЕТРЕНКО Каріни Юріївни
(шифр групи) (прізвище, ім'я, по батькові)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.


(підпис)

Каріна ПЕТРЕНКО
(Ім'я та ПРІЗВИЩЕ здобувача)

Керівник професор, д.е.н, Сергій ЛЄОНОВ
(посада, науковий ступінь, вчене звання, Ім'я та ПРІЗВИЩЕ)


(підпис)

Суми – 2024

Ministry of Education and Science of Ukraine

Sumy State University

Educational and Scientific Institute of Business, Economics and Management

Department of Economic Cybernetics

«Admitted to the defense»
Head of Department
_____ Vitaliia Koibichuk
(signature) (First and LAST NAME)
____ _____ 2024 p.

QUALIFICATION WORK

to obtain an educational degree master
(bachelor / master)

from the specialty 051 Economics ,
(code and name)

educational-professional programs «Economic cybernetics»
(educational-professional / educational-scientific) (the name of the program)

on the topic: The impact of digitalization on the development of financial crimes: economic and security effects.

Student of the group EC.m-31 PETRENKO Karina
(group code) (full name)

The qualification work contains the results of own research. The use of ideas, results and texts of other authors are linked to the corresponding source

(signature)

Karina PETRENKO
(Name and SURNAME of the acquirer)

Head professor, PhD Serhiy LYEONOV
(position, academic degree, academic title, Name and SURNAME)

(signature)

Sumy – 2024

Міністерство освіти і науки України
Сумський державний університет
Навчально-науковий інститут бізнесу, економіки та менеджменту
Кафедра економічної кібернетики

ЗАТВЕРДЖУЮ
Завідувач кафедри
к.е.н., доцент
Віталія КОЙБІЧУК
«___» _____ 2024 р.

ЗАВДАННЯ НА КВАЛІФІКАЦІЙНУ МАГІСТЕРСЬКУ РОБОТУ
(спеціальність 051 Економіка «Економічна кібернетика»)

студентці 2 курсу, групи ЕК.м-31

Петренко Каріні Юріївні
(прізвище, ім'я, по батькові студента)

1. Тема роботи Вплив діджиталізації на розвиток фінансових злочинів: економічні та безпекові ефекти затверджена наказом по університету від «14» жовтня 2024 року № 1082-VI.
2. Термін подання студентом закінченої роботи «04» грудня 2024 року.
3. Мета кваліфікаційної роботи: вивчення теоретичних аспектів поняття фінансових злочинів та цифровізації, ідентифікація функціональної взаємодії між фінансовими злочинами та діджиталізацією.
4. Об'єкт дослідження фінансові злочини, та вплив цифрового розвитку країни на їх виникнення.
5. Предмет дослідження: науково-методичні засади взаємодії цифрового розвитку та виникнення, розвитку та протидії фінансовим злочинів.
6. Кваліфікаційна робота виконується на матеріалах баз даних Міжнародного валютного фонду, Базельського інституту управління, Європейської комісії.
7. Орієнтовний план кваліфікаційної роботи, терміни подання розділів керівникові та зміст завдань для виконання поставленої мети

Розділ 1 Теоретичні та методичні аспекти фінансових злочинів та цифровізації- 23 жовтня 2024 року
(назва – термін подання)

У розділі 1: дослідження поняття фінансових злочинів, діджиталізації та їх роль в економічному середовищі; бібліометричний аналіз наукових досліджень у сфері фінансових шахрайств та цифрового розвитку; формулювання гіпотез на основі проведеного аналізу.
(зміст конкретних завдань до розділу, які повинен виконати студент)

Розділ 2 Побудова математичної моделі взаємодії між фінансовими злочинами та діджиталізацією - 15 листопада 2024 року
(назва – термін подання)

У розділі 2: вибір та опис вхідних даних; розробка математичної моделі та опис методів дослідження
(зміст конкретних завдань до розділу, які має виконати студент)

Розділ 3 Інтерпретація отриманих результатів - 04 грудня 2024 року
(назва – термін подання)

У розділі 3: інтерпретація результатів з урахуванням особливостей економік країн; розробка рекомендацій щодо протидії виникнення фінансової злочинності.
(зміст конкретних завдань до розділу, які має виконати студент)

8. Консультації з роботи:

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
1	Лєонов С.В., професор	18.10.2024	18.10.2024
2	Лєонов С.В., професор	28.10.2024	28.10.2024
3	Лєонов С.В., професор	18.11.2024	18.11.2024

9. Дата видачі завдання: «18» жовтня 2024 року

Керівник кваліфікаційної роботи (підпис) С.В. Лєонов (ініціали, прізвище)

Завдання до виконання одержав (підпис) К.Ю. Петренко (ініціали, прізвище)

АНОТАЦІЯ

Дослідження фінансових злочинів та їх взаємодії з процесами діджиталізації є актуальним питанням, враховуючи масштаби фінансових правопорушень та швидкий розвиток технологій. Розуміння впливу діджиталізації на фінансові злочини є важливим для розробки ефективних стратегій протидії, впровадження інноваційних технологічних рішень та адаптації регуляторних і правових рамок до нових викликів.

Метою цього дослідження є вивчення теоретичних аспектів поняття фінансових злочинів та ідентифікація функціональної взаємодії між діджиталізацією та фінансовими злочинами.

Об'єктом дослідження є фінансові злочини в умовах дуального впливу діджиталізації на рівні країни.

Предметом дослідження є взаємодія між діджиталізацією та фінансовими злочинами, а саме вплив цифрових технологій на виникнення, розвиток та протидію фінансовим злочинам, з акцентом на економічні та безпекові аспекти цього процесу.

У процесі дослідження вирішено наступні завдання: досліджено поняття фінансових злочинів та діджиталізації та їх роль в економічному середовищі; проведено бібліометричний аналіз наукових досліджень у сфері діджиталізації та фінансових злочинів; сформульовано гіпотези на основі проведеного аналізу; обрано та описано вхідні дані; проведено кластерний аналіз, розроблено математичні моделі та описано методи дослідження; розроблено рекомендації щодо протидії фінансовим злочинам.

Методи дослідження включають аналіз публікацій та наявних баз даних, синтез, бібліометричний аналіз, кластерний аналіз, кореляційний аналіз, лінійну та робастну регресії.

Інформаційною базою дослідження є бази даних Міжнародного валютного фонду, Базельського інституту управління, Європейської комісії, публікації іноземних та українських науковців, документація мови програмування Python та статистичне програмне забезпечення Stata SE.

Наукова новизна отриманих результатів полягає у кластеризації економік країн на основі показників, що є ключовими факторами цифрового розвитку та ризиків виникнення фінансової злочинності. Це дозволило ідентифікувати взаємозв'язок між фінансовими правопорушеннями та діджиталізацією на рівні 134 країн світ, що відрізняється від існуючих досліджень більш глибоким розумінням взаємодії цих процесів.

Зміст кваліфікаційної магістерської роботи викладено на 63 сторінках. Список використаних джерел із 45 найменувань, розміщений на 49-53 сторінках. Робота містить 4 таблиці, 20 рисунків, додатки А, В.

Рік виконання кваліфікаційної роботи – 2024 рік.

Рік захисту роботи – 2024 рік.

SUMMARY

Masters's level qualification work

The impact of digitalization on the development of financial crimes: economic and security effects

Karina Petrenko

The master's thesis "The impact of digitalization on the development of financial crimes: economic and security effects" examines the relationship between digitalization and financial crimes, highlighting how digital technologies can both facilitate new forms of financial offences and provide effective prevention tools. The primary objective is to understand the dual impact of digitalization on financial crimes to develop comprehensive strategies that address the challenges related to economic growth and security in today's world.

The study aims to explore the theoretical aspects of financial crimes and their relationship with digitalization. It seeks to identify how these two factors interact and analyze how digitalization influences the proliferation of financial crimes through empirical data. Investigating this relationship is crucial because financial offences pose significant economic and security challenges, particularly in light of the rapid advancement of digital technologies. A thorough understanding of this connection will help develop effective countermeasures and adapt regulatory frameworks to address emerging threats.

Digitalization has significantly changed the landscape of financial crimes by introducing new methods and opportunities for criminals. Several key factors connect digitalization to financial crimes. The rise of digital technologies has led to the growth of cybercrimes, online fraud, and money laundering through cryptocurrencies. Criminals take advantage of digital platforms for their anonymity, speed, and global accessibility, which makes detection and prevention increasingly challenging. Advanced technologies such as cryptocurrencies, blockchain, and encrypted communications are utilized by criminals to carry out illegal activities. Moreover, the instantaneous nature of digital transactions complicates the monitoring and interception of illegal financial flows. Additionally, the

global reach of digital platforms facilitates cross-border crimes, which further complicates jurisdictional enforcement and legal proceedings.

Traditional financial crimes, such as fraud, money laundering, and embezzlement, have adapted to the digital environment. Fraud has evolved into online scams, phishing attacks, and identity theft conducted via the internet. Money laundering now often involves cryptocurrencies and digital transfers to obscure money trails and avoid detection. Embezzlement has also taken on a new form, using digital manipulation of financial accounts and transactions, which allows perpetrators to conceal their activities more effectively. The scale and complexity of these crimes have increased due to digitalization, making them harder to detect and prevent using traditional methods.

The research employs international indices such as the Basel AML Index, which evaluates risks related to money laundering and terrorist financing, and the AI Preparedness Index, which measures a country's readiness for implementing artificial intelligence. Statistical tools like cluster analysis and regression modelling are utilized, using Stata SE18 and the Python programming language. To address multicollinearity among variables, the study selects the AI Preparedness Index as the primary indicator of digitalization and conducts separate regression models for its components. The validity of the findings is ensured through robust regression techniques and logarithmic transformation to meet the assumptions required for regression analysis. This methodology guarantees reliable and valid results by carefully selecting variables, addressing statistical issues, and using reputable data sources.

The study reveals an inverse relationship between digitalization and the risks of financial crime. Higher levels of digitalization, as measured by the AI Preparedness Index, are linked to lower financial crime risks, which are assessed through the Basel AML Index. Among the various components of the AI Preparedness Index, the Regulation and Ethics aspect has the most significant impact on reducing financial crime risks. This highlights the importance of effective regulatory frameworks and ethical standards.

Additionally, the role of human capital and innovation is critical; countries that excel in these areas tend to experience lower financial crime risks. The research concludes that digitalization has a dual effect on financial crime—it can either mitigate or exacerbate

risks, depending on the robustness of regulatory mechanisms and ethical standards in place. Therefore, effective regulation and ethical practices are essential to ensure that digitalization positively contributes to the fight against financial crimes.

Law enforcement and regulatory bodies face several challenges in combating digital financial crimes. Rapid technological advancements often outpace regulatory updates, making it difficult for legal frameworks to keep up with emerging types of digital financial crimes. The global nature of these crimes adds complexity, as cross-border jurisdictional issues require international cooperation and coordination. Resource constraints limit authorities' ability to implement the advanced detection systems and technologies necessary to address sophisticated crimes effectively. Moreover, existing legal frameworks may not fully capture the complexities of new digital financial crimes, resulting in gaps in regulation and enforcement capabilities.

The thesis highlights the potential of technology in effectively combating financial crimes. Artificial intelligence and machine learning algorithms can analyze vast amounts of data to identify anomalies and predict fraudulent activities in real time. Additionally, blockchain technology improves transparency and traceability in financial transactions, making it more difficult for criminals to conceal illicit activities. Enhanced digital infrastructure allows for better monitoring and enforcement, enabling authorities to respond more swiftly to emerging threats. By adopting advanced technologies, financial institutions and regulatory bodies can strengthen their capacity to prevent, detect, and address financial crimes. For financial institutions and businesses, the rise of digital financial crimes requires significant changes in operations and strategies. Risk management now demands substantial investments in cybersecurity to protect against sophisticated threats. Compliance has become increasingly important, as organizations must adhere to evolving regulations to avoid legal penalties and reputational damage. Maintaining robust security measures builds customer trust and confidence, which is vital for long-term business sustainability.

International cooperation is essential for addressing the global nature of digital financial crimes. Effective collaboration among nations is necessary to tackle cross-border crimes, as criminals often operate across multiple jurisdictions. Standardizing regulations

and legal frameworks can significantly enhance the effectiveness of combating financial crimes on a global scale. International agreements and frameworks promote information sharing, enabling countries to exchange data, intelligence, and best practices. This cooperation strengthens collective capabilities to detect, prevent, and prosecute financial crimes that cross national boundaries.

The thesis outlines several policy recommendations aimed at reducing the impact of digitalization on financial crimes. First, it is essential to strengthen regulatory frameworks by updating laws and regulations to specifically address digital financial crimes and emerging technologies. Additionally, promoting high ethical standards within organizations fosters responsible practices, which can help deter illicit activities.

Investing in the development of human capital is crucial for building a workforce that is skilled in financial crime prevention and cybersecurity. Furthermore, it is important to balance innovation with oversight, supporting technological advancements while ensuring that appropriate regulatory mechanisms are in place to prevent misuse.

Policymakers should proactively adapt regulations to keep pace with technological changes, striving to create an environment where digitalization benefits society without increasing the risks of financial crime.

The study indicates that emerging technologies will continue to pose both challenges and opportunities in the realm of financial crimes. The dual impact of digitalization on these crimes is expected to persist, making it crucial for policymakers, regulatory bodies, and financial institutions to remain vigilant. Strong institutions with effective governance and regulatory practices will be essential in managing the risks associated with digital financial crimes. Ongoing research and monitoring are necessary to fully grasp the evolving landscape and to develop proactive strategies that address future threats.

This study enhances the current body of knowledge by providing a thorough analysis of how digitalization influences financial crimes, highlighting its dual impact and the importance of regulation and ethics. It offers practical implications for policymakers, financial institutions, businesses, and other stakeholders in crafting effective strategies to combat financial crimes in the digital age. By underscoring the critical factors that

influence the relationship between digitalization and financial crimes, this thesis directs efforts to harness the benefits of digital technologies while mitigating the associated risks.

The study recognizes several limitations that may affect how its findings are interpreted. Relying on specific indices to represent complex concepts like digitalization and financial crime risks may not capture all dimensions of these issues comprehensively. Furthermore, external factors such as cultural and geopolitical variables, which were not addressed in the study, could also influence the relationship between digitalization and financial crimes in various countries. These limitations indicate that caution should be taken when attempting to generalize the findings and emphasize the need for further research to deepen our understanding.

Digitalization has a dual impact on financial crimes: it can facilitate new criminal activities while also providing tools for effective prevention and detection. The effectiveness of regulatory mechanisms and ethical standards is crucial in determining whether digitalization will heighten or reduce the risks of financial crime. Policymakers, financial institutions, and other stakeholders must recognize this duality and work together to maximize the benefits of digitalization while minimizing its associated risks. By strengthening regulations, promoting ethical practices, investing in human capital, and responsibly leveraging technology, we can safeguard the integrity of the global financial system and enhance economic security in the digital age.

Keywords: digitalization, financial crimes, financial fraud, economy, cluster analysis, regression, technological impact.

The content of the master's qualification thesis is presented on 63 pages. The list of references, consisting of 45 titles, is located on pages 49–53. The work contains 4 tables, 20 figures, and Appendices A and B.

Year of completion of the qualification work: 2024.

Year of defense of the work: 2024.

ЗМІСТ

ВСТУП

Враховуючи масштаби фінансових злочинів та швидкий розвиток технологій, дослідження фінансових злочинів та їх взаємозв'язку з цифровим розвитком є важливою темою. У 2023 році через глобальну фінансову систему пройшло близько 3,1 трильйона доларів США незаконних коштів (NASDAQ, 2023). Відмивання грошей складає значну частину цих сум, включаючи 346,7 мільярда доларів США в торгівлі людьми та 782,9 мільярда доларів США в незаконному обігу наркотиків, а також 11,5 мільярда доларів США в фінансуванні тероризму. Дослідження фінансових злочинів та їх взаємодії з процесами цифровізації є актуальним питанням з огляду на економічні та безпекові виклики, які постають перед сучасним світом. Діджиталізація, з одного боку, створює нові можливості для зміцнення кібербезпеки та протидії злочинам, але з іншого боку, злочинці також отримують доступ до нових інструментів здійснення незаконних операцій (KPMG, 2024).

Тому, розуміння впливу діджиталізації на тенденції фінансових злочинів є важливим для розробки ефективних стратегій протидії, впровадження інноваційних технологічних рішень та адаптації регуляторних та правових рамок до нових викликів.

Метою цього дослідження є вивчення теоретичних аспектів поняття фінансових злочинів та ідентифікація функціональної взаємодії між діджиталізацією та фінансовими злочинами.

Об'єктом дослідження є фінансові злочини в умовах дуального впливу цифровозації на рівні країни.

Предметом дослідження є взаємодія між діджиталізацією та фінансовими злочинами, а саме вплив цифрових технологій на виникнення, розвиток та протидію фінансовим злочинам.

Проведення дослідження вимагає виконання наступних завдань:

- дослідження понять фінансових злочинів, діджиталізації та їх роль в економічному середовищі;
- бібліометричний аналіз наукових досліджень у сфері цифровізації та фінансових злочинів;

- формулювання гіпотез на основі проведеного аналізу;
- вибір та опис вхідних даних;
- розробка математичної моделі та опис методів дослідження;
- розробка рекомендацій щодо протидії фінансовим злочинам.

Методи дослідження: аналіз публікацій та наявних баз даних, синтез, бібліометричний аналіз, кластерний аналіз, кореляційний аналіз, лінійна регресія, робастна регресія.

Інформаційною базою для дослідження є бази даних Міжнародного валютного фонду, Базельського інституту управління, Європейської комісії, а також публікації іноземних та українських науковців, документація мови програмування Python, статистичне програмне забезпечення Stata SE.

Наукова новизна отриманих результатів полягає у кластеризації економік країн на основі показників, що є ключовими факторами цифрового розвитку країн та ризиків виникнення фінансової злочинності, що відрізняється від існуючих досліджень тим, що дозволяє ідентифікувати взаємозв'язок між фінансовими правопорушеннями та цифровізацією на рівні країн.

Наукова робота виконана в межах науково-дослідної теми «Національна безпека України через запобігання фінансовим шахрайствам та легалізації брудних грошей: воєнні та післявоєнні виклики» (№ д/р 0123U101945), що фінансується Державним бюджетом України. За результатами роботи подано та прийнято до публікації статтю "Економічні злочини під час війни: бібліометричний аналіз" у «Modeling the development of the economic systems» (2024 р., № 4) та подано до друку статтю "The impact of digitalization on the development of financial crimes: economic and security effects" до наукового журналу «Фінансово-кредитна діяльність: проблеми теорії та практики (Scopus/WoS)».

РОЗДІЛ 1. ТЕОРЕТИЧНІ ЗАСАДИ ВПЛИВУ ДІДЖИТАЛІЗАЦІЇ НА ФІНАНСОВІ ЗЛОЧИНИ

1.1 Сутність фінансових злочинів в умовах діджиталізації

Фінансові злочини — це незаконні дії або бездіяльність, що здійснюються індивідами або групами з метою отримання неправомірної фінансової вигоди чи привілеїв шляхом обману, зловживання довірою, порушення законів чи регуляторних норм. Термін "фінансові злочини" охоплює широкий спектр протиправних дій у фінансовій сфері. Вони негативно впливають на економіку, суспільство, безпеку держави, та характеризуються використанням різних схем, маніпуляцій та порушеннями, які призводять до фінансових втрат для окремих осіб, організацій або уряду. Міжнародна група з протидії відмиванню брудних грошей (Financial Action Task Force on Money Laundering, FATF) визначає фінансові злочини як такі, що включають відмивання грошей, фінансування тероризму, корупцію, шахрайство, податкові злочини та інші види незаконної діяльності, які використовують фінансову систему для легалізації незаконних доходів або фінансування незаконних дій [5]. За оцінками, щорічно у світі через відмивання грошей – одного з видів фінансових злочинів – проходить сума, яка становить від 2 до 5% глобального ВВП, що еквівалентно від 800 мільярдів до 2 трильйонів доларів США у поточних цінах. Однак через прихований характер відмивання грошей складно точно визначити загальний обсяг коштів, що проходять через цей процес [1].

Згідно з визначенням, наданим Управлінням з фінансового регулювання і нагляду Великобританії (Financial Conduct Authority, FCA), фінансові злочини охоплюють будь-які види кримінальної діяльності, пов'язані з грошовими коштами, фінансовими послугами або фінансовими ринками. Це включає правопорушення, які стосуються: шахрайства або нечесності, неналежної поведінки на фінансовому ринку або неправомірного використання інформації пов'язаної з фінансовим ринком, обігу доходів, отриманих злочинним шляхом, і фінансування тероризму [2].

Європол інтегрує поняття економічних та фінансових злочинів, визначаючи їх як незаконні дії, вчинені індивідом або групою осіб з метою отримання фінансової або професійної переваги. Основним мотивом у таких злочинах є економічний прибуток [3]. Організація економічного співробітництва та розвитку (Organisation for Economic Cooperation and Development, OECD) додатково наголошує про фінансові злочини у вигляді ухилення від сплати податків та корупції [4].

Міжнародний валютний фонд (International Monetary Fund, IMF) наголошує, що фінансові злочини мають глибокий вплив на життя людей та їх засоби до існування, особливо найбільш вразливих верств населення, і що наслідки від фінансових злочинів є значними та продовжують зростати. МВФ виділяє два типи витрат внаслідок незаконних фінансових дій: прямі витрати та непрямі витрати. Прямі витрати можуть включати зменшення доходів, збільшення витрат, санкції, підвищення фінансової нестабільності. Непрямі витрати мають значно більший масштаб впливу, оскільки охоплюють всю економіку. Внаслідок їх дії можуть підживлюватися цикли економічного буму та спаду, а ціни на житло стають недоступними для нижчих верств населення. Крім того, відмивання грошей може збільшувати волатильність міжнародних потоків капіталу, підривати ефективність державного управління, провокувати політичну нестабільність та загалом зменшувати довіру до уряду та інституцій [6].

Водночас слід зазначити, що фінансові злочини поширені у різних галузях, та впливають на всі сектори економіки та категорії суспільства. Згідно з даними, представленими на діаграмі (рис. 1.1), протягом 2022–2023 років найбільша кількість інцидентів кіберзлочинності була зареєстрована у сфері державного управління. Дана статистика може вказувати на наявність недоліків у системах кібербезпеки державних установ, а також на підвищений інтерес кіберзлочинців до інформації та ресурсів, якими володіють державні органи.

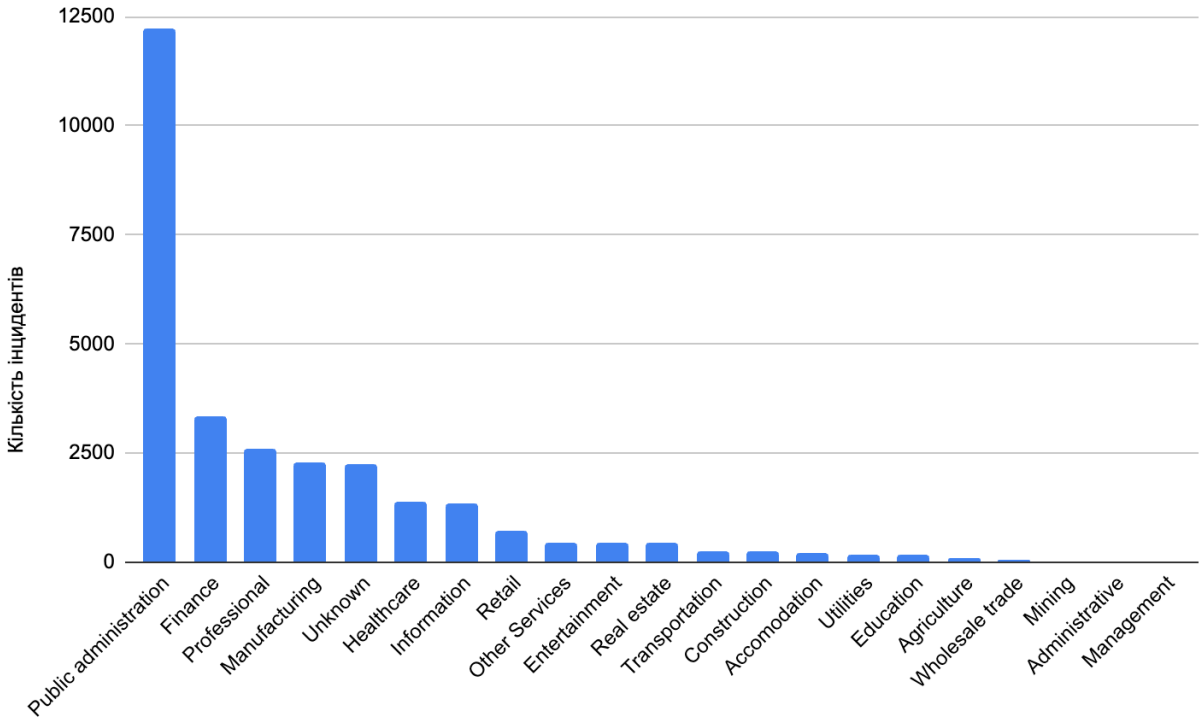

Рисунок 1.1 – Глобальна кількість інцидентів кіберзлочинності з листопада 2022 року по жовтень 2023 року за галузями.

Джерело: розроблено авторкою на основі [18]

Існує широкий різновид фінансових злочинів, проте немає єдиної узгодженої класифікації. Готшалк (2010) у своїй роботі визначив чотири основні категорії фінансових злочинів: корупція (corruption), шахрайство (fraud), крадіжки (theft), маніпуляція (manipulation) [7]. При цьому автор відніс кіберзлочини та відмивання грошей до категорії маніпуляцій. Однак слід зауважити, що кіберзлочини можуть охоплювати як правопорушення проти інформаційно-комунікаційних технологій (ІКТ), так і злочини, у яких ІКТ виступають інструментом для їх здійснення. Ахім та ін. (2021) досліджують фінансові та економічні злочини, використовуючи проксі-показники, які охоплюють лише корупцію, тіньову економіку, відмивання грошей та кіберзлочинність [8].

Схема, представлена на рисунку 1.2, відображає розроблену авторкою класифікацію фінансових злочинів.

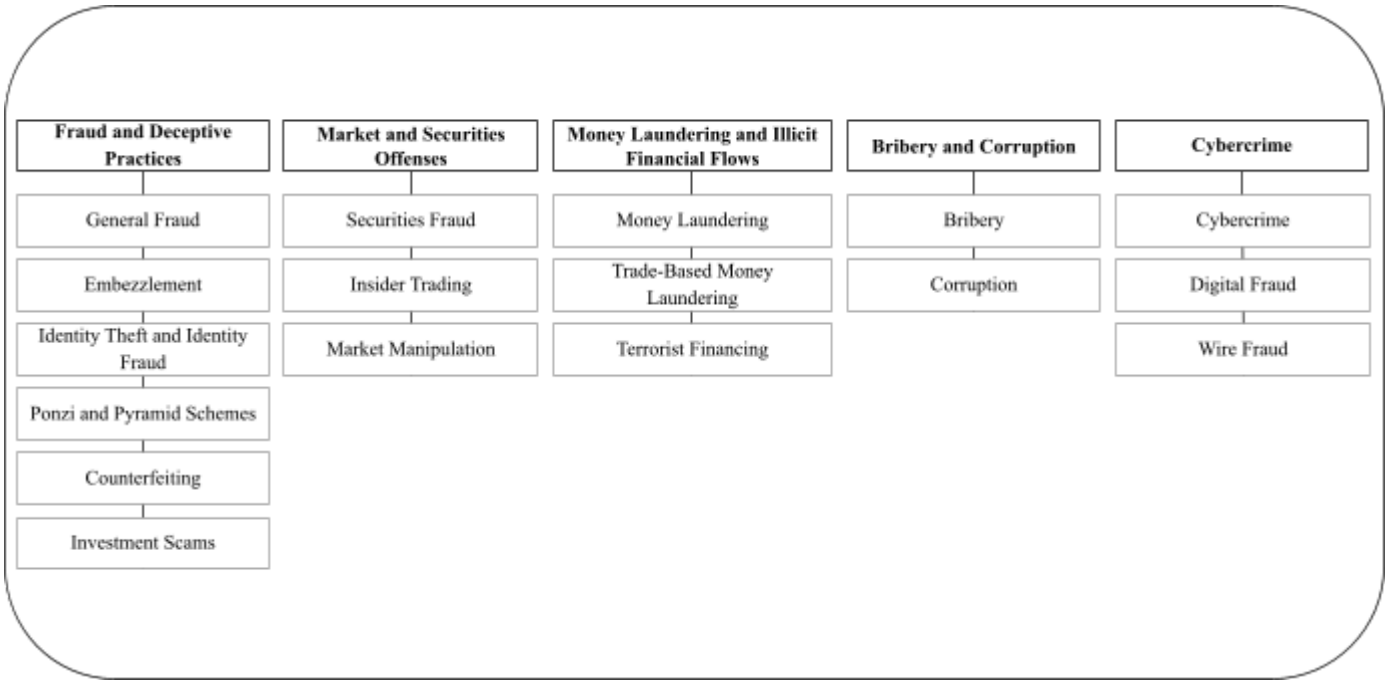

Рисунок 1.2 – Класифікація фінансових злочинів.

Джерело: розроблено авторкою на основі аналізу літературних джерел.

Категорія шахрайства та обманних практик охоплює злочини, пов'язані з умисним введенням в оману або порушенням довіри з метою отримання фінансової вигоди. Ці правопорушення включають використання фальшивих заяв або зловживання довірою жертв з метою незаконного отримання грошей, майна чи послуг:

- Звичайне шахрайство – навмисний обман для отримання неправомірної вигоди. Прикладами такого правопорушення є страхове шахрайство та шахрайство з іпотекою.
- Привласнення коштів – неправомірне присвоєння або використання коштів, які були довірені особі для управління чи контролю.
- Крадіжка особистості та особистих даних – несанкціоноване використання особистої інформації іншої особи для фінансової вигоди.
- Пірамідальні схеми та схеми Понці – інвестиційні шахрайства, що покладаються на нові інвестиції для виплат попереднім інвесторам, створюючи ілюзію прибутковості та стійкості інвестиції.

- Підробки – несанкціоноване відтворення валюти чи товарів з метою обману та отримання неправомірної вигоди.

Категорія правопорушень на фінансових ринках охоплює всі види злочинної діяльності, що здійснюється у сфері фінансових ринків та спрямована на підрив цілісності ринкових механізмів. До цієї категорії відносяться:

- Шахрайство з цінними паперами – умисний обман, пов'язаний з операціями з цінними паперами, включаючи фальсифікацію фінансової звітності та введення інвесторів в оману.
- Інсайдерська торгівля – здійснення торговельних операцій на основі непублічної, цінної інформації, що надає неправомірну перевагу перед іншими учасниками ринку.
- Маніпуляції ринком – дії, спрямовані на навмисне спотворення функціонування вільних та чесних ринків для особистої вигоди, наприклад, використання схем "накачки та скидання" (pump and dump schemes).

Наступна категорія фінансових злочинів – відмивання грошей та незаконні фінансові потоки. Ця категорія охоплює правопорушення, пов'язані з переміщенням та трансформацією нелегальних коштів з метою приховування їхнього незаконного походження або фінансування протизаконної діяльності. До цієї категорії належать:

- Відмивання грошей – процес приховування джерел походження коштів, отриманих від кримінальної діяльності, шляхом інтеграції їх у легальну фінансову систему.
- Торговельно орієнтоване відмивання грошей – використання торговельних операцій та транзакцій для переміщення та присвоєння нелегальних коштів. Це може включати маніпуляції з цінами, кількістю, якістю товарів і послуг у міжнародній торгівлі з метою приховування незаконних фінансових потоків.
- Фінансування тероризму – надання або збирання фінансових ресурсів для підтримки терористичних організацій чи здійснення терористичних актів. Ця діяльність часто пов'язана з методами відмивання грошей через приховані джерела та призначення коштів.

Категорія хабарництво та корупція охоплює злочини, пов'язані із зловживанням владою з метою отримання особистої вигоди. Ці правопорушення зазвичай реалізуються шляхом надання, отримання або вимагання неправомірних переваг з метою впливу на рішення чи дії.

Кіберзлочини представлені як окрема категорія фінансових злочинів. Ця категорія охоплює правопорушення, які здійснюються з використанням інформаційно-комунікаційних технологій та спрямовані на електронні системи, дані або фінансові активи з метою отримання неправомірної вигоди, включаючи хакерство, фішинг та інші форми кібер обману. За даними Федерального бюро розслідувань (ФБР), у 2023 році в Сполучених Штатах найбільших фінансових втрат від кіберзлочинів зазнали жертви в сфері інвестицій (рис. 1.3). Інвестиційне шахрайство є оманливою практикою, яка спонукає інвесторів здійснювати покупки або вкладення на основі неправдивої інформації. Такі шахрайські схеми зазвичай обіцяють потенційним жертвам високі прибутки з мінімальним ризиком.

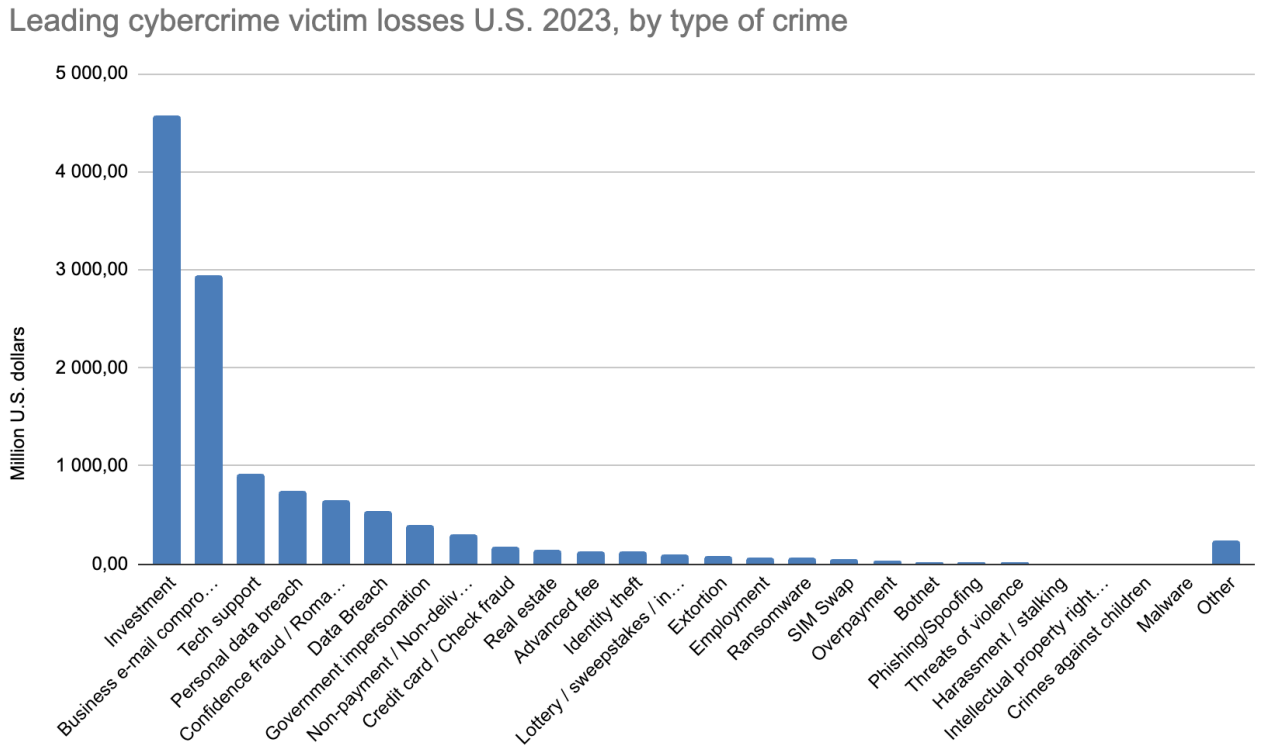

Рисунок 1.3 – Типи кіберзлочинів з найбільшими фінансовими втратами в США у 2023 році, втрати жертв (у млн доларів США)

Джерело: розроблено авторкою на основі [19]

Кіберзлочини набувають особливої актуальності в сучасному цифровому суспільстві, оскільки використання інформаційно-комунікаційних технологій суттєво розширює можливості злочинців у сфері фінансових правопорушень. Це включає в себе здійснення правопорушень з інших категорій із застосуванням цифрових технологій, що посилює складність і масштаб кіберзагроз у економіці.

Процеси відмивання грошей є тісно пов'язаними з іншими видами злочинної діяльності, такими як незаконний обіг наркотиків, шахрайство, контрабанда, підробка, торгівля людьми та ухилення від сплати податків [15, 33, 34]. Отримані доходи від цих кримінальних дій потребують легалізації, що спонукає до використання різноманітних методів відмивання грошей. Корупція часто виступає каталізатором для інших фінансових злочинів: посадові особи можуть приймати хабарі за сприяння в ухиленні від сплати податків, приховуванні фактів шахрайства або непритягненні до відповідальності за відмивання грошей. Хабарництво може забезпечити злочинцям доступ до конфіденційної інформації, яка використовується для інсайдерської торгівлі або маніпулювання ринком. Незаконна експлуатація природних ресурсів, така як нелегальна вирубка лісів або видобуток корисних копалин, генерує значні доходи, що також “відмиваються” [17]. За даними Інтерполу, вартість чорного ринку незаконної торгівлі об'єктами дикої природи досягає до 20 мільярдів доларів США на рік. Внаслідок цього, браконьєрство та нелегальна торгівля дикими тваринами стали однією з основних сфер діяльності організованих злочинних угруповань [16]. Ці злочини також часто пов'язані з корупцією, оскільки злочинці підкуповують офіційних осіб для отримання дозволів або уникнення санкцій.

Підсумовуючи, фінансові злочини можна класифікувати за різними категоріями, кожна з яких має свої унікальні особливості та виклики. Незважаючи на

це, фінансові злочини часто не є ізольованими явищами; вони тісно пов'язані між собою, утворюючи складні мережі незаконної діяльності.

1.2 Діджиталізація як інструмент протидії фінансовим злочинам

Діджиталізація є невід'ємною складовою сучасного розвитку, яка визначає напрям еволюції суспільства та економіки. Вона відкриває нові можливості для інновацій, але також ставить перед суспільством виклики, пов'язані з безпекою даних, цифровою нерівністю та необхідністю адаптації до технологічних змін.

У багатьох наукових публікаціях діджиталізація визначається як інтенсивне впровадження інформаційно-комунікаційних технологій (ІКТ) в економічні процеси, що охоплює широкий спектр цифрових технологій, концепцій і тенденцій, таких як штучний інтелект, Інтернет речей (Internet of Things, IoT) та Четверта промислова революція [9, 10, 11]. Діджиталізація передбачає трансформацію соціально-технічних структур, які раніше були опосередковані не цифровими артефактами, у структури, опосередковані цифровими артефактами [9, 12, 13]. Цанетакіс (2023) цитуючи Джейкоб і Тіля (2017), зазначає, що спочатку діджиталізація означала процес перетворення аналогової інформації в цифрову, що передбачає можливість електронної обробки цих даних [14].

Існує широкий спектр показників та індексів, призначених для відображення рівня діджиталізації. Проте варто зазначити, що деякі з цих інструментів оцінюють рівень діджиталізації країни лише на основі кількості користувачів онлайн-сервісів або ступеня інтернет-покриття. Цанетакіс (2023) наголошує, що діджиталізація охоплює більше, ніж Інтернет. У загальному сенсі, вона стосується процесів зберігання та обробки даних. Діджиталізація є процесом, що формується під впливом соціальних та політичних факторів, де технології виступають засобом, а не самостійною причиною змін. Однак, хоча цифрові технології є важливими інструментами, вони не виступають основним драйвером змін у суспільстві. Вплив технологій і напрямок їх розвитку залежать від того, як суспільство вирішує їх використовувати, регулювати та інтегрувати в різні сфери життя. Це включає

суспільні обговорення ідеї та значення технологій у суспільстві; колективні оцінки – суспільне сприйняття та ставлення до нововведень; та політичні підходи до регулювання – як уряди та інституції вибудовують політики щодо впровадження та контролю технологій [14].

Діджиталізація спричинила значні зміни в бізнес-моделях, фінансових послугах, ринкових структурах та взаємодії між економічними суб'єктами. Впровадження цифрових технологій дозволило підприємствам розвивати нові бізнес-моделі, зосереджені на використанні інноваційних рішень. Завдяки діджиталізації стали можливими такі явища, як електронна комерція, платформи спільної економіки та дистанційні послуги. Компанії активно використовують великі дані, штучний інтелект та машинне навчання для оптимізації виробничих процесів, прогнозування споживчого попиту та підвищення конкурентоспроможності. Фінансовий сектор зазнав значних змін під впливом діджиталізації. З'явилися фінансові технології, які пропонують інноваційні продукти та послуги, зокрема мобільні платежі, електронні гаманці, криптовалюти та блокчейн-технології. Це сприяло підвищенню доступності фінансових послуг для населення, особливо в регіонах з недостатньо розвинутою фінансовою інфраструктурою.

Цифрові технології сприяли подальшій глобалізації економіки, дозволяючи компаніям виходити на міжнародні ринки без значних інвестицій у фізичну інфраструктуру. Завдяки інтернет-комунікації, електронній комерції та цифровим платформам бізнеси отримали можливість оперативно встановлювати присутність у різних країнах, адаптуючись до місцевих ринків та залучаючи глобальну аудиторію.

Однак, поряд із позитивними змінами, глобалізація має і зворотний бік. Багато досліджень визначають глобалізацію як один із ключових чинників, що впливають на відмивання грошей [35]. Глобалізація створює додаткові складнощі для контролюючих органів, оскільки фінансові потоки можуть проходити через декілька юрисдикцій з різними рівнями регуляторного контролю та нагляду. Розширення міжнародних економічних зв'язків сприяє стрімкому розвитку новітніх схем відмивання грошей, надаючи злочинцям можливість оперативного та транскордонного переміщення капіталу. Зокрема, використання криптовалют, таких

як біткоїн, забезпечує підвищену анонімність та швидкість транзакцій, що збільшує ймовірність уникнення виявлення правоохоронними органами [36]. Цифрові валюти працюють на децентралізованих платформах, які не мають централізованого регулятора, що створює труднощі для моніторингу та контролю фінансових операцій. Наприклад, криптовалюти на кшталт Monero пропонують розширені можливості для збереження анонімності завдяки додатковим функціям, таким як використання прихованих адрес [37, 38]. Псевдо анонімність транзакцій та відсутність єдиного підходу до регулювання в різних країнах сприяють використанню криптовалют у фінансових злочинах, зокрема для відмивання грошей [37, 43].

Незважаючи на вище зазначені ризики, діджиталізація є потужним інструментом у боротьбі з фінансовими злочинами. Штучний інтелект (ШІ) займає ключову позицію у протидії фінансовим злочинам, особливо в галузі виявлення шахрайства [32, 42, 45]. Згідно з даними компанії PwC [29], ШІ надає значні можливості для підвищення ефективності протидії фінансовим злочинам у різних аспектах діяльності фінансових установ. Одним із ключових напрямів є виявлення аномалій, де ШІ застосовується для ідентифікації патернів у транзакційних даних, виявлення підозрілої поведінки, що може свідчити про фінансові зловживання. У сфері оцінки ризиків ШІ може аналізувати моделі та комбінації факторів, які є потенційними індикаторами високого рівня ризику, що дозволяє більш точно та оперативно виявляти потенційно небезпечних контрагентів. У процесах пошуку та класифікації суб’єктів ШІ автоматизує пошук і категоризацію осіб, організацій або інших сутностей, залучених у фінансові транзакції, що підвищує точність та швидкість обробки даних. Наприклад, банк HSBC з допомогою ШІ щомісяця перевіряє близько 1,35 мільярда транзакцій на предмет ознак фінансових злочинів, обслуговуючи понад 40 мільйонів клієнтів [28]. Моніторингові системи на базі ШІ не обмежуються простим попередженням про підозрілу активність; вони також ефективно обробляють ці сповіщення, інтегруючи дані з інших санкційних списків, профілів "Знай свого клієнта" та процедур безпеки, формуючи повний профіль користувача [26, 27].

Таким чином, цифровізація процесів фінансової сфери за допомогою штучного інтелекту, є яскравим прикладом використання цифрових технологій для ефективної боротьби з фінансовими злочинами, підвищенню рівня безпеки та відповідності нормативним вимогам.

1.3 Огляд патентних даних щодо реєстрації технологій виявлення та запобігання фінансових шахрайств

Для перевірки актуальності теми було здійснено пошук патентів технологій для виявлення та запобігання фінансових шахрайств. Набір даних містить 4553 патенти, 49,7% (2266 патенти) з яких було опубліковано протягом 2023-2024 років. Дана динаміка відображає збільшення інтересу до розвитку та впровадження новітніх технологій у сфері боротьби з фінансовими злочинами. У результаті поверхневого аналізу патентів, а саме рандомної вибірки з 1000 патентів, було виявлено, що основними технологіями, які застосовуються проти фінансових шахрайств, є використання машинного навчання та штучного інтелекту, блокчейн-технологій, прогнозного моделювання.

На рисунку 1.4 представлено графік, який показує розподіл опублікованих патентів у сфері технологій запобігання фінансовим злочинам серед різних країн та їхній відсотковий внесок у загальну кількість.

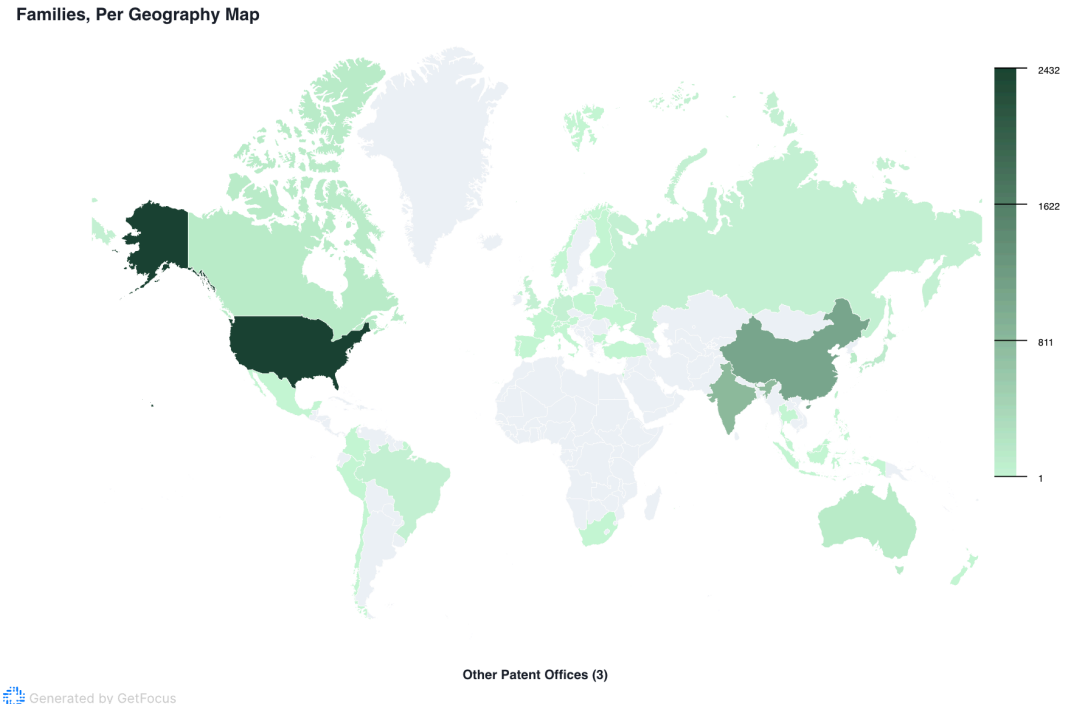

Рис. 1.4 – Кількість опублікованих патентів по країнам, 1999-2024.

Сполучені Штати Америки є безперечним лідером, маючи 2432 опублікованих патентів що становить 53,3% від загальної кількості. Значна кількість патентів може пояснюватись високим рівнем економічного розвитку США та їхнім домінуючим положенням у глобальному фінансовому секторі. Крім того, американські компанії є світовими дідерамиу у постачанні фінансових послуг. Китай займає другу позицію з 1076 патентами (23,6%). Швидке економічне зростання та масштабна цифровізація економіки Китаю сприяють активному розвитку фінансових технологій. Індія, з 821 патентними публікаціями (18%), також демонструє значну активність у цій галузі. Наявність значної кількості патентів, зареєстрованих через Всесвітню організацію інтелектуальної власності (WIPO) та Європейське патентне відомство (EPO), вказує на глобальний характер проблеми фінансових злочинів та активність європейських організацій у даній сфері. Реєстрація патентів на міжнародному рівні дозволяє компаніям захищати свої розробки у різних юрисдикціях, що є важливим в умовах глобалізації фінансових ринків та транскордонних фінансових операцій.

Країни як Канада, Південна Корея та Австралія, кожна з яких має близько 3% від загальної кількості патентів, демонструють помітний рівень активності, що корелює з їхнім високим рівнем розвитку цифрової економіки. Південна Корея,

відома своїми технологічними досягненнями та високим рівнем проникнення інтернету, активно впроваджує інновації у фінансовому секторі. Канада та Австралія, маючи стабільні економіки та розвинену фінансову інфраструктуру, також впроваджують передові технології для забезпечення безпеки фінансових систем.

Згідно даної вибірки даних, Україна має три патенти опубліковані у період з 2021 по 2024 рік, два з яких належать Міжнародному науково-навчальний центр інформаційних технологій та систем НАН та МОН України, та один був запатентований ТОВ "Тентенс Тек".

Загальний аналіз даних свідчить про те, що країни з високим рівнем економічного розвитку та розвиненою цифровою інфраструктурою є лідерами у патентуванні технологій запобігання фінансовим злочинам.

Аналіз активності у публікації патентів представлений на рисунку 1.5. Так, до 10 компаній з найбільшою кількістю опублікованих патентів, що стосуються технологій для запобігання фінансовим злочинам, належать: IBM, Capital One, ICBC, Mastercard, Bank Of America, Ping An, FICO, Visa, Paypal, Intuit.

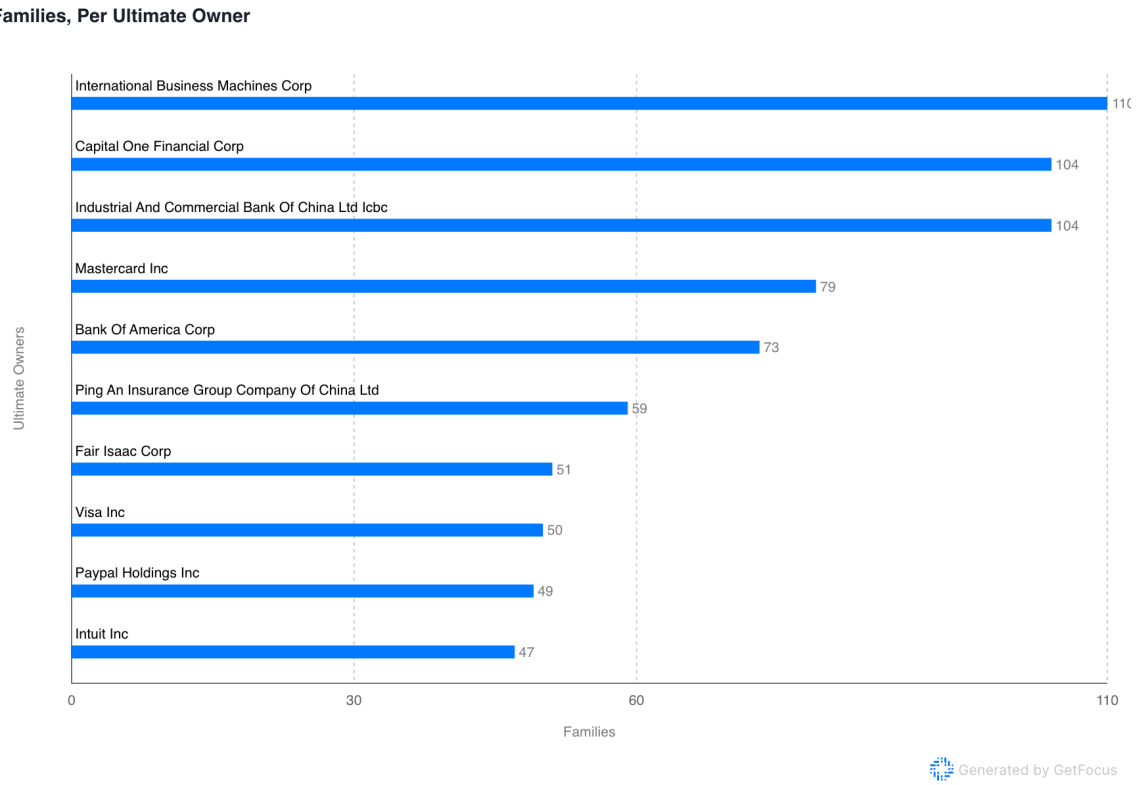

Рис. 1.5 – Топ 10 організацій за кількістю опублікованих патентів, 1999-2024.

Дві з десяти організацій є китайськими: ICBC (Industrial and Commercial Bank of China) та Ping An, решта вісім організацій – американські: IBM, Capital One, Mastercard, Bank of America, FICO, Visa, Paypal та Intuit.

Більшість цих компаній є провідними фінансовими установами або технологічними компаніями, які активно діють у фінансовому секторі. Традиційні банки, такі як Capital One, Bank of America, ICBC (Industrial and Commercial Bank of China) та Ping An, разом із компаніями, що спеціалізуються на платіжних системах та фінансових технологіях, такими як Mastercard, Visa та Paypal, інтенсивно інвестують у розробку технологій для боротьби з фінансовими злочинами. Це свідчить про те, що фінансові інститути усвідомлюють критичну важливість безпеки у своїй діяльності та прагнуть захистити себе та своїх клієнтів від ризиків шахрайства. Присутність компаній IBM та FICO, які відомі своїм експертним досвідом у сфері інформаційних технологій та аналізу даних, вказує на зростаючу роль передових технологій, таких як штучний інтелект, машинне навчання та великі дані, у запобіганні фінансовим злочинам. Intuit, відома своїми фінансовими програмними рішеннями, також робить вагомий внесок у розробку інструментів для забезпечення фінансової безпеки.

Протягом минулого року відбулися значні досягнення у технологіях з виявлення фінансових шахрайств, зосереджені переважно на інтеграції штучного інтелекту та машинного навчання. Одним із ключових нововведень є системи виявлення шахрайства в режимі реального часу, засновані на штучному інтелекті. Ці системи використовують алгоритми машинного навчання для моніторингу та запобігання шахрайським діям у фінансових транзакціях у режимі реального часу, часто включаючи модулі моніторингу транзакцій та системи миттєвого сповіщення. Також спостерігається розвиток технік машинного навчання для виявлення аномалій у транзакціях, таких як відмивання грошей або шахрайські операції з кредитними картками. Ці моделі аналізують поведінку транзакцій та використовують архітектури моделей глибокого навчання, зокрема рекурентні

нейронні мережі (RNNs) та мережі з довготривалою короткочасною пам'яттю (LSTMs). Інтеграція блокчейн-технологій з машинним навчанням стала ще одним важливим кроком вперед. Деякі системи поєднують блокчейн з машинним навчанням для автоматизації процесів та виявлення аномалій, демонструючи синергію між децентралізованими технологіями розподіленого реєстру та передовими моделями штучного інтелекту. Крім того, з'явилися нейросимвольні системи штучного інтелекту. Цей вид інноваційної технології поєднує нейронні мережі з символьним виведенням для підвищення ефективності виявлення шахрайства, приділяючи особливу увагу інтерпретованості та надійності в різних секторах.

Таким чином, останні досягнення у технологіях виявлення шахрайства свідчать про тенденцію активної інтеграції штучного інтелекту та машинного навчання з метою запобігання виникнення фінансових шахрайств.

1.4 Формулювання гіпотез

Діджиталізація, як один із провідних чинників сучасного розвитку, значно впливає на всі сфери суспільного життя, зокрема на економіку та фінансовий сектор. Активне впровадження цифрових технологій у фінансові системи відкриває нові можливості для підвищення ефективності послуг, розширення доступу до фінансових інструментів та стимулювання економічного зростання. Проте разом з цими перевагами діджиталізація створює умови для виникнення нових видів фінансових злочинів. У зв'язку з цим виникає необхідність дослідження двостороннього впливу діджиталізації на розвиток фінансових злочинів, враховуючи як економічні, так і безпекові аспекти.

Розвиток цифрових технологій розширює можливості для здійснення фінансових правопорушень. Анонімність, яку забезпечує Інтернет, та глобальна доступність цифрових платформ дозволяють злочинцям використовувати нові методи для здійснення шахрайства, відмивання грошей, кіберзломів та інших злочинів. Недостатня захищеність цифрових систем, а також недостатній рівень

фінансової та цифрової грамотності користувачів, сприяють зростанню кількості та складності фінансових злочинів. Таким чином, діджиталізація може виступати каталізатором для збільшення фінансової злочинності.

Поряд із викликами, які приносить діджиталізація, цифрові технології надають потужні інструменти для боротьби з фінансовими злочинами. Використання таких технологій, як штучний інтелект, машинне навчання, блокчейн та аналіз великих даних, дозволяє фінансовим установам та правоохоронним органам:

- Ефективніше виявляти та попереджати підозрілі транзакції.
- Підвищувати точність прогнозування потенційних загроз.
- Автоматизувати процеси моніторингу та контролю.
- Підвищувати рівень кібербезпеки та захисту даних.

Впровадження цифрових технологій сприяє економічному розвитку, підвищенню продуктивності, створенню нових робочих місць та галузей, сприяє фінансовій інклюзії та стимулює інновації, проте з іншого боку, вона створює нові ризики та загрози безпеці, пов'язані з кіберзлочинністю, втратами конфіденційності даних та можливістю економічних збитків через шахрайство. Тому необхідно контролювати впровадження та регулювання цифрових інструментів.

На основі аналізу наукової літератури та емпіричних спостережень сформульовано такі гіпотези дослідження:

1. Діджиталізація сприяє зростанню фінансових злочинів.
2. Цифрові технології можуть ефективно протидіяти злочинам.
3. Економічні та безпекові ефекти діджиталізації є двосторонніми.

РОЗДІЛ 2. ПОБУДОВА МАТЕМАТИЧНОЇ МОДЕЛІ ВЗАЄМОДІЇ МІЖ ФІНАНСОВОЮ ЗЛОЧИННІСТЮ ТА РІВНЕМ ДІДЖИТАЛІЗАЦІЇ

2.1 Опис вхідних змінних

Аналізуючи вплив діджиталізації на розвиток фінансових злочинів, важливо враховувати, що цифрові технології можуть як сприяти появі нових видів правопорушень, так і надавати інструменти для ефективної боротьби з ними. Тому комплексний підхід до дослідження, який поєднує економічні та безпекові аспекти, дозволить глибше зрозуміти двосторонні ефекти діджиталізації.

Для того, щоб підтвердити або спростувати сформовані гіпотези, проведемо дослідження, де показники діджиталізації є незалежними змінними, а показники економічних злочинів є залежною змінною. Так, було обрано перелік змінних для репрезентації рівня діджиталізації та рівня фінансової злочинності.

Індекс розвитку інформаційно-комунікаційних технологій (ICT Development Index, IDI) є комплексним інструментом, розробленим Міжнародним союзом електрозв'язку (ITU), який спрямований на оцінювання рівня розвитку ІКТ у різних країнах. Головна мета IDI полягає в тому, щоб визначити, наскільки універсальним і значущим є підключення до інформаційно-комунікаційних мереж у глобальному вимірі [23].

Індекс розвитку електронного уряду (EGDI) є комплексним показником, що оцінює рівень діджиталізації в різних країнах. Він відображає те, як держава застосовує інформаційно-комунікаційні технології (ІКТ) з метою покращення доступу громадян до цифрових послуг та їхнього залучення до використання цих сервісів. EGDI розраховується як середньозважене значення нормалізованих оцінок за трьома ключовими компонентами цифрового урядування: обсягом і якістю онлайн-сервісів, що надаються урядом (Індекс онлайн-послуг); рівнем розвитку телекомунікаційної інфраструктури країни (Індекс телекомунікаційної інфраструктури); та рівнем розвитку людського капіталу в контексті використання цифрових технологій (Індекс людського капіталу) [20].

Індекс готовності до штучного інтелекту (AI Preparedness Index, AIPI) оцінює рівень цифрового розвитку в 174 країнах на основі готовності до впровадження штучного інтелекту, базуючись на широкому наборі показників, які охоплюють цифрову інфраструктуру, людський капітал і політику на ринку праці, інновації та економічну інтеграцію, а також регулювання і етичні стандарти. AIPI є сумою чотирьох ключових вимірів, що представлені як окремі індикатори: Digital Infrastructure, Innovation and Economic Integration, Human Capital and Labor Market Policies, Regulation and Ethics [21]. Джерела даних включають: Інститут Фрейзера, Міжнародну організацією праці, Міжнародний союз електрозв'язку, Організацію Об'єднаних Націй, Конференцію ООН з торгівлі та розвитку, Всесвітній поштовий союз, Світовий банк та Всесвітній економічний форум.

Індекс готовності до мережевих технологій (Network Readiness Index, NRI) є комплексним показником, який оцінює спроможність країн ефективно використовувати інформаційно-комунікаційні технології (ІКТ) для стимулювання національного розвитку та конкурентоспроможності. NRI базується на чотирьох субіндексах: Технології, Люди, Управління та Вплив [22].

Для дослідження фінансової злочинності було обрано Глобальний індекс організованої злочинності (Global Organized Crime Index) та Базельський індекс боротьби з відмиванням грошей (Basel AML Index). Базельський індекс боротьби з відмиванням грошей (Basel AML Index) розроблений для того, щоб надавати всеосяжну оцінку ризику відмивання грошей (ML) та фінансування тероризму (TF) у різних країнах. Цей індекс розглядає ризик як ступінь вразливості держави до діяльності, пов'язаної з ML/TF, а також її спроможність ефективно протидіяти таким загрозам. Важливо підкреслити, що Basel AML Index репрезентує потенційний ризик та ефективність заходів, спрямованих на протидію цим злочинам, а не вимірює фактичний обсяг відмивання грошей чи фінансування тероризму в конкретній країні. Індекс складається з 18 індикаторів та 5 доменів. Кожний домен відображає певний аспект ризику відмивання грошей та фінансування тероризму: якість рамок протидії відмиванню грошей та фінансуванню тероризму (65% індексу), ризик корупції та хабарництва (10% індексу), фінансова прозорість та

стандарти (10%), публічна прозорість та підзвітність (5%), політичний та правовий ризик (10%). Кожен із доменів Базельського індексу боротьби з відмиванням грошей (Basel AML Index) інтегрує в собі важливі та загальновизнані індекси, що забезпечує комплексний і багатогранний підхід до оцінки ризиків відмивання грошей та фінансування тероризму. Залучення таких авторитетних показників, як оцінки FATF, Індекс фінансової секретності Tax Justice Network, Індекс сприйняття корупції Transparency International та інших, дозволяє розширити аналіз, врахувати складність та взаємопов'язаність процесів у реальному світі, охоплюючи різні аспекти, включаючи законодавчу базу, ефективність інституцій, рівень корупції, фінансову прозорість та політичні ризики [25].

Під час попереднього аналізу даних, між Індексом розвитку електронного уряду, Індексом готовності до штучного інтелекту, Індексом готовності до мережевих технологій та Індексом розвитку інформаційно-комунікаційних технологій була виявлена мультиколінеарність, з $r^2 > 0,84$. Так як змінні несуть схожу інформацію, було прийнято рішення залишити лише Індекс готовності до штучного інтелекту для проведення подальшого аналізу.

Таким чином, на основі вище зазначених індексів та їх складових факторів, для дослідження впливу діджиталізації на розвиток фінансових злочинів, було обрано Базельський індекс боротьби з відмиванням грошей (Basel AML Index), Індекс готовності до штучного інтелекту (AI Preparedness Index) та його індикатори: Digital Infrastructure, Innovation and Economic Integration, Human Capital and Labor Market Policies, Regulation and Ethics. Дані представлено для 134 країн світу з актуальними значеннями за 2023 рік.

2.2 Розробка математичної моделі та опис методів дослідження

Для проведення дослідження було виконано два етапи статистичного аналізу: кластерний аналіз та побудова регресійної моделі, з використанням статичного програмного забезпечення Stata SE18 та мови програмування Python.

Програма Stata SE призначена для проведення статистичного аналізу, економетричного моделювання та обробки великих масивів даних.

Python – це високорівнева мова програмування загального призначення. Завдяки широкому спектру спеціалізованих бібліотек, таких як Scikit-learn, Pandas, NumPy, SciPy, Plotly, Seaborn, Python дозволяє виконувати як базові математичні операції, так і складні статистичні моделі, будувати графіки та візуалізувати дані.

За допомогою команд summarize, describe, misstable summarize у Stata, було проведено попередній статистичний аналіз змінних AI Preparedness Index, Basel AML Index, Digital Infrastructure Index, Innovation and Economic Integration Index, Human Capital and Labor Market Policies Index, Regulation and Ethics Index. В результаті, набір даних не містить пропущених значень. Окрім того, між незалежними змінними була виявлена мультиколінеарність, що необхідно враховувати у подальшому аналізі. Високий рівень кореляції між незалежними змінними може спровокувати упереджені оцінки, тому, необхідно застосувати методи для зменшення впливу мультиколінеарності, щоб забезпечити надійні та значущі результати регресійного аналізу. Також, було виявлено аномальне значення у Innovation and Economic Integration Index, що дорівнює 0.004 одиниць при середньому значенні 0.12. Аномальне значення описує Innovation and Economic Integration Index Узбекистану. Незважаючи на це, було прийнято рішення не виключати дане значення з вибірки. Оскільки аналіз зосереджений на перехресних даних по країнах, збереження даного значення дозволяє врахувати можливі унікальні характеристики окремих країн та забезпечити більш повне та достовірне розуміння досліджуваних явищ.

Таблиця 2.1 - Описова статистика змінних

Змінна	Obs	Mean	Std. dev.	Min	Max
AI Preparedness	134	0.496	0.152	0.232	0.800
Basel AML	134	5.327	1.286	2.870	8.250
Digital Infrastructure	134	0.116	0.048	0.030	0.208

Innovation and Economic Integration	134	0.120	0.033	0.004	0.190
Human Capital and Labor Market Policies	134	0.128	0.032	0.041	0.195
Regulation and Ethics	134	0.130	0.048	0.022	0.230

Джерело : розроблено авторкою за допомогою використання Stata

Obs - загальна кількість спостережень, Mean – середнє значення змінної, Std. dev. – стандартне відхилення, Min – мінімальне значення, Max – максимальне значення

Для емпіричної перевірки сформульованих гіпотез щодо двостороннього впливу діджиталізації на ризик виникнення фінансових злочинів доцільно проаналізувати взаємозв'язок між цифровим рівнем розвитку країн та їхньою вразливістю до відмивання грошей і фінансування тероризму. У цьому контексті проведення кластерного аналізу між Індексом готовності до штучного інтелекту (AI Preparedness Index) та Базельським індексом боротьби з відмиванням грошей (Basel AML Index) виступає першим кроком у спростуванні або підтвердженні висунутих гіпотез.

Штучний інтелект є передовою технологією, яка справляє значний вплив на розвиток сучасного суспільства в багатьох галузях, таких як економіка, наука, промисловість, бізнес, освіта, медицина, транспорт та інші. Впровадження ШІ відкриває нові перспективи для інновацій та підвищення ефективності, проте водночас вимагає уваги до технічних, етичних, правових та соціальних питань, пов'язаних із його використанням. Зважаючи на багатогранність впливу штучного інтелекту та необхідність комплексної оцінки цифрового розвитку, для представлення рівня цифровізації було обрано індекс, що відображає готовність країни до впровадження ШІ на різних рівнях. Він дозволяє проаналізувати готовність країн до сучасних технологічних викликів та оцінити потенційний вплив діджиталізації на економічні та безпекові аспекти, що є основними цілями даного дослідження.

Базельський індекс боротьби з відмиванням грошей (Basel AML Index) репрезентує рівень ризику фінансових злочинів на національному рівні, включаючи відмивання грошей та фінансування тероризму.

Використання кластерного аналізу дозволяє згрупувати країни за схожістю показників діджиталізації та ризиків виникнення фінансових злочинів, що надає змогу виявити приховані закономірності. Зокрема, аналіз допоможе визначити, чи існує тенденція до зростання ризиків фінансових злочинів у країнах з високим рівнем цифрового розвитку, що відповідало б першій гіпотезі: діджиталізація сприяє зростанню фінансових злочинів. Також можна оцінити, чи країни з високим рівнем цифрового розвитку (підготовленості до штучного інтелекту) демонструють нижчі ризики за Basel AML Index, що підтверджувало б гіпотезу про те, що за умови забезпечення цифровими технологіями можна ефективно протидіяти фінансовим злочинам.

Кластерний аналіз методом k-середніх (k-means clustering) – це алгоритм некерованого машинного навчання, який використовується для розподілу набору даних на k кластерів на основі подібності між об'єктами. У методі k-середніх Евклідова відстань використовується як міра близькості між об'єктами даних та центрами кластерів.

Для визначення оптимальної кількості кластерів, використаємо метод ліктя та побудуємо відповідний графік використовуючи Python. Точка перегину вказує на оптимальну кількість кластерів, оскільки подальше збільшення кількості кластерів не призводить до суттєвого покращення внутрішньої однорідності кластерів. Згідно графіку (рис. 2.1) оптимальна кількість кластерів дорівнює 3.

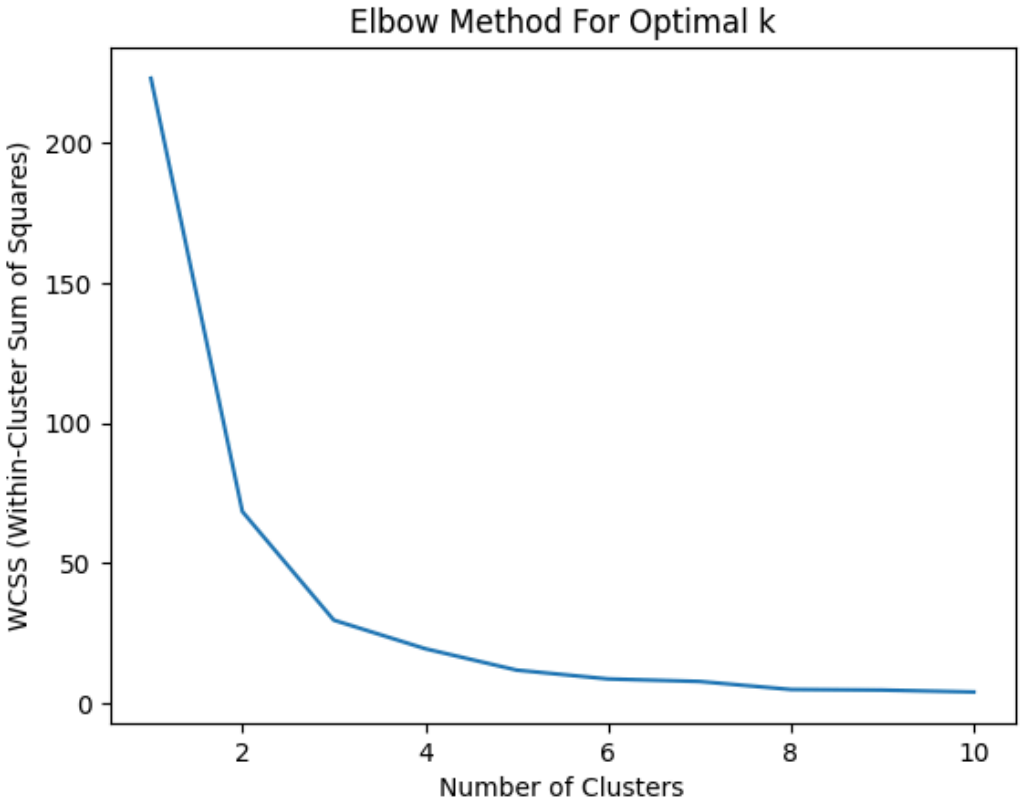

Рисунок 2.1 – Результат визначення оптимальної кількості кластерів методом ліктя

Джерело: розроблено авторкою за допомогою Python

Розрахунок коефіцієнта силуету є додатковим методом оцінки якості кластеризації. Так, коефіцієнт силуету при розподілі на 3 кластери дорівнює 0.50, що є більшим за значення коефіцієнту при розподілі на 4 кластери, що відповідно дорівнює 0.34.

Так, кластер №1 включає країни: Кіпр, Мальта, Греція, Словаччина, Польща, Словенія, Ізраїль, Чилі, Чехія, Італія, Португалія, Іспанія, Франція, Швейцарія, Бельгія, США, Канада, Литва, Ірландія, Японія, Австралія, Нідерланди, Швеція, Німеччина, Австрія, Люксембург, Велика Британія, Латвія, Сінгапур, Естонія, Нова Зеландія, Норвегія, Корея, Данія, Ісландія, Фінляндія.

У складі кластері №2: Таджикистан, Зімбабве, Білорусь, Туреччина, Парагвай, Шрі-Ланка, Киргизстан, Єгипет, Узбекистан, Молдова, Пакистан, Саудівська Аравія, Гондурас, Гватемала, Мексика, Філіппіни, Індонезія, Перу, Бангладеш, Туніс, Україна, Замбія, Казахстан, Намібія, Малаві, Бруней, Марокко, Панама, Бутан,

Таїланд, Домініканська Республіка, Еквадор, Угорщина, Сербія, Об'єднані Арабські Емірати, Албанія, Гамбія, Монголія, Сейшельські острови, Грузія, Північна Македонія, Болгарія, Тринідад і Тобаго, Ямайка, Катар, Бахрейн, Фіджі, Гана, Ботсвана, Багамські острови, Маврикій, Йорданія, Сент-Люсія, Колумбія, Південна Африка, Коста Ріка, Китай, Вірменія, Малайзія, Хорватія, Румунія, Барбадос, Кабо Верде, Уругвай.

Країни, що належать до кластеру №3: М'янма, Венесуела, Нікарагуа, Конго (Республіка), гроші, Чад, Гаїті, Гвінея-Бісау, Сурінам, Мавританія, Камерун, Ліберія, Габон, Конго, Мозамбік, Сватіні, Мадагаскар, Лаос, Буркіна Фасо, Нігер, Бенін, Камбоджа, Уганда, Сьєрра-Леоне, Танзанія, Алжир, Ангола, Того, Ефіопія, В'єтнам, Кот д'Івуар, Кенія, Нігерія, Сенегал.

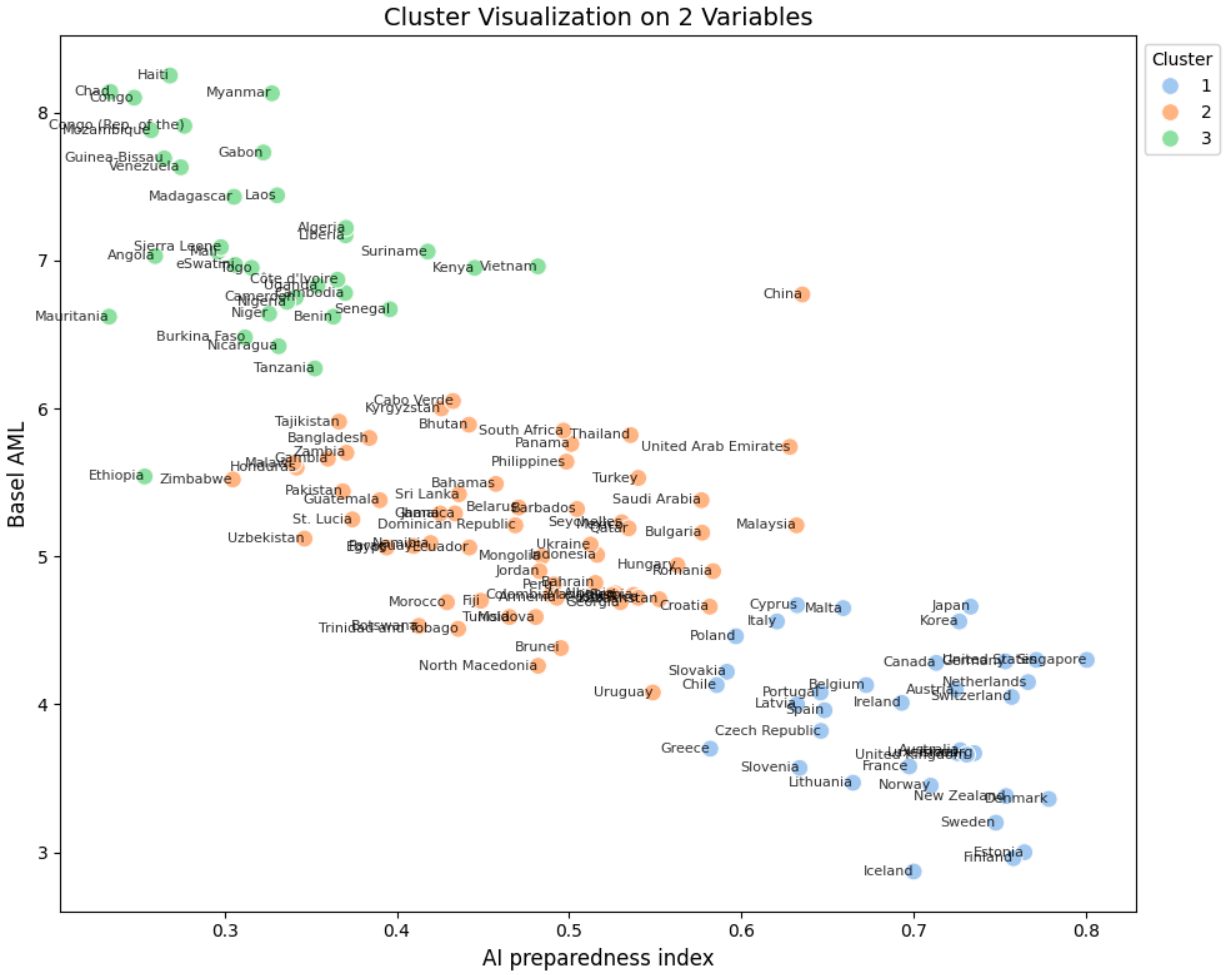

Рисунок 2.2 – Розподіл країн по кластерам.

Джерело: розроблено авторкою за допомогою Python

Розташування кластерів на рисунку 2.2 вказує на негативну кореляцію між рівнем цифрового розвитку країн та рівнем ризику виникнення фінансових злочинів.

Середні та мінімальні значення показників для кожного кластеру наведені у таблиці 2.2.

Таблиця 2.2 – Середні та мінімальні значення показників за кластером.

Змінна	Кластер №1	Кластер №2	Кластер №3
Average Basel AML	3,90	5,17	7,11
Average AI Preparedness	0,69	0,47	0,32
Average Digital Infrastructure	0,1774	0,1110	0,0632
Average Innovation and Economic Integration	0,1631	0,1114	0,0940
Average Human Capital and Labor Market Policies	0,1649	0,1283	0,0897
Average Regulation and Ethics	0,1910	0,1248	0,0765
Min Basel AML	2,87	4,08	5,54
Min AI Preparedness	0,581	0,304	0,232
Min Digital Infrastructure	0,1475	0,0473	0,0302
Min Innovation and Economic Integration	0,1242	0,0044	0,0682
Min Human Capital and Labor Market Policies	0,1347	0,0888	0,0417
Min Regulation and Ethics	0,1390	0,0550	0,0220

Джерело : розроблено авторкою за допомогою використання Stata

Наступним етапом, для перевірки виявленої залежності між рівнем цифровізації та фінансових злочинності, проведемо регресійний аналіз з використанням Stata. Це дозволить кількісно оцінити силу та напрямок взаємозв'язку між досліджуваними змінними, а також перевірити статистичну значущість отриманих результатів. Незалежними змінними на цьому етапі аналізу є індекси, які в сукупності формують AI Preparedness Index: Digital Infrastructure Index, Innovation and Economic Integration Index, Human Capital and Labor Market Policies Index,

Regulation and Ethics Index. При попередньому аналізі між цими індексами була виявлена мультиколінеарність. Включення всіх компонентів одночасно в одну регресійну модель може призвести до мультиколінеарності, що спотворить оцінки параметрів та знизить надійність висновків. У економетриці часто застосовується підхід до побудови окремих моделей у випадку мультиколінеарності, щоб отримати чисті оцінки впливу кожної змінної. Побудова окремих регресійних моделей дозволяє дослідити вплив кожного компонента AI Preparedness Index на Basel AML Index окремо. Це сприяє поглибленому розумінню того, як саме кожен аспект діджиталізації впливає на ризики фінансових злочинів. Окрім того, використання окремих моделей зменшує стандартні похибки оцінок коефіцієнтів і підвищує їх статистичну значущість.

Залежна змінна Basel AML Index не відповідає нормальному розподілу. Для зменшення асиметрії та відповідності припущенням регресійного аналізу, змінна була логарифмована. Результати тесту Шапіро-Вілка для логарифмованої змінної (W = 0,98360; p-value = 0,10755), вказує на те, що після перетворення, змінна не демонструє значущих відхилень від нормального розподілу.

Після побудови моделі лінійної регресії між Basel AML Index та Innovation and Economic Integration Index, й Basel AML Index з Regulation and Ethics Index, було виявлено статистично значущу гетероскедастичність в результаті проведення тесту Бройша-Пагана. Для усунення проблеми гетероскедастичності було застосовано робастну регресію, оскільки вона враховує неоднорідність дисперсії та знижує вплив викидів, які можуть спотворювати оцінки.

Результати побудови моделей наведені у таблиці 2.3.

Таблиця 2.3 – Результати регресійного аналізу

Basel AML	**Coefficient**	**t**	**P > | t |**	**R^2**	**F-statistic**
Digital Infrastructure*	-4.07	-15.04	0.000	0.65	226.27
Innovation and Economic Integration	-4.83	-10.48	0.000	0.45	109.76
Human Capital and Labor Market Policies	-5.94	-14.95	0.000	0.62	223.49

Regulation and Ethics	-4.20	-17.78	0.000	0.70	315.97

Джерело : розроблено авторкою за допомогою використання Stata

*Результати на основі робастної регресії.

Розроблена модель для характеристики зв'язку між ризиком виникнення фінансових злочинів та індексом регулювання та етики (Regulation and Ethics Index) має наступний вигляд (1):

$$y = -4,204 * x_1 + 2,192 \quad (1)$$

де, y – ризик виникнення фінансових злочинів;

x_1 – індекс регулювання та етики.

Модель для характеристики зв'язку між ризиком виникнення фінансових злочинів та індексом цифрової інфраструктури (Digital Infrastructure Index) (2):

$$y = -4,075 * x_2 + 2,119 \quad (2)$$

де, y – ризик виникнення фінансових злочинів;

x_2 – індекс цифрової інфраструктури.

Модель, яка описує взаємозв'язок між ризиком виникнення фінансових злочинів та індексом інновацій та економічної інтеграції (Innovation and Economic Integration Index) виглядає наступним чином (3):

$$y = -4,835 * x_3 + 2,228 \quad (3)$$

де, y – ризик виникнення фінансових злочинів;

x_3 – індекс інновацій та економічної інтеграції.

Взаємозв'язок між ризиком виникнення фінансових злочинів та індексом політики людського капіталу та ринку праці (Human Capital and Labor Market Policies Index) описується моделлю (4):

$$y = -5,946 * x_4 + 2,4 \qquad (4)$$

де, y – ризик виникнення фінансових злочинів;

x_4 – індекс політики людського капіталу та ринку праці.

Згідно результатів оцінок *F*-statistic (таблиця 2.2), кожна розроблена модель є статистично значущою (p-value < 0,05), а залежна змінна має статистично значущий зв'язок з незалежними змінними.

Значення R^2 свідчать про середній зв'язок між ризиком виникнення фінансових злочинів та інтеграцією інновацій, та сильним зв'язком між цифровою інфраструктурою, і регуляцією правової бази та механізмів людського капіталу, етики, ефективності уряду.

Зважаючи, що значення незалежних змінних коливаються у межах від 0 до 1, а значення залежної змінної – від 0 до 10, результати регресії мають наступну інтерпретацію: зі зменшенням Regulation and Ethics Index на одиницю вимірювання, ризик виникнення фінансових злочинів, зростає на 4,2 %; зі зменшенням Digital Infrastructure Index на одиницю вимірювання, ризик виникнення фінансових злочинів, зростає на 4,07 %; зі зменшенням Innovation and Economic Integration Index на одиницю вимірювання, ризик виникнення фінансових злочинів, зростає на 4,83 %; зі зменшенням Human Capital and Labor Market Policies Index на одиницю вимірювання, ризик виникнення фінансових злочинів, зростає на 5,94 %.

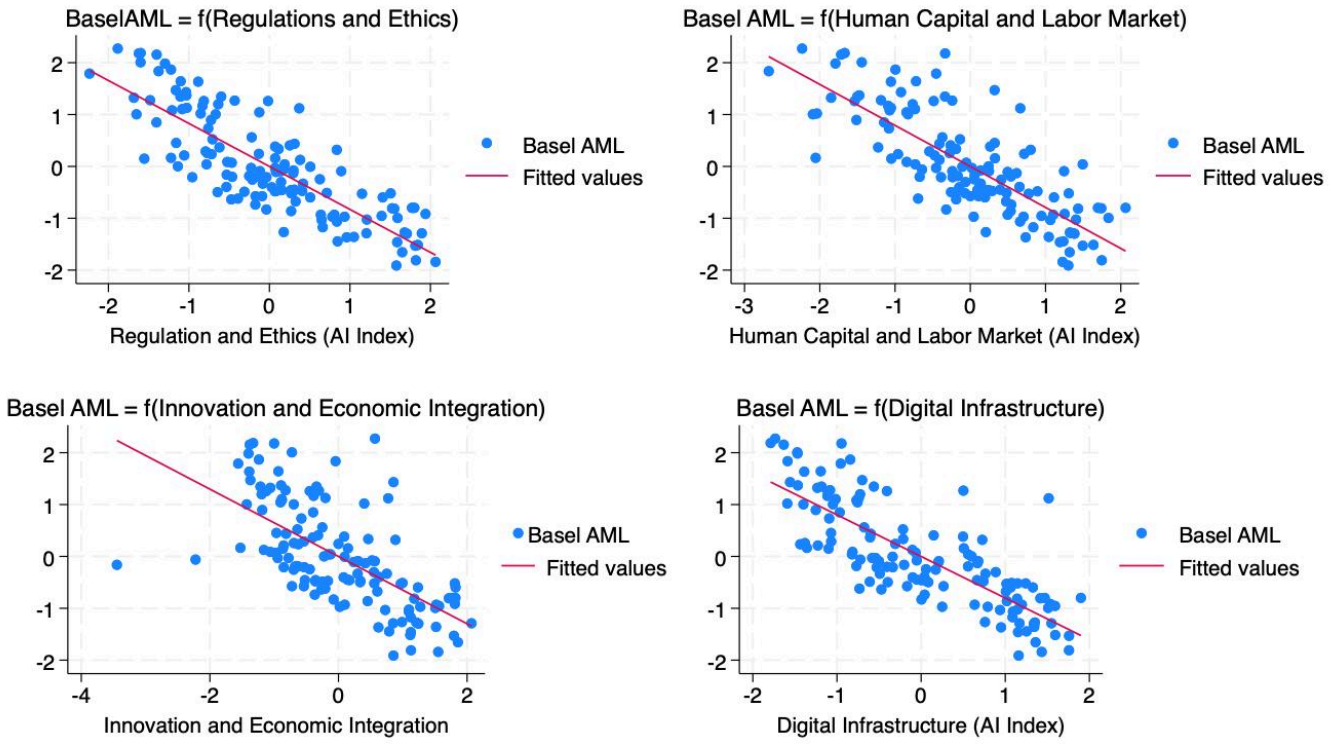

Рисунок 2.3 – Ілюстрація взаємозв'язку між Basel AML Index та субіндексів AI Index

Джерело : розроблено авторкою за допомогою використання Stata

Діаграми розсіювання на рисунку 2.3 демонструють обернені взаємозв'язки між Basel AML Index та відповідними компонентами, що свідчить про наступне:

- Покращення цифрової інфраструктури, зокрема підвищення рівня зв'язності та впровадження передових технологій, пов'язане зі зниженням ризиків відмивання грошей.
- Ефективне регулювання та високі етичні стандарти асоціюються з нижчим ризиком відмивання грошей.
- Доступність кваліфікованих кадрів та сприятливі умови на ринку праці, пов'язані з нижчим ризиком відмивання грошей.
- Розвинуті інноваційні екосистеми та економічна інтеграція, сприяють покращенню практик боротьби з фінансовими злочинами.

РОЗДІЛ 3. ІНТЕРПРЕТАЦІЯ РЕЗУЛЬТАТІВ АНАЛІЗУ ТА РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЕФЕКТИВНОГО ВПРОВАДЖЕННЯ ДІДЖИТАЛІЗАЦІЇ ТА МІНІМІЗАЦІЇ РИЗИКІВ ФІНАНСОВИХ ЗЛОЧИНІВ

3.1 Інтерпретація отриманих результатів.

Загальні висновки аналізу свідчать про те, що підвищення рівня розвитку регуляторно-етичних норм, людського капіталу, інноваційної діяльності та цифрової інфраструктури має позитивний вплив на зниження ризиків виникнення фінансових злочинів.

Регресійний аналіз показав, що найбільший вплив на ризик виникнення фінансових злочинів має субіндекс Регулювання та етика (Regulation and Ethics Index). Це свідчить про те, що рівень регуляторних механізмів у сфері діджиталізації є критичним фактором у протидії фінансовим злочинам. Зважаючи на це, для інтерпретації результати кластерного аналізу було проведено додатковий аналіз Democracy Index [30] та Global Digitalization Index (GDI) від Huawei [31], який групує країни за рівнем зрілості ІКТ та економічного розвитку на "Frontrunners", "Adopters" та "Starters".

Кластер 1 включає країни з високим рівнем діджиталізації та низьким ризиком фінансових злочинів. До цього кластеру належать переважно розвинені держави, такі як Швейцарія, Бельгія, США, Канада, Японія, Австралія, Нідерланди, Швеція, Сінгапур, Естонія, Нова Зеландія, Норвегія, Корея, Данія, Ісландія, Фінляндія та інші. 56% країн що належать до першого кластеру є "повними демократіями" (Full democracies), а 44% — "дефектними демократіями" (Flawed democracies). Крім того, 21 з 22 країн, віднесених до групи "Frontrunners", належать до першого кластеру. Це свідчить про високий рівень політичних свобод, громадянських прав та ефективне функціонування демократичних інститутів, що сприяє ефективній протидії фінансовим злочинам.

Кластер 2 містить країни з середнім рівнем діджиталізації та помірним ризиком фінансових злочинів. До нього входять держави, такі як Угорщина, Сербія,

Об'єднані Арабські Емірати, Туреччина, Україна, Хорватія, Китай та інші. У цьому кластері 42% країн є "дефектними демократіями", 29% — "гібридними режимами" (Hybrid regimes), 24% — "авторитарними режимами" (Authoritarian regimes), і лише 6% — "повними демократіями". Державний устрій вказує на можливе пояснення приналежності цих країн до другого кластеру: низька ефективність заходів з протидії фінансовим злочинам, недостатня прозорість та підзвітність інституцій.

Кластер 3 охоплює країни з низьким рівнем діджиталізації та високим ризиком фінансових злочинів, такі як М'янма, Венесуела, Нікарагуа, Конго, Гаїті та інші. Дана вибірка містить 62% країн які мають "авторитарний режим", 32% — "гібридний режим", і лише 6% — "дефектну демократію", що свідчить про відсутність демократичних принципів та слабкі регуляторні механізми, що в свою чергу створюють сприятливі умови для поширення фінансових злочинів.

Результати дослідження підтверджують, що країни з високим рівнем діджиталізації демонструють нижчі ризики за Basel AML Index. Сам по собі рівень діджиталізації не є визначальним фактором збільшення ризиків. Показовим є випадок Китаю, який, незважаючи на високий технічний розвиток та діджиталізацію, має високий ризик фінансових злочинів через авторитарний політичний режим. Це свідчить про те, що сам по собі технологічний прогрес без належного інституційного супроводу не гарантує економічної безпеки та стабільності. Ключову роль відіграють ефективність регуляторних механізмів та наявність демократичних інститутів. Окрім того економічні та безпекові ефекти діджиталізації є двосторонніми. З одного боку, діджиталізація сприяє економічному розвитку та може покращити механізми протидії фінансовим злочинам. З іншого боку, без належного регулювання та етичних стандартів вона може створювати нові можливості для здійснення таких злочинів.

3.2 Розробка рекомендацій за результатами проведеного аналізу.

На основі результатів дослідження, було створено наступний перелік практичних рекомендацій для урядів, державних установ, правових органів, та

бізнесу з метою ефективного впровадження діджиталізації та мінімізації ризиків фінансових злочинів:

Таблиця 3.1 - Рекомендації щодо мінімізації ризиків фінансових злочинів.

Рекомендація	**Очікувані ефекти**
1. Зміцнення регуляторних та правових рамок у сфері діджиталізації	Підвищення ефективності боротьби з фінансовими злочинами Зниження ризику відмивання грошей Створення прозорого бізнес-середовища
2. Підвищення етичних стандартів та культури ділової етики	Зменшення корупційних практик Підвищення довіри інвесторів Сприяння відповідальному веденню бізнесу
3. Розвиток людського капіталу та підвищення кваліфікації	Забезпечення кваліфікованих фахівців для цифрової економіки Підвищення інноваційного потенціалу Покращення конкурентоспроможності країни
4. Покращення цифрової інфраструктури з акцентом на безпеку	Зниження ризиків кіберзлочинності Підвищення надійності та швидкості фінансових транзакцій Сприяння цифровій трансформації економіки
5. Стимулювання інновацій та економічної інтеграції	Підвищення економічного зростання Збільшення зайнятості Розширення ринків збуту
6. Підвищення прозорості та підзвітності інституцій	Покращення якості державних послуг Зниження рівня корупції Підвищення довіри громадян до влади
8. Застосування технологій штучного інтелекту у протидії фінансовим злочинам	Підвищення швидкості та точності виявлення злочинів Зниження операційних витрат Покращення прогнозування та запобігання ризикам
9. Удосконалення політичних інститутів та зміцнення демократії	Підвищення інституційної стійкості Покращення інвестиційного клімату Забезпечення стабільності та передбачуваності політики

Джерело: розроблено авторкою

Незважаючи на очевидність деяких рекомендацій, їх впровадження важливе для удосконалення регуляторних рамок, розвитку людського капіталу, інновацій та

технологій, а також зміцнення демократичних інститутів, що, як показало дослідження, є ключовим для успішного подолання викликів, пов'язаних з фінансовою злочинністю у еру діджиталізації.

ВИСНОВКИ

У даній роботі було проведено дослідження впливу діджиталізації на розвиток фінансових злочинів з метою виявлення взаємозв'язків між рівнем цифрового розвитку країни та ризиками виникнення фінансових правопорушень.

Результати досліджень описані в наявних наукових працях, визначають фінансові злочини як незаконні дії з метою отримання неправомірної вигоди, що призводять до фінансових втрат. Крім того, було встановлено відсутність загальноприйнятої класифікації фінансових злочинів, у зв'язку з чим у роботі запропоновано власну класифікацію їх видів. Також, у ході дослідження було враховано, що кіберзлочини можуть охоплювати як правопорушення проти інформаційно-комунікаційних технологій, так і злочини, у яких ІКТ виступають інструментом для їх здійснення.

Даними для проведення аналізу було обрано Базельський індекс боротьби з відмиванням грошей як показник ризику фінансових злочинів, Індекс готовності до штучного інтелекту, який відображає рівень цифрового розвитку та його складники, у розрізі 134 країн світу.

У процесі статистично-математичного моделювання зокрема методом регресійного аналізу (лінійна та робастна регресії) та кластеризації методом k-середніх, було виявлено, що країни з більш розвиненими правовими рамками та високими етичними стандартами демонструють нижчий ризик фінансової злочинності.

Кластеризація країн методом k-середніх та окремий аналіз показників значущих факторів по кожному кластеру з урахуванням Індексу демократії та Глобального індексу цифровізації дозволив оцінити країни за стійкістю до виникнення фінансових злочинів та рівнем діджиталізації незалежно від традиційного групування країн запропонованого світовими організаціями як Група Світового банку, Європарламент тощо.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Overview*. United Nations : Office on Drugs and Crime. (n.d.). https://www.unodc.org/unodc/en/money-laundering/overview.html
2. *Financial crime*. Financial Conduct Authority. (n.d.). https://www.handbook.fca.org.uk/handbook/glossary/G416.html
3. Europol. (n.d.). *Economic crime*. Дата звернення: 20 жовтня 2024, з https://www.europol.europa.eu/crime-areas/economic-crime
4. Organisation for Economic Co-operation and Development. (n.d.). *Tax and crime*. Дата звернення: 20 жовтня 2024, з https://www.oecd.org/en/topics/tax-and-crime.html
5. Financial Action Task Force. (2012). *International standards on combating money laundering and the financing of terrorism & proliferation: The FATF recommendations*. Дата звернення: 20 жовтня 2024, з https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202012.pdf.coredownload.inline.pdf
6. International Monetary Fund. (2023, December 7). *Financial crimes hurt economies and must be better understood and curbed*. Дата звернення: 20 жовтня 2024, з https://www.imf.org/en/Blogs/Articles/2023/12/07/financial-crimes-hurt-economies-and-must-be-better-understood-and-curbed
7. Gottschalk, P. (2010). Categories of financial crime. *Journal of Financial Crime, 17*(4), 441–458. Дата звернення: 22 жовтня 2024, з https://doi.org/10.1108/13590791011082797
8. Ryan Merlin Yonk. Improving Quality of Life: Exploring Standard of Living, Wellbeing, and Community Development. Дата звернення: 24 жовтня 2024, з https://books.google.com.ua/books?id=HbdaEAAAQBAJ&lr=&hl=uk&source=gbs_navlinks_s
9. Rodrigues, M. G. (2020). *Title of the Work*. Дата звернення: 23 жовтня 2024, з https://comum.rcaap.pt/bitstream/10400.26/36935/1/10.1007%40978-3-030-43616-247.pdf

10. Morley, J., Widdicks, K., & Hazas, M. (2018). Digitalisation, energy and data demand: The impact of internet traffic on overall and peak electricity consumption. *Energy Research & Social Science, 38*(1), 128–137. https://doi.org/10.1016/j.erss.2018.01.021
11. International Energy Agency. (2017). *Digitalization & Energy*. Дата звернення: 24 жовтня 2024, з http://www.iea.org/digital/
12. Gebre-Mariam, M., & Bygstad, B. (2019). Digitalization mechanisms of health management information systems in developing countries. *Information and Organization, 29*(1), 1–22. https://doi.org/10.1016/j.infoandorg.2019.100255
13. Yoo, Y., Lyytinen, K., Boland, R., & Berente, N. (2010). The next wave of digital innovation: Opportunities and challenges: A report on the research workshop 'Digital challenges in innovation research'. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.1622170
14. Décary-Hétu, D., & Aldridge, J. (2023). Introduction: The digital transformations of illicit drug markets as a process of reconfiguration and continuity. In *Emerald Insight Work*. Дата звернення: 27 жовтня 2024, з https://www.emerald.com/insight/content/doi/10.1108/978-1-80043-866-820231001/full/pdf
15. Rodrigues, S., & Ramos, M. (2021). Digital business transformation: Challenges for developing digital competencies in multinational enterprises. *Critical Perspectives on International Business*. Дата звернення: 27 жовтня 2024, з https://www.emerald.com/insight/content/doi/10.1108/cpoib-10-2021-0088/full/html#sec006
16. Interpol. (2023). Illegal wildlife trade has become one of the world's largest criminal activities. Дата звернення: 27 жовтня 2024, з https://www.interpol.int/News-and-Events/News/2023/Illegal-wildlife-trade-has-become-one-of-the-world-s-largest-criminal-activities
17. Emerald Insight. (2023). Illegal wildlife trade: The critical role of the banking sector in combating money laundering. *Journal of Money Laundering Control.* Дата

звернення: 30 жовтня 2024, з https://www.emerald.com/insight/content/doi/10.1108/jmlc-06-2023-0105/full/pdf

18. Statista. Cybercrime incidents victim industry size. Дата звернення: 20 жовтня 2024, з https://www.statista.com/statistics/194246/cybercrime-incidents-victim-industry-size/
19. Federal Bureau of Investigation. (2023). *2023 Internet Crime Report*. Дата звернення: 30 жовтня 2024, з https://www.ic3.gov/AnnualReport/Reports/2023_IC3Report.pdf
20. United Nations Department of Economic and Social Affairs. (2024). *UN E-Government Survey 2024*. Дата звернення: 30 жовтня 2024, з https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2024
21. International Monetary Fund. (n.d.). *DataMapper: Advanced Indicators and Policy Insights (AIPI)*. Дата звернення: 30 жовтня 2024, з https://www.imf.org/external/datamapper/datasets/AIPI
22. Network Readiness Index. (n.d.). *The Network Readiness Index*. Дата звернення: 27 жовтня 2024, з https://networkreadinessindex.org/
23. International Telecommunication Union. (2024). *ICT Development Index 2024*. Дата звернення: 27 жовтня 2024, з https://www.itu.int/itu-d/reports/statistics/idi2024/
24. Organized Crime Index. (n.d.). *The Organized Crime Index*. Дата звернення: 27 жовтня 2024, з https://ocindex.net/
25. Basel Institute on Governance. (n.d.). *Basel AML Index Methodology*. Дата звернення: 27 жовтня 2024, з https://index.baselgovernance.org/methodology
26. Forbes Technology Council. (2024, February 7). Fighting financial crime with AI is not a trend: It's a necessity. *Forbes*. Дата звернення: 30 жовтня 2024, з https://www.forbes.com/councils/forbestechcouncil/2024/02/07/fighting-financial-crime-with-ai-is-not-a-trend-its-a-necessity/

27. KPMG. (2023, August). Manage economic crime risk with AI. Дата звернення: 13 листопада 2024, з https://kpmg.com/uk/en/home/insights/2023/08/manage-economic-crime-risk-with-ai.html
28. HSBC. (n.d.). Harnessing the power of AI to fight financial crime. Дата звернення: 1 листопада 2024, з https://www.hsbc.com/news-and-views/views/hsbc-views/harnessing-the-power-of-ai-to-fight-financial-crime
29. PwC. (n.d.). Improving financial crime programs with AI: How to help implement effectively. Дата звернення: 2 листопада 2024, з https://riskproducts.pwc.com/insights/improving-financial-crime-programs-with-ai-how-to-help-implement-effective/
30. The Economist Intelligence Unit. (2024). *Democracy Index 2023: Final report*. Дата звернення: 21 листопада 2024, з https://latinoamerica21.com/wp-content/uploads/2024/02/Democracy-Index-2023-Final-report.pdf
31. Huawei. (n.d.). *Global Digital Index*. Дата звернення: 24 жовтня 2024, з https://www.huawei.com/en/gdi
32. KPMG. (n.d.). A paradigm shift in financial crime. Дата звернення: 24 жовтня 2024, з https://kpmg.com/xx/en/our-insights/risk-and-regulation/a-paradigm-shift-in-financial-crime.html
33. Abu Olaim, A., & Rahman, A. (2016). Recent development of anti-money laundering law in Jordan. *Journal of Money Laundering Control, 19*(4), 316–328. https://doi.org/10.1108/JMLC-07-2015-0027
34. Warde, I. (2007). The war on terror, crime and the shadow economy in the MENA countries. *Mediterranean Politics, 12*(2), 233–248. https://doi.org/10.1080/13629390701398033
35. Alldridge, P. (2008). Money laundering and globalization. *Journal of Law and Society, 35*, 437–463. https://doi.org/10.1111/j.1467-6478.2008.00446.x

36. Kaygin, E., Topcuoglu, E., & Ozkes, S. (2019). Investigating the bitcoin system and its properties within the scope of business ethics. *Turkish Journal of Business Ethics, 11*(2), 186–192. https://doi.org/10.12711/tjbe.2018.11.2.0020
37. Emerald Insight. (2022). *Journal of Financial Crime*. Дата звернення: 20 жовтня 2024, з https://www.emerald.com/insight/content/doi/10.1108/jfc-07-2022-0161/full/html
38. Greenberg, A. (2018). The dark web's favorite currency is less untraceable than it seems. *Wired.* Дата звернення: 27 жовтня 2024, з https://www.wired.com/story/monero-privacy/
39. Dyntu, V., & Dykyi, O. (2018). Cryptocurrency in the system of money laundering. *Baltic Journal of Economic Studies, 4*(5), https://www.researchgate.net/publication/331092947_CRYPTOCURRENCY_IN_THE_SYSTEM_OF_MONEY_LAUNDERING
40. Mabunda, S. (2018). Cryptocurrency: The new face of cyber money laundering. *2018 International Conference on Advances in Big Data, Computing and Data Communication Systems (ICABCD)*, 1–6. https://doi.org/10.1109/ICABCD.2018.8465415
41. Arasasingham, A., & DiPippo, G. (2022). Cryptocurrency's role in the Russia-Ukraine crisis. *Center for Strategic and International Studies*. Дата звернення: 29 жовтня 2024, з https://www.csis.org/analysis/cryptocurrencys-role-russia-ukraine-crisis
42. Nicholls, J., Kuppa, A., & Le-Khac, N.-A. (2021). Financial cybercrime: A comprehensive survey of deep learning approaches to tackle the evolving financial crime landscape. *IEEE Access, 9*, 163965–163986. https://doi.org/10.1109/ACCESS.2021.3134076
43. Alweqyan, D. (2024). Cyberattacks in the context of international law enforcement. *Journal of Financial Crime, 31*(5), 1052–1066. https://doi.org/10.1108/JFC-07-2023-0164
44. Peltier-Rivest, D. (2024). Gift or bribe? The characteristics and the role of gift policies in the prevention of corruption. *Journal of Financial Crime, 31*(5), 1094–1105. https://doi.org/10.1108/JFC-09-2023-0222
45. Pavlidis, G. (2023). Deploying artificial intelligence for anti-money laundering and asset recovery: The dawn of a new era. *Journal of Money Laundering Control, 26*(7), 155–166. https://doi.org/10.1108/JMLC-03-2023-0050

ДОДАТКИ

ДОДАТОК А

SUMMARY

Petrenko K.The impact of digitalization on the development of financial crimes: economic and security effects. Master's thesis. Sumy State University, Sumy, 2024.

This study aims to explore the theoretical aspects of digitalization and financial crimes, as well as the relationship between them, with a particular focus on the impact of digital technologies on the emergence, evolution, and prevention of financial offenses. To achieve this, the research analyzes key concepts related to financial crimes and digitalization. It reviews relevant scientific literature regarding the use of technology in crime prevention, assesses the current state of digital development in Ukraine and globally, and outlines the research methodology. Using data from 134 countries, the study employs cluster analysis and constructs four single-factor regression models to illustrate the functional relationship between the risk of financial crimes and digitalization.

Keywords: digitalization, financial crimes, financial fraud, economy, cluster analysis, regression, technological impact.

АНОТАЦІЯ

Петренко К.Ю. Вплив діджиталізації на розвиток фінансових злочинів: економічні та безпекові ефекти. Кваліфікаційна робота магістра. Сумський державний університет, Суми, 2024 р.

Метою роботи є вивчення теоретичних аспектів взаємодії між діджиталізацією та фінансовими злочинами, а також аналіз впливу цифрових технологій на виникнення, розвиток та протидію фінансовим правопорушенням. Відповідно до поставлених задач було досліджено поняття фінансових злочинів та цифровізації; проведено аналіз наукових досліджень у сфері фінансових злочинів та застосуванні технологій для їх запобіганню, аналіз сучасного стану цифрового розвитку в Україні та світі; сформовано методологію дослідження, запропоновано та описано масив

вхідних даних; змодельовано та спроектовано результати функціональної залежності між ризиком виникнення фінансових злочинів та цифровізацією. В результаті було проведено кластерний аналіз та побудовано чотири однофакторних регресійних моделі на основі даних, що охоплюють 134 країни.

Ключові слова: економіка, економічні злочини, кластеризація, регресія, фінансові злочини, цифровізація, шахрайство.

ДОДАТОК В

```
. describe AIpreparednessindex BaselAML DigitalInfrastructureAIIndex InnovationandEconomicIntegra
> t HumanCapitalandLaborMarketP RegulationandEthicsAIIndex

Variable      Storage   Display    Value
    name         type    format    label      Variable label
------------------------------------------------------------------------------
AIpreparednes~x double  %14.2f                 AI preparedness index
BaselAML        double  %14.2f                 Basel AML
DigitalInfras~x double  %14.2f                 Digital Infrastructure (AI Index)
Innovationand~t double  %14.2f                 Innovation and Economic Integration (AI Index)
HumanCapitala~P double  %14.2f                 Human Capital and Labor Market Policies (AI Index)
Regulationand~x double  %14.2f                 Regulation and Ethics (AI Index)
```

Рисунок В.1 – Описові статистики змінних

```
. summarize AIpreparednessindex DigitalInfrastructureAIIndex InnovationandEconomicIntegrat HumanC
> apitalandLaborMarketP RegulationandEthicsAIIndex BaselAML

    Variable |        Obs        Mean    Std. dev.       Min        Max
-------------+---------------------------------------------------------
AIprepared~x |        134     .496516    .1526665    .232901   .8005667
DigitalInf~x |        134     .116768    .0483626   .0302884   .2086174
Innovation~t |        134    .1209401    .0338141   .0044147   .1909364
HumanCapit~P |        134    .1284158     .032353   .0417673   .1951995
Regulation~x |        134     .130392    .0484712   .0220851   .2304401
-------------+---------------------------------------------------------
    BaselAML |        134     5.32791    1.286145       2.87       8.25
```

Рисунок В.2 – Описові статистики змінних

```
. correlate ICTDevelopmentIndexIDI EGDI AIpreparednessindex NRI
(obs=113)

             | ICTDev~I     EGDI AIprep~x      NRI
-------------+------------------------------------
ICTDevelop~I |   1.0000
        EGDI |   0.9485   1.0000
AIprepared~x |   0.8401   0.8954   1.0000
         NRI |   0.8418   0.8932   0.9739   1.0000
```

Рисунок В.3 – Кореляційна матриця між індексами, що розглядались як незалежні змінні

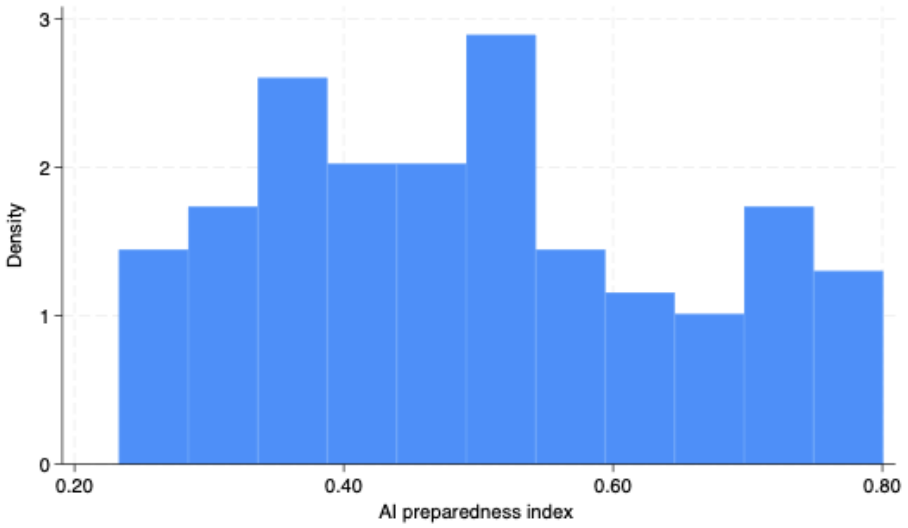

Рисунок В.4 – Гістограма для перевірки нормальності розподілу AI preparedness index

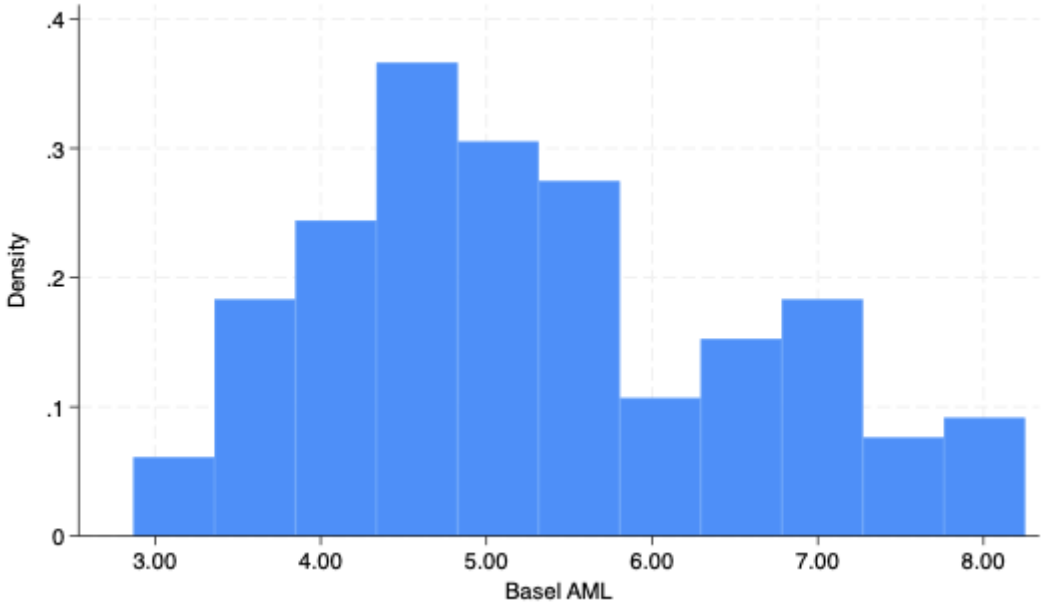

Рисунок В.5 – Гістограма для перевірки нормальності розподілу Basel AML

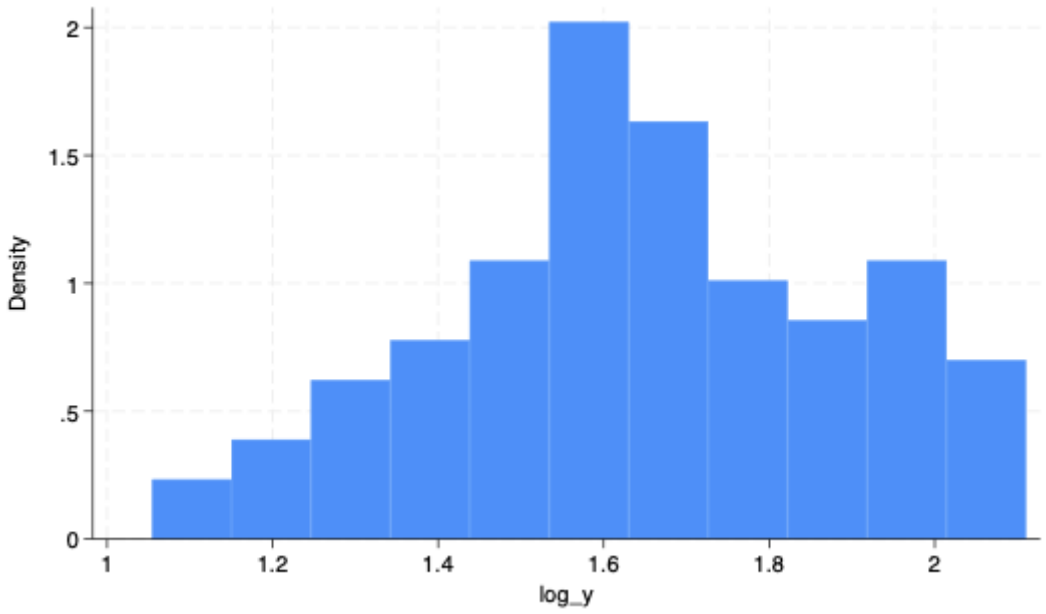

Рисунок В.5 – Гістограма для перевірки нормальності розподілу після логарифмування Basel AML

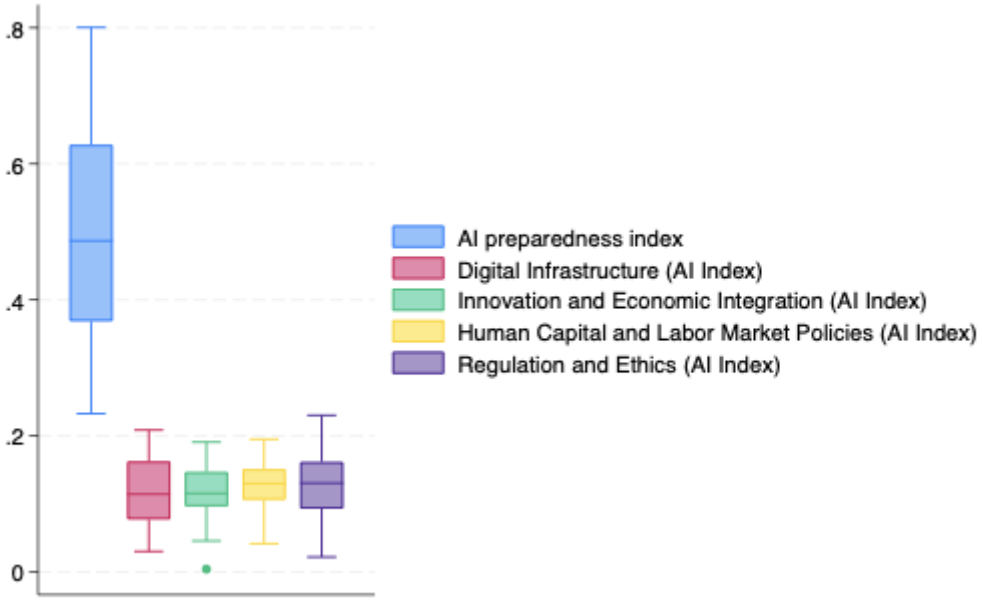

Рисунок В.6 – Діаграма розмаху для перевірки аномальних значень незалежних змінних

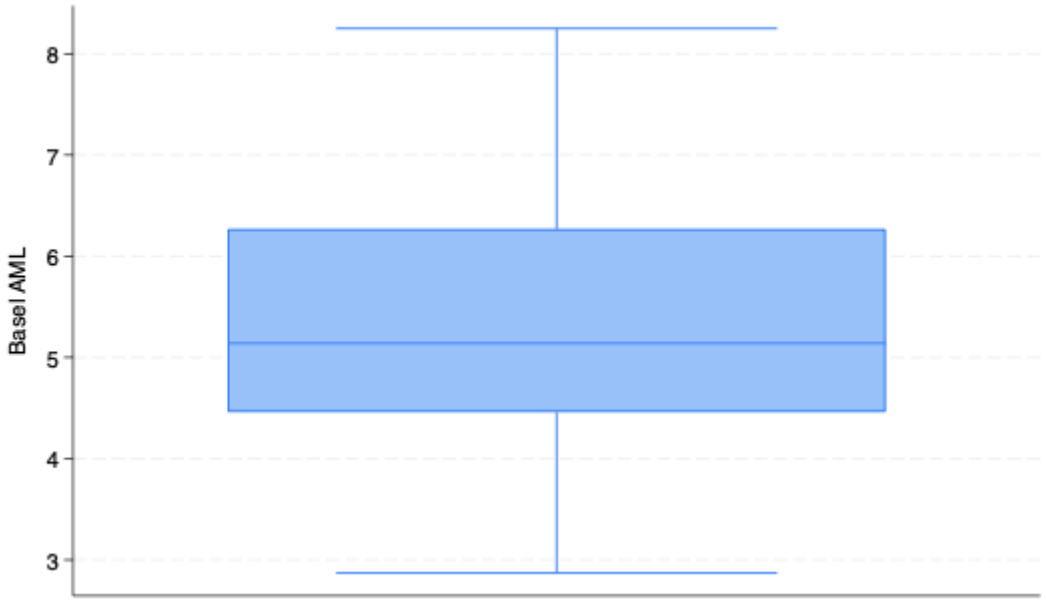

Рисунок В.7 – Діаграма розмаху для перевірки аномальних значень залежної змінної

```
. regress log_y HumanCapitalandLaborMarketP

      Source |       SS           df       MS      Number of obs   =       134
-------------+----------------------------------   F(1, 132)       =    223.49
       Model |  4.92297603         1  4.92297603   Prob > F        =    0.0000
    Residual |  2.90761842       132  .022027412   R-squared       =    0.6287
-------------+----------------------------------   Adj R-squared   =    0.6259
       Total |  7.83059445       133   .05887665   Root MSE        =    .14842

------------------------------------------------------------------------------
       log_y | Coefficient  Std. err.      t    P>|t|     [95% conf. interval]
-------------+----------------------------------------------------------------
HumanCapita~P |  -5.946669   .3977788    -14.95   0.000    -6.733515   -5.159823
       _cons |   2.407653   .0526656     45.72   0.000     2.303476    2.511831
------------------------------------------------------------------------------

. estat hettest

Breusch-Pagan/Cook-Weisberg test for heteroskedasticity
Assumption: Normal error terms
Variable: Fitted values of log_y

H0: Constant variance

         chi2(1) =     2.14
Prob > chi2 =   0.1433
```

Рисунок В.8 – Побудова лінійної регресії, де x - Human Capital and Labor Market Policies Index та перевірка на гетероскедастичність

```
. regress log_y RegulationandEthicsAIIndex
```

Source	SS	df	MS	Number of obs	=	134
				F(1, 132)	=	315.97
Model	5.52319978	1	5.52319978	Prob > F	=	0.0000
Residual	2.30739468	132	.017480263	R-squared	=	0.7053
				Adj R-squared	=	0.7031
Total	7.83059445	133	.05887665	Root MSE	=	.13221

log_y	Coefficient	Std. err.	t	P>|t|	[95% conf.	interval]
RegulationandEthicsAIIndex	-4.204226	.2365182	-17.78	0.000	-4.672082	-3.736369
_cons	2.192205	.0328871	66.66	0.000	2.127151	2.257259

```
. estat hettest

Breusch-Pagan/Cook-Weisberg test for heteroskedasticity
Assumption: Normal error terms
Variable: Fitted values of log_y

H0: Constant variance

    chi2(1) =   0.26
Prob > chi2 = 0.6084
```

Рисунок В.9 – Побудова лінійної регресії, де x - Regulations and Ethics Index та перевірка на гетероскедастичність

```
. regress log_y InnovationandEconomicIntegrat
```

Source	SS	df	MS		
Model	3.55505755	1	3.55505755	Number of obs	= 134
				F(1, 132)	= 109.76
Residual	4.2755369	132	.032390431	Prob > F	= 0.0000
				R-squared	= 0.4540
				Adj R-squared	= 0.4499
Total	7.83059445	133	.05887665	Root MSE	= .17997

log_y	Coefficient	Std. err.	t	P>|t|	[95% conf.	interval]
InnovationandEconomicIntegrat	-4.835035	.4615137	-10.48	0.000	-5.747955	-3.922115
_cons	2.228757	.0579404	38.47	0.000	2.114145	2.343369

```
. estat hettest

Breusch-Pagan/Cook-Weisberg test for heteroskedasticity
Assumption: Normal error terms
Variable: Fitted values of log_y

H0: Constant variance

    chi2(1) =   2.03
Prob > chi2 = 0.1540
```

Рисунок В.10 – Побудова лінійної регресії, де x - Innovation and Economic Integration Index та перевірка на гетероскедастичність

```
. regress log_y DigitalInfrastructureAIIndex
```

Source	SS	df	MS		
Model	5.16723813	1	5.16723813	Number of obs	= 134
Residual	2.66335633	132	.020176942	F(1, 132)	= 256.10
				Prob > F	= 0.0000
Total	7.83059445	133	.05887665	R-squared	= 0.6599
				Adj R-squared	= 0.6573
				Root MSE	= .14205

log_y	Coefficient	Std. err.	t	P>|t|	[95% conf.	interval]
DigitalInfrastructureAIIndex	-4.075624	.2546787	-16.00	0.000	-4.579404	-3.571845
_cons	2.11991	.0321705	65.90	0.000	2.056274	2.183546

```
. estat hettest

Breusch-Pagan/Cook-Weisberg test for heteroskedasticity
Assumption: Normal error terms
Variable: Fitted values of log_y

H0: Constant variance

    chi2(1) =   4.06
Prob > chi2 = 0.0439
```

Рисунок В.11 – Побудова лінійної регресії, де x - Digital Infrastructure Index та перевірка на гетероскедастичність

```
. regress log_y DigitalInfrastructureAIIndex, vce(robust)

Linear regression                               Number of obs     =        134
                                                F(1, 132)         =     226.27
                                                Prob > F          =     0.0000
                                                R-squared         =     0.6599
                                                Root MSE          =     .14205
```

log_y	Coefficient	Robust std. err.	t	P>|t|	[95% conf.	interval]
DigitalInfrastructureAIIndex	-4.075624	.2709447	-15.04	0.000	-4.61158	-3.539669
_cons	2.11991	.0311749	68.00	0.000	2.058243	2.181577

Рисунок В.12 – Побудова робастної регресії, де x - Digital Infrastructure Index