УДК 336.7:004.9]:001.891(477)(/047.31)
УКПП
№ державної реєстрації 0121U100467
Інв. №

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

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

_____ А.М.Чорноус

ЗВІТ
ПРО НАУКОВО-ДОСЛІДНУ РОБОТУ

Data-Mining для протидії кібершахрайствам та легалізації кримінальних доходів в умовах цифровізації фінансового сектору економіки України

ФОРМАЛІЗАЦІЯ ТА ОЦІНКА ЯКІСНИХ І КІЛЬКІСНИХ ПАРАМЕТРІВ ВИЗНАЧЕННЯ ПЕРЕДУМОВ ТА ДЕТЕРМІНАНТІВ ЗДІЙСНЕННЯ ЗЛОЧИННОЇ ДІЯЛЬНОСТІ У ФІНАНСОВОМУ СЕКТОРІ ЕКОНОМІКИ УКРАЇНИ

(проміжний)

Керівник НДР
д-рка. екон. наук, професорка О.В.Кузьменко

2021

Рукопис закінчено 15 грудня 2021 р.

Результати роботи розглянуті науковою радою СумДУ, протокол від 25.11.2021 р. № 5

СПИСОК АВТОРІВ

Керівник НДР – Головна наукова співробітниця, д-рка екон. наук, професорка	_____ 15.12.2021	О.В. Кузьменко (підрозділ 2.2, 2.4, 3.3)
Відповідальний виконавець, старша наукова співробітниця, канд. екон. наук	_____ 15.12.2021	В.В. Боженко (підрозділ 1.1, 1.2, 2.2, 2.3)
Виконавці: Старший науковий співробітник, доктор екон. наук	_____ 15.12.2021	А.О. Бойко (підрозділ 3.3)
Молодша наукова співробітниця, канд. екон. наук	_____ 15.12.2021	Т.В. Доценко (підрозділ 1.3)
Фахівчиня 1 категорії, канд. психол. наук	_____ 15.12.2021	Н.М. Теслик (підрозділ 3.1)
Виконавець за договором підряду, канд. екон. наук	_____ 15.12.2021	А.Ю. Семеног (підрозділ 2.4)
Виконавиця за договором підряду, канд. екон. наук	_____ 15.12.2021	О.М. Пахненко (підрозділ 1.1)
Виконавиця за договором підряду, канд. екон. наук	_____ 15.12.2021	Н.С. Ситник (вступ, підрозділ 2.1)
Виконавець за договором підряду, аспірант	_____ 15.12.2021	О.С. Кущнерьов (підрозділ 2.2, 2.3, 3.2, 3.3)

Виконавець за договором підряду, аспірант	_____ 15.12.2021	С.В. Миненко (підрозділ 2.4)
Виконавиця за договором підряду, аспірантка	_____ 15.12.2021	Я.С. Гарбар (підрозділ 1.3)
Виконавець за договором підряду, студент	_____ 15.12.2021	Є.І. Пігуль (підрозділ 1.1,1.2)
Виконавиця за договором підряду, студентка	_____ 15.12.2021	Л.О. Скринька (підрозділ 2.1)
Виконавиця за договором підряду, студентка	_____ 15.12.2021	К.Ю. Петренко (підрозділ 3.2)
Виконавиця за договором підряду, студентка	_____ 15.12.2021	А.Д. Кільдей (підрозділ 2.2)
Виконавиця за договором підряду, студентка	_____ 15.12.2021	М.М. Габенко (підрозділ 2.2)
Виконавиця за договором підряду, студентка	_____ 15.12.2021	Е.В. Шрамко (висновки)

РЕФЕРАТ

Звіт про НДР: 198 с., 23 табл., 60 рис., 3 дод., 91 джерело.

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

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

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

У процесі дослідження застосовувалися методи бібліометричного аналізу (з використанням інструментаріїв VOSviewer v.1.6.10 та SciVal by Elsevier), методи економіко-математичного моделювання (регресійнь модель на основі панельних даних, модель розподіленого лагу, SVM-моделі машинного навчання двох типів (epsilon-SVM regression та nu-SVM regression), лінійне програмування методом узагальненого знижуючого градієнту, багатоваріантні адаптивні регресійні сплайни, структурне моделювання, асоціативні правила, метод Парето, метод головних компонент, мультиплікативна згортка Кіні).

При виконанні НДР були отримані наступні нові наукові та прикладні результати: 1) вперше розроблено науково-методичний підхід до оцінювання каузальних зв'язків між розвитком фінтех інновацій, кількістю фінансових та кібернетичних правопорушень шляхом побудови багатомірних адаптивних регресивних MAR-сплайнів.; 2) вперше розроблено методологію формалізації факторів стрімкого поширення кіберзагроз, що базується на побудові сигмоїдної моделі із застосуванням методів машинного навчання SVM;

3) вперше розроблено методологію інтегрального оцінювання кібервразливості споживачів фінансових послуг шляхом системного поєднання за допомогою методів головних компонент, узагальненого знижуючого градієнту та мультиплікативної згортки Кіні; 4) досконалено методологічний базис обґрунтування причинно-наслідкових зв'язків між сумнівними фінансовими транзакціями.

Практичне значення одержаних результатів полягає у тому, що вони впровадженні у навчальний процес Сумського державного університету, що підтверджується актом впровадження від 23 грудня 2021 року, а саме використано у навчальний процес наукові праці з даної проблематики, розроблено практично-орієнтовані лабораторні роботи з дисципліни «Технології інтелектуальну аналізу даних» та «Прикладна економетрика».

У межах дослідження підготовлено та захищено 2 магістерські кваліфікаційні роботи: Пігуля Є.І. «Моделювання впливу цифровізації на розвиток фінансових технологій» [1] та Скриньки Л.О. «Економіко-математичне моделювання ефективності Національної системи протидії кібершахрайствам та легалізації кримінальних доходів на основі методів аналізу виживання» [2]; 1 кандидатської дисертації Доценко Т.В «Удосконалення системи фінансового моніторингу як інструмент забезпечення економічної безпеки національної економіки» [3], що й слугували частиною даного звіту. У межах даної науково-дослідної роботи здійснюється підготовка 2 кандидатських дисертацій (Миненко С.В., Кушнерьов О.С.), 1 докторської дисертації (Боженко В.В.).

ЗМІСТ

ВСТУП

У сучасному світі швидкий розвиток технологій, цифровізація фінансових відносин, популяризація та активне використання криптовалют для розрахунків вплинули на зростання кількості кібершахрайств у фінансовій сфері та збільшення нелегального відтоку коштів. Так впродовж останніх десятиліть спостерігається прискорення еволюції методів кібершахрайств та легалізації доходів, отриманих злочинним шляхом, які стають все більш розмаїтими. Механізми надання кримінальним доходам вигляду легальних прибутків та здійснення кіберзлочинів ускладняються і диверсифікуються. Відмивання незаконних доходів у світі все більшою мірою загрожує стабільності фінансової системи будь-якої країни, а також призводить до низки таких негативних наслідків суспільного характеру як втрата довіри населення до банківського сектору, крадіжка персональних даних клієнтів фінансових установ та нарощенню соціальної напруги загалом. Тож обрана проблематика є достатньо гострою та займає одне з провідних місць не лише в межах України, але й на міжнародній арені.

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

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

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

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

У межах дослідження підготовлено та захищено 2 магістерські кваліфікаційні роботи: Пігуля Є.І. «Моделювання впливу цифровізації на розвиток фінансових технологій» [1] та Скриньки Л.О. «Економіко-математичне моделювання ефективності Національної системи протидії кібершахрайствам та легалізації кримінальних доходів на основі методів аналізу виживання» [2]; 1 кандидатської дисертації Доценко Т.В «Удосконалення системи фінансового моніторингу як інструмент забезпечення економічної безпеки національної економіки» [3], що й слугували частиною даного звіту. У межах даної науково-дослідної роботи здійснюється підготовка 2 кандидатських дисертацій (Миненко С.В., Кушнерьов О.С.), 1 докторської дисертації (Боженко В.В.).

1 ВПЛИВ ЦИФРОВИХ ТРАНСФОРМАЦІЙ НА СИСТЕМУ ФІНАНСОВИХ ВІДНОСИН

1.1. Трансформація системи фінансових відносин під впливом цифровізації

Протягом останнього десятиліття фінансові установи фактично виконували роль своєрідних «першопроходців» в реалізації інноваційних рішень для удосконалення свого функціонування, заснованих на використанні цифрових технологій. Починаючи з автоматизації бізнес-процесів, запровадження онлайн-банкінгу, встановлення банківських терміналів самообслуговування та закінчуючи використанням штучного інтелекту для аналізу та моніторингу фінансових транзакцій, що загалом приносить вигоду як споживачам фінансових послуг, так і фінансовим установам. Встановлено, що до 2030 року ринок банківських послуг заощадить понад 1 трлн дол США за рахунок запровадження технологій штучного інтелекту та машинного навчання, що становить близько 22% витрат банківських установ [5]. Інтенсивний розвиток цифрових технологій трансформував ринок фінансових послуг, ставлячи нові виклики та загрози для подальшого функціонування традиційних фінансових установ. Встановлено, що із-за стрімкого розвитку інноваційних технологій фінансові компанії можуть втратити до третини свого доходу [6]. У даних умовах фінансові установ дедалі активніше починають співпрацювати з фінтех компаніями та інтенсивно інвестують кошти в модернізацію їх інфраструктури, оптимізацію бізнес-процесів, покращення якості фінансових послуг, а також підвищення рівня їх інформаційної безпеки.

Проведенням наукових досліджень окремих аспектів щодо розвитку інноваційних фінансових технологій та їх впливу на конкурентоспроможність фінансових установ, співпраці банків та фінтех компаній займаються такі вітчизняні вчені як А. Гулей [7], О. Луцишин [8], З. Руденко [9], П. Рубанов [10, 11, 12], А. Семеног [13], О. Шевченко [14] та інші. Розвиток

фінансових технологій є однією із головних тем для обговорення на міжнародних економічних форумах і конференціях, дана проблематика широко висвітлена у працях зарубіжних вчених. На думку С. Альбешр та Х. Нобані [15] блокчейн може повністю змінити та трансформувати банківські послуги, оскільки він має високий рівень безпеки, високу прозорість транзакцій, децентралізовану систему та може ефективніше здійснювати транзакції.

У роботі [16] оцінено вплив потенційних загроз та ризиків, спричинених стрімким зростанням інформаційних технологій, на стабільність функціонування фінансової системи. Проведений регресійний аналіз засвідчив, що за умови підвищення рівня системного ризику в країні відбувається зменшення позитивного ефекту від впровадження цифрових технологій на фінансову стабільність. Фрейм і Уайт [17] переконані, що фінансові інновації трансформують фінансовий сектор у трьох вимірах: нові продукти та / або послуги, нові процеси виробництва, та нові бізнес-моделі.

Окремої уваги заслуговує робота групи науковців [18], в якій запропоновано інтегральний показник для оцінювання рівня технологізації фінансових послуг на основі агрегування індикаторів, що характеризують рівень цифровізації суспільства, фінансової інклюзії населення та використання цифрового каналу для надання фінансових послуг. За результатами розрахунку даного інтегрального показника встановлено, що рівень технологізації фінансових послуг в Україні стабільно з кожним роком зростає, але суттєво відстає від європейських країн (у 2017 році: Україна – 17,7, Норвегія – 57,3%, Латвія – 40,4%).

За результатами проведення фронтірного аналізу встановлено, що збільшення обсягу інвестицій банків у розвиток власної цифрової інфраструктури стимулює зростання обсягу фінансових транзакцій через цифрові канали [19].

Розвиток цифрових технологій та акумулювання значного масиву даних дозволили технологіям fintech-кредитування стати потенційно

перспективним рішенням для зниження вартості позики та збільшення фінансової інклюзії. У роботі [20] для оцінювання платоспроможності клієнта використано методи машинного навчання, а саме: моделі на основі дерев рішень з різними алгоритмами побудови, векторні моделі та нейронні мережі. Крім цього, в іншому дослідженні [21] проведено оцінювання рівня кредитоспроможності позичальника на основі, по-перше, великих даних та моделей машинного навчання, по-друге, наданих фінансових даних клієнтом з використанням класичних банківських методик. Проведене емпіричне дослідження засвідчило, що фінтех підхід дозволяє побудувати більш точніший прогноз ризику невиплати коштів за позиками як у періоди економічної стабільності, так і в кризовий період. Таким чином, застосування інноваційних рішень для аналізу платоспроможності юридичних та фізичних осіб дозволяє удосконалити систему ризик-менеджменту банку та сформувати умови для стабільного його функціонування.

Поряд з фінансово-кредитними установами та фінтех компаніями на ринок банківських послуг поступово заходять нові гравці – BigTech компанії (великі IT компанії), початково розробляючи власні платіжні системи та розширюють спектр інноваційно-технологічних фінансових послуг [22, 23, 24,25].

Для дослідження впливу взаємодії фінтехкомпаній та банків використано методи якісного (SWOT та PEST матриці) та кількісного (коефіцієнти кореляції, регресійна модель) аналізу [26]. Отримані результати дослідження засвідчили, що на прикладі банківської системи Литви технологізація та інформатизація сприяє підвищенню ефективності його діяльності та вимагає посиленню співпраці між фінансовими установами та IT компаніями для задоволення потреб клієнтів. Автори даного дослідження наголошують, що для аналізу взаємоємозв’язку між банківськими та фінансовими технологіями, краще обирати методи якісного аналізу

Компанії, які розробляють гнучкі фінансові технології, можуть не тільки підвищувати ефективність діяльності фінансових компаніям, але також

допомагати національним регуляторам удосконалювати підходи у сфері пруденційного регулювання та нагляду, моніторингу шахрайських транзакцій, грошово-кредитної політики тощо [27]. Нині центральні банки багатьох країн світу здійснюють перехід від перевірок за участю працівників регулятора до автоматизованого, заснованого на алгоритмах навчання нейронних мереж.

Основними драйверами технологізації та цифровізації фінансових процесів є:

– потужний розвиток електронних обчислювальних машин, мобільних пристроїв дозволив підвищити швидкість обробки даних та отримати постійний доступ до фінансових послуг. Так, у 2019 році у світі нараховувалося близько 5,2 млрд мобільних користувачів, що охоплює 67% населення світу, тоді як у 2015 р.– 4,66 млрд, 2010 р. – 3,219 млрд осіб [2828].

– збільшення інвестицій у розвиток фінтех інновацій. Протягом 2018-2020 рр. середньорічний обсяг глобальних інвестицій у секторі фінтех становив 140 млрд дол США, для порівняння у 2017 р. – 59,2 млрд дол США, а 2012 р. – 4 млрд дол США [29].

– зростання масштабів електронної комерції, що вимагає здійснення безготівкових грошових розрахунків за торговими операціями.

– запровадження клієнтоорієнтованого обслуговування та покращення фінансової інклюзії населення.

– збільшення кількості користувачів соціальних мереж, які акумулюють значний обсяг персональної інформації, що використовується в подальшому для оцінки споживчих вподобань, а також слугують ефективним каналом просування інноваційних фінансових продуктів. Відповідно до Emarketer рівень проникнення соціальних мереж у світі у 2020 р. становив 41,9% від загальної кількості населення або 3,23 млрд користувачів. Для порівняння: у 2017 р. – 2,3 млрд користувачів або 31,2%, у 2013 р. – 1,6 млрд користувачів або 22,8% [30].

– ліберальна та стимулююча політика регулюючих фінансових органів у різних країнах світу у сфері розвитку інноваційних фінансових технологій

шляхом налагодження комунікації між фінтех компаніями та регуляторами, удосконалення платіжної інфраструктури, встановлення пільгового режиму оподаткування, легалізація розрахунків з криптовалютою тощо.

Фахівці PwC розглядають фінансові технології (фінтех) як динамічно розвиваючий сегмент на перетині секторів фінансових послуг і технологій, в якому фінансові установи, технологічні стартапи і нові учасники фінансового ринку застосовують інноваційні підходи до продуктів і послуг [30].

Основними передовими технологіями є штучний інтелект, блокчейн, Big Data, хмарні технології, Інтернет речей, автоматизація роботизованих процесів, біометричні технології, технології віртуальної реальності тощо.

Під Big Data доцільно розуміти сукупність структурованих та неструктурованих даних, що прямо або опосередковано мають відношення до досліджуваного об'єкта. Дані можуть бути використані на будь-якому етапі життєвого циклу фінансової установи: визначення цільової аудиторії та вартості фінансової послуги, оцінка рівня кредитоспроможності позичальника, розробка політики просування та продажу фінансової послуги на ринок, ідентифікація шахрайських транзакцій тощо. Таким чином, аналіз великих даних дозволяє залучити нових клієнтів, а потім утримати їх, максимально задовольняючи їх очікування та прогнозуючи їх поведінку. Встановлено, що до 2030 року ринок банківських послуг заощадить понад 1 трлн дол США за рахунок запровадження технологій штучного інтелекту та машинного навчання, що становить близько 22% витрат банківських установ [5]. Прикладами використання штучного інтелекту в банківській сфері є:

– запровадження чат-ботів, які надають автоматизовану допомогу на вимогу (наприклад, відповідь на найбільш поширені питання), здійснюють обслуговування банківських рахунків тощо;

– система управління відносинами з клієнтами (CRM), що передбачає автоматизацію взаємодії з споживачами фінансових установ та задоволення їх потреб;

– система для оцінювання ризику використання фінансових установ для здійснення шахрайських транзакцій. За даними дослідження [19], проведеного Асоціацією сертифікованих експертів з питань шахрайства, у 2019 році 13% компаній вже використовують штучний інтелект для боротьби з фінансовою злочинністю.

Враховуючи переваги технології розподіленого реєстру (блокчейну), фінансові установи дедалі частіше використовують дану технологію баз даних, яка дозволяє створювати, забезпечувати безпечну передачу та зберігати інформацію. Варто відзначити, що дана технологія не контролюється та не заадмініструється централізовано. Блокчейн використовується для створення інтелектуальних контрактів або домовленостей, які автоматично виконують узгоджену транзакцію при дотриманні певних умов. Це дозволяє зберігати будь-яку цифрову інформацію та дозволяє стороні отримувати доступ або змінювати дані лише відповідно до набору заздалегідь визначених правил. Крім цього, блокчейн збільшує швидкість обробки транзакцій.

Хмарні технології забезпечують економічну та відносно легко масштабовану обробку даних на вимогу, що дозволяє мінімізувати операційні витрати фінансових установ, побудувати комплементарну систему інформаційної безпеки, а також підвищити гнучкість управлінських заходів до викликів зовнішнього середовища.

Автоматизація є особливо важливою складовою цифрової трансформації для фінансових компаній. Сфера фінансових послуг ґрунтується на трансакціях, що генерують великі обсяги даних, і тому їх автоматична обробка дозволяє підвищити ефективність та рентабельність своєї діяльності.

Біометричні технології передбачають розпізнавання фізіологічних або поведінкових характеристик, які можуть бути використані для автентифікації особи шляхом виявлення характеристик, унікальних для окремих людей. Серед методів, які зараз використовуються для перевірки, є сканування

відбитків пальців, аутентифікація голосу, розпізнавання обличчя, сканування райдужної оболонки та розпізнавання ходи

Вплив діджиталізації на розвиток основних фінансових технологій представлено в таблиці 1.1.

Таблиця 1.1 – Вплив цифровізації на розвиток фінансових технологій

	Основні фінансові послуги				Внутрішні бізнес-процеси	
	Грошові розрахунки та перекази	Фінансування	Послуги з управління капіталом	Страхування	Комунікація з клієнтами	Безпека та захист
Вплив цифрових технологій	БЛК	БЛК, ВД, ХТ	БЛК, ВД, ШІ, ВР	БЛК, ВД, ШІ, БМ	БЛК, ВД, ШІ, ВР	БЛК, ВД, БМ
Види фінансових технологій	Сервіси онлайн-платежів, сервіси онлайн-переказів, Р2Р- платежі, криптовалюта, мобільні та web гаманці	Р2Р споживче кредитування, Р2Р бізнес-кредитування, краудфандинг, удосконалення скорингової моделі	робоедвайзінг, застосунки з фінансового планування, платформи для соціального трейдингу, алгоритмічна біржова торгівля	цифрове страхування, платформи для перестрахування, удосконалення андерайтингу, Р2Р страхування	чат-боти, персональні повідомлення-нагадування	шифрування даних, удосконалення процедури аутентифікації та авторизації.
БЛК – блокчейн; ВД - великі неструктуровані дані; ХТ - хмарні технології; ШІ - штучний інтелект, БМ- біометричні технології; ВР - технології віртуальної реальності.						

Джерело: складено на основі [10, 13, 5, 32]

Пандемія COVID-19 також внесла свої корективи в функціонування національних фінансових системи у всьому світі, включаючи надання цифрових фінансових послуг та організацію роботу ринку FinTech. Введення численних карантинних обмежень та соціальне дистанціювання актуалізувало необхідність використання цифрових каналів надання фінансових послуг, а так інших послуг у сфері електронної комерції.

Фахівцями Світового Банку проведено ґрунтовне дослідження впливу пандемії COVID-19 на зміни у регуляторному середовищі діяльності фінтех компаній у різних країнах світу. Дане дослідження ґрунтувалося на основі

даних про опитування представників зі 118 національних регуляторних органів світу у фінансовій сфері. За даними дослідження встановлено, що в період пандемії відбулося збільшення використання продуктів FinTech у світі. Зокрема, 65% респондентів у розвинутих країнах світу повідомили про зростання цифрових платежів та грошових переказів, тоді як у країнах, що розвиваються – лише 50 % (рис. 1.1). Варто відзначити, що інтенсивність нарощення послуг у сфері цифрового страхування та інвестування є вищою у країнах з економікою, що розвивається.

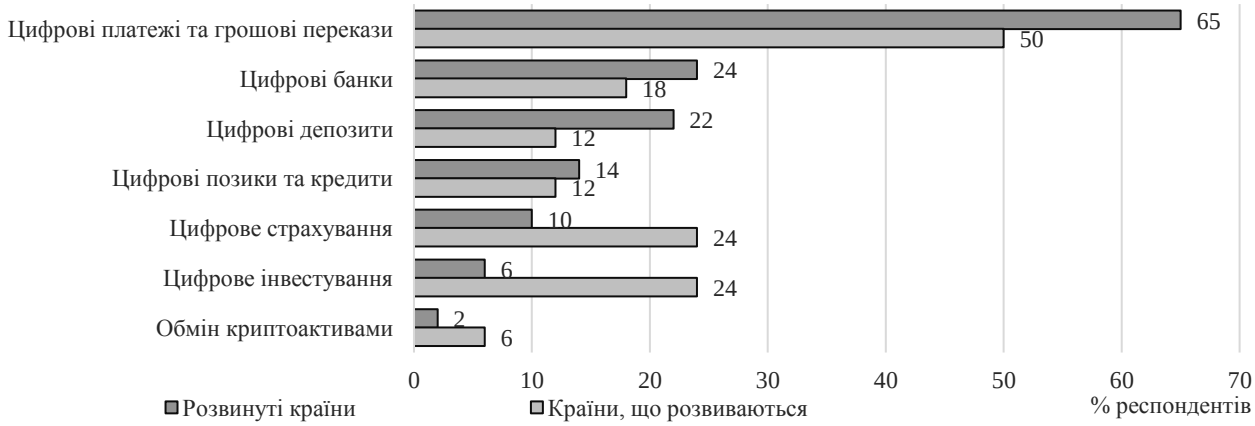


Рисунок 1.1 – Частка респондентів, які повідомили про збільшення використання продуктів FinTech у період пандемії

Джерело: складено на основі [33]

Однією з ключових загроз діджиталізації є збільшення частоти та масштабів кібершахрайств, що мають негативні наслідки для стабільного функціонування надавачів фінансових послуг та їх споживачів, а саме: втрата інформації, відсутність доступу до неї, несанкціоноване втручання у роботу корпоративних інформаційних систем, розповсюдження персональної фінансової інформації про клієнтів тощо. Крім цього, наслідком шахрайських дій кіберзлочинців є репутаційні втрати фінансових установ та зменшення довіри населення до безпечності та надійності здійснення фінансових транзакцій як за участю конкретної фінансової установи, так і фінансової

системи загалом. Зокрема, під час пандемії кількість порушень у сфері кібербезпеки серед FinTech компаній в середньому збільшився на 17% [3433].

Таким чином, зростання кількості користувачів мобільних пристроїв, поширення проникнення інтернету, стрімке нарощення обсягів електронної комерції, а також світова пандемія призвели до збільшення попиту на цифрові фінансові продукти. За даних умов активна участь держави в розвитку цифрових технологій на фінансовому ринку є одним з основних факторів розвитку цифрової економіки. Для ефективного і безпечного розвитку і функціонування цифрового фінансового простору необхідна реалізація скоординованих заходів на рівні всіх його учасників, яке буде, з одного боку, підтримувати стабільність фінансової системи і захищати права споживачів, а з іншого - сприяти розвитку та впровадженню цифрових інновацій.

1.2. **Моделювання впливу діджиталізації на розвиток фінансових технологій**

На сьогоднішній день цифровізація стала глобальним стратегічним пріоритетом для розвитку фінансових установ. Драйвером змін, що відбуваються на фінансових ринках, є сучасні фінансові технології. Масове впровадження цифрових технологій створює додаткові можливості для розвитку фінансових установ за рахунок оптимізації управлінських та операційних витрат, удосконалення механізму взаємодії з клієнтами, покращення якості системи ризик-менеджменту тощо. Водночас, слід врахувати, що поява нового практично безбар’єрного глобального середовища взаємодії несе в собі і певні загрози для учасників фінансової системи. Зокрема, до основних загроз слід віднести ризик порушення процесів, витік конфіденційних даних, а також банкрутсво окремих фінансових установ із-за посилення конкуренції на ринку фінансових послуг. Виходячи з цього, у межах даного дослідження цифровізацію будемо розглядати з позиції стимулятора та інгібітора розвитку фінансових установ.

Для характеристики стану впровадження цифрових технологій у різні сфери суспільного життя в країні існує значна кількість індикаторів. Виходячи з цього, для потреб даного дослідження запропоновано здійснити відбір найбільш значущих показників, які відображають зміни у інтенсивності використання інформаційних технологій в діяльності органів державної влади, суб'єктів господарювання, а також індивідумів.

Зауважимо, з метою дослідження діджиталізації як драйвера та інгібітора розвитку фінансових технологій, а також беручи до уваги відсутність належної статистичної бази за тривалий період часу, у роботі вирішено побудувати декілька економіко-математичних моделей: модель з розподіленим лагом та панельна регресійна модель.

Математичні розрахунки та побудову моделі було здійснено використовуючи програмний пакет STATISTICA та Eviews. Зазначені програми зручні у використанні та завдяки вбудованим функціями, інструментам дослідження полегшить процес проектувальних розрахунків.

Оскільки питання діджиталізації та його вплив на різні сфери суспільного життя стало актуальним тільки протягом останніх років, тому формування достатньої за обсягом інформаційної бази для дослідження є одним із головних викликів проведеного дослідження. Одним із шляхів вирішення даної проблеми є моделювання на основі панельних даних.

Панельна регресійна модель передбачає використання даних, які відображають іфнормацію про одну і ту ж множину об'єктів за ряд послідовних періодів часу. Отже, панельні дані це комбінація просторових даних (cross – sectional data) та даних часових рядів (time – series data) [3635, 36].

Панельні дані дозволяють аналізувати і виокремлювати зміни на індивідуальному рівні кожного об'єкта. Перевагою даного підходу є акумулювання великої кількості статистичних спостережень, що дозволяє збільшити число ступенів свободи і зменшити залежність факторів за рахунок того, що враховуються індивідуальні особливості залежних змінних. Отже,

виходять оцінки за результатами економіко-математичного моделювання, які є більш ефективними.

У загальному вигляді модель з панельними даними може бути предствлена як [35]:

$$Y_{it} = \alpha + X_{it}\beta_{it} + \varepsilon_{it} \quad (1.1)$$

де Y_{it} – значення досліджуваного показника для і-го об'єкта в і-й період часу;

X_{it} – вектор порядку пояснюючих змінних (факторів);

ε_{it} – збурення для і-го об'єкта в і-й період часу;

α –скаляр;

β_{it} –параметри моделі, що вимірюють часткові ефекти від зміни X_{it} в період t для певного і.

Модель (1..) має загальний вигляд, тому доцільно ввести додаткові обмеження на параметри моделі. Стандартним припущенням, дійсним для багатьох емпіричних ситуацій, є припущення постійності параметрів β_{it} для всіх значень t та і. За таких умов модель (1.1) набуває вигляду:

$$Y_{it} = \alpha + \beta_1 X_{1it} + \beta_2 X_{2it} + \cdots + \beta_k X_{kit} + \varepsilon_{it} \quad (1.2)$$

Модель (1.2) є загальною моделлю панельних даних (pooled model). Побудова, оцінювання параметрів та дослідження такої моделі відбувається як при класичних багатофакторних регресійних моделей. Відзначимо, що дана специфікація не враховує індивідуальні особливості об'єктів, що вивчаються (у межах даного дослідження – країн).

Економетричні моделі на основі панельних даних залежно від поведінки компоненти збурень розподіляються на моделі з фіксованими ефектами та моделі з випадковими ефектами.

Модель панельних даних з фіксованими ефектами (fixed effects models) має наступний загальний вигляд:

$$Y_{it} = \mu_i + \beta \ \ X_{it} + u_{it} \quad (1.3)$$

Крім того, припускається, що всі X_{it} незалежні від всіх u_{it}, а збурення u_{it} є незалежними однаково розподіленими випадковими величинами з математичним сподіванням нуль та постійною дисперсією.

Модель з фіксованими ефектами доцільно застосовувати до даних, якщо існує потреба врахування неспостережуваних факторів, які відрізняються для різних моментів часу.

У випадку, якщо μ_i представляється собою як реалізації незалежних від випадкових величин X_{it} з середнім розподілом α_i та дисперсією, то модель (1.3) відноситься до класу моделей панельних даних з випадковими ефектами (random effects models):

$$Y_{it} = \alpha + \beta \ \ X_{it} + \mu_i + u_{it} \quad (1.4)$$

Оцінка параметрів за побудованими моделями з панельними даними може проводитися за допомогою методу 1МНК. Для встановлення найбільш адекватної моделі використовуються тести Вальда, Бройша–Пагана, Хаусмана.

Крім цього у роботі запропоновано методичні засади для оцінювання закономірностей між масштабами кібершахрайств та розвитком інформаційних технологій на основі побудови моделі з розподіленим лагом. Дана модель містить в якості лагових змінних незалежні (екзогенні) змінні. Для характеристики стримуючого впливу діджиталізації на розвиток фінансових відносин обрано таку змінну як кількість кібершахрайств. Даний підхід передбачає врахування певної часової затримки (лагу) між розвитком

цифрових технологій та масштабами кіберзлочинності. Оскільки статистична інформація про обсяги кібершахрайств у вільному доступі представлена тільки для однієї європейської країни – Бельгії, тому модель з розподіленим лагом побудовано виключно для цієї країни.

Загальний вигляд моделі з розподіленим лагом має наступний вигляд [3737]:

$$Y_t = \delta + \beta_0 X_t + \beta_1 X_{t-1} + \beta_2 X_{t-2} + \cdots + \beta_T X_{t-T} + \varepsilon_t \quad (1.5)$$

Послідовність вагових коефіцієнтів, β_1, β_2, β_T називається структурою лагу. Відповідно до методу Алмона структура лагу описується поліномом другого ступеня:

$$\beta_j = c_0 + c_1 j + c_2 j^2 \quad (1.6)$$

Реалізація запропонованого методичного підходу до оцінювання впливу діджиталізації на розвиток фінансових технологій буде здійснюватися поетапно, що представлено на рисунку 1.2.

Оскільки метою побудови моделювання є використання її результатів для ухвалення науково обгрунтованих рішень, тому вкрай важливим є дотримання етапів реалізації економетричної моделі та економічна інтерпретація отриманих закономірностей.

Побудова економіко-математичних методів можлива за наявності якісних інформаційних ресурсів, що повноцінно характеризують процеси з діджиталізації. Беручи до уваги особливості бізнес-середовища, можливості і загрози від впровадження інформаційних технологій у сферу фінансових відносин, необхідно створити повноцінну та якісну, достатньо структуровану інформаційно-аналітичну базу для прийняття науково обгрунтованих управлінських рішень.

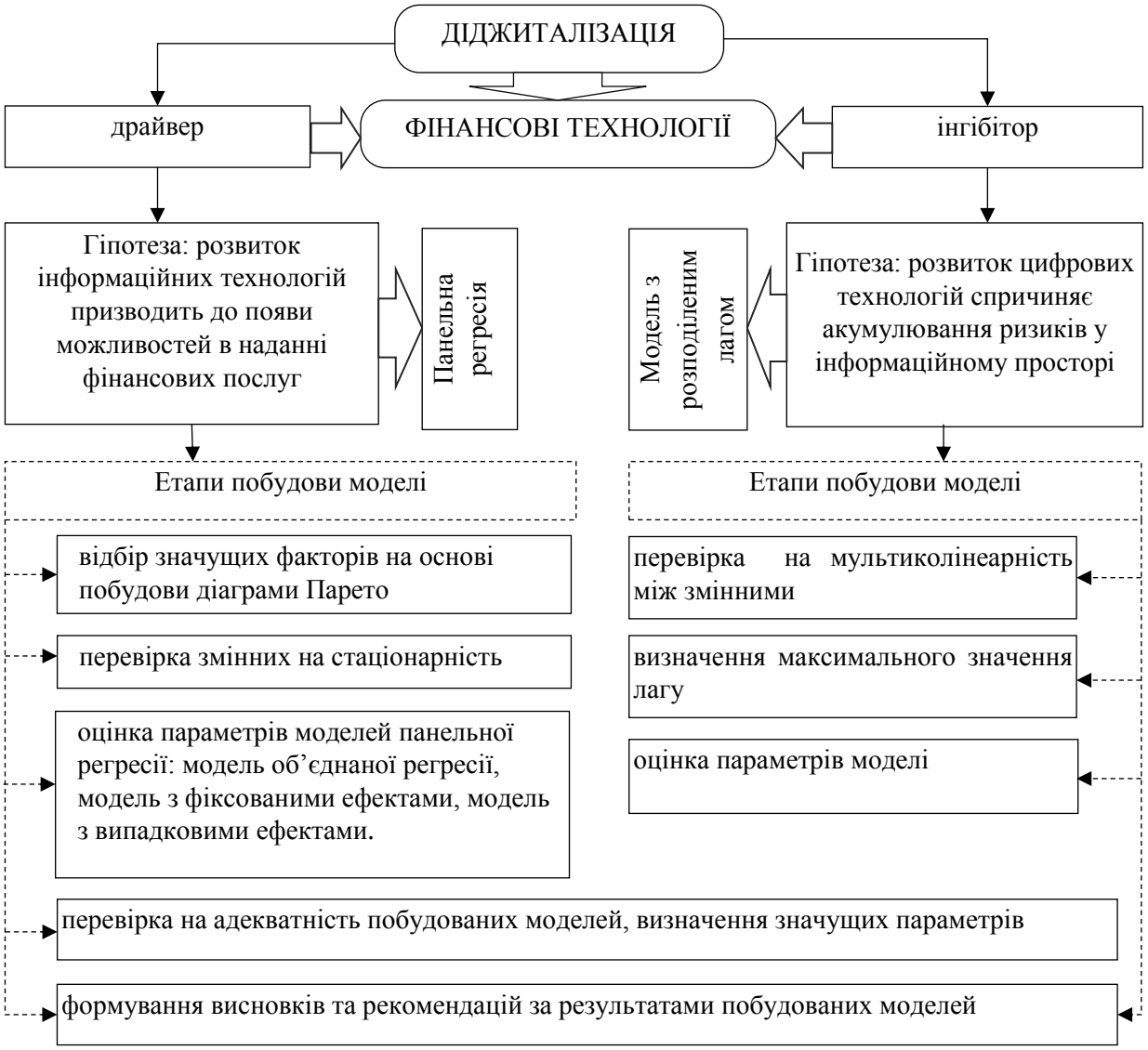


Рисунок 1.2 – Етапи оцінювання впливу діджиталізації на розвиток фінансових технологій

Для характеристики рівня розвитку фінансових технологій у розрізі різних країн світу обрано наступні індикатори: рівень використання електронного банкінгу, рівень використання фінансових послуг онлайн (купівля-продаж акцій, облігацій та інших інвестиційних активів), кількість випадків з кібершахрайства.

Водночас цифровізацію економіки запроновано аналізувати на основі таких індикаторів як: рівень доступу до мережі Інтернет серед домогосподарств, рівень використання Інтернету фізичними особами, рівень

інтернет-покупок, рівень електронного урядування, частка підприємств, які здійснюють e-commerce продажі, рівень електронної комерції (e-commerce), рівень використання комп'ютерних технологій та інтернету працівниками компаній, рівень інтеграції внутрішніх систем, частка підприємств, які проводили навчання для розвитку / підвищення кваліфікації інформаційно-комунікативних технологій персоналу, рівень зайнятого населення у сфері інформаційно-комунікативних технологій, рівень використання веб-сайтів, частка сфери інформаційно-комунікативних технологій у ВВП країни.

Інформаційною базою побудованої моделі слугуватимуть річні дані, опис яких наведено в таблиці 1.2 із зазначенням можливого діапазону коливань обраних показників та джерел їх збору.

Для вирішення поставлених задач акумульована сбалансована панель даних у розрізі 23 країн Європейського Союзу протягом 2014-2019 рр.

Таким чином, достовірність, об'єктивність та повнота отриманих результатів залежать від вибору інформаційної бази для дослідження, а також від попередньої обробки статистичної інформації. На основі вищезазначених індикаторів будуть сформовані вхідні параметри моделі, що дозволить визначити змінні для оцінювання закономірностей розвитку фінансових технологій від впливом діджиталізації.

Вагому роль при побудові економетричної моделі є відбір значущих для моделі вхідних ознак. Скорочення числа незалежних змінних дозволяє зменшити розмірність моделі, а саме нівелювати вплив незначущих індикаторів та усунути надлишкові ознаки. Дублювання інформації у вигляді схожих за економічним змістом показників не тільки не покращує якість моделі, але і часом, навпаки, погіршує його (наприклад, у випадку з мультіколінеарністю).

Таблиця 1.2 – Опис показників вхідних даних

Показник	Умовне позначення	Шкала вимірювання	Допустимі значення	Джерело
Рівень доступу домогосподарств до мережі Інтернет	INT_H	% від домогосподарств	(0;100)	Eurostat
Рівень використання фізичними особами Інтернету	INT_I	% від фізичних осіб	(0;100)	Eurostat
Рівень інтернет-покупок	IP_I	% від фізичних осіб	(0;100)	Eurostat
Рівень електронного урядування	EG_I	% від фізичних осіб	(0;100)	Eurostat
Частка підприємств, які здійснюють e-commerce продажі	ECM_E	% підприємств	(0;100)	Eurostat
Рівень електронної комерції	ECM	% продажів	(0;100)	Eurostat
Рівень використання комп'ютерних технолоій та інтернету працівниками компаній	INT_EM	% від зайнятого населення	(0;100)	Eurostat
Рівень інтеграції внутрішніх систем	IIP	% підприємств	(0;100)	Eurostat
Частка підприємств, які проводили навчання та підвищення кваліфікації персоналу інформаційно-комунікативним технологіям	TR_E	% підприємств	(0;100)	Eurostat
Рівень зайнятого населення у сфері інформаційно-комунікативних технологій	EMP	% від зайнятого населення	(0;100)	Eurostat
Рівень використання веб-сайтів	WEB	% підприємств	(0;100)	Eurostat
Частка сфери інформаційно-комунікативних технологій у ВВП	ICT/GDP	%	(0;+∞)	Eurostat
Рівень інтернет банкінгу	INR	% від фізичних осіб	(0;100)	Eurostat
Рівень використання фінансових послуг онлайн	FIN	% від фізичних осіб	(0;100)	Eurostat
Кількість випадків з кібершахрайства	CC	шт	(0;+∞)	Statista

З поміж значної кількості підходів до відбору значущих змінних для включення їх в економетричну модель нами побудовано діаграму Парето методом сигма-обмеженої параметризації. Вхідною інформаційною базою для побудова діаграми Парето є індикатори для характеристики рівня цифровізації економіки, що представлено в таблиці 1.2. Для потреб даного виду аналізу необхідним є визначення результативного показника, яким обрано частку

сфери інформаційно-комунікативних технологій у ВВП. Варто відзначити, що об’єктом дослідження взято загальні дані 28 країн ЄС. Вхідна статистична база подана в таблиці 1.3.

Таблиця 1.3 – Вхідна інформаційна база для відбору значущих індикаторів для характеристики рівня цифровізації

	INT_H	IP_I	EG_I	IIP	TR_E	EMP	ECM	WEB	ICT to GDP
2011	72,0	29,0	41,0	23,0	16,0	3,0	13,0	98,0	4,1
2012	75,0	31,0	44,0	24,0	18,0	3,2	14,0	70,0	4,0
2013	77,0	33,0	42,0	29,0	20,0	3,3	13,0	72,0	3,9
2014	80,0	36,0	46,0	34,0	21,0	3,4	14,0	73,0	4,1
2015	81,0	38,0	46,0	38,0	21,0	3,5	16,0	74,0	4,1
2016	84,0	41,0	48,0	37,0	21,0	3,6	16,0	76,0	4,2
2017	86,0	44,0	49,0	36,0	22,0	3,7	18,0	76,0	4,4
2018	88,0	46,0	51,0	36,0	23,0	3,8	17,0	76,0	4,5
2019	90,0	49,0	53,0	36,0	20,0	3,9	18,0	77,0	4,5
2020	91,0	54,0	57,0	35,0	20,0	4,3	20,0	77,0	4,7

Діаграма Парето дозволяє отримати візуалізацію за допомогою значень t-критерію Стьюдента пріоритетності показників. Даний підхід відноситься до одного із одномірних тестів значущості. Актуалізація даного інструментарію проводиться шляхом виконання команди Statistics, Advanced Linear/Nonlinear Models, GRM Results у програмі Statistica. На рисунку 1.3 представимо результати побудови одномірного тесту значущості впливу показників, що характеризують рівень цифровізації економіки, на результативний показник – частка сфери інформаційно-комунікативних технологій у ВВП.

Аналізуючи рисунок 1.3, можна зробити висновки, що на рівні 5% відхилення (допустимого в більшості випадків для економічних досліджень) значущим виступає 5 показників: рівень доступу домогосподарств до мережі Інтернет (INT_H), рівень інтернет-покупок (IP_I), рівень електронного урядування (EG_I), частка підприємств, які проводили навчання та підвищення кваліфікації персоналу інформаційно-комунікативним технологіям (TR_E), рівень зайнятого населення у сфері інформаційно-комунікативних технологій (EMP). Для вищезазначених показників

найбільшою є як сума квадратів відхилень SS, так майже нульова ймовірність відхилення гіпотези про недоцільність використання даних індикаторів для характеристики цифровізації економіки.

Effect	Parameter Estimates (Spreadsheet2) Sigma-restricted parameterization									
	ICT_GDP Param.	ICT_GDP Std.Err	ICT_GDP t	ICT_GDP p	-95,00% Cnf.Lmt	+95,00% Cnf.Lmt	ICT_GDP Beta (?)	ICT_GDP St.Err.?	-95,00% Cnf.Lmt	**+95,00% Cnf.Lmt**
Intercept	22,012	1,134	19,409	0,033	7,601	36,422				
INT_H	-0,247	0,014	-17,676	0,036	-0,425	-0,069	-6,214	0,352	-10,681	-1,747
IP_I	0,374	0,020	19,070	0,033	0,125	0,624	11,859	0,622	3,957	19,761
EG_I	0,055	0,002	25,229	0,025	0,027	0,082	1,057	0,042	0,525	1,589
IIP	0,007	0,001	6,049	0,104	-0,008	0,023	0,155	0,026	-0,171	0,482
TR_E	0,063	0,003	23,068	0,028	0,028	0,098	0,488	0,021	0,219	0,757
EMP	-4,033	0,197	-20,429	0,031	-6,542	-1,525	-5,900	0,289	-9,570	-2,230
ECM	-0,055	0,005	-11,287	0,056	-0,118	0,007	-0,512	0,045	-1,088	0,064
WEB	-0,016	0,001	-11,676	0,054	-0,034	0,001	-0,494	0,042	-1,032	0,044

Рисунок 1.3 – Одномірний тест значущості впливу показників, що характеризують рівень цифровізації економіки, на результативний показник

Візуальне представлення отриманих результатів представлено шляхом побудови діаграми Парето (рис.1.4).

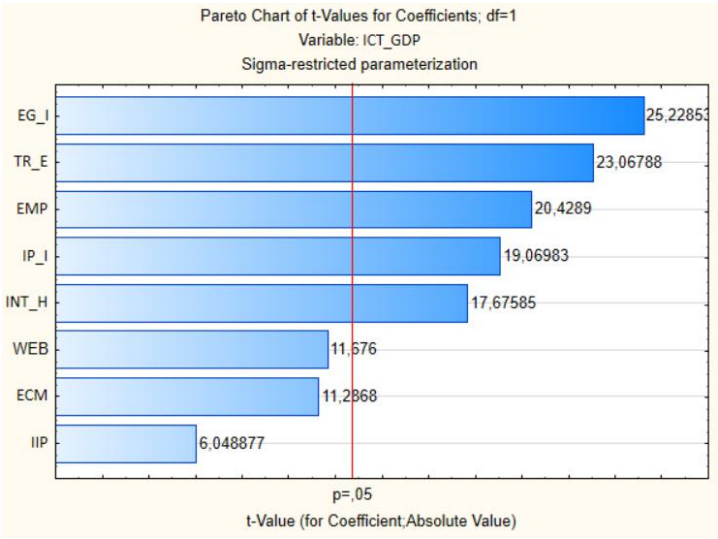


Рисунок 1.4 – Діаграма Парето t-значень значущості впливу показників показників, що характеризують рівень цифровізації економіки, на результативний показник

На основі даних рисунку 1.4 щодо діаграми Парето проведемо ранжування значущості врахування вхідних показників для подальшого їх

включення в економетричну модель. Так, ранг 1 – EG_I; ранг 2 – TR_E; ранг 3 – EMP; ранг 4 – IP_I; ранг 5 – INT_H. Таким чином, дані індикатори в наступному розділі кваліфікаційної роботи будуть використовуватися для побудови економетричної моделі.

Згідно з основними етапами розробленої структурно-логічної схеми дослідження (рис. 1.2), нами попередньо визначені 5 найбільш значущих індикаторів, що відображають процеси з цифровізації економіки, та розроблено модель оцінювання впливу цих індикаторів на розвиток фінансових технологій. У межах побудови моделі на панельних даних для характеристики розвитку фінансових технологій обрано такі індикатори як рівень інтернет банкінгу та рівень використання фінансових послуг онлайн.

Всі змінні, які включені до складу економетричної моделі, були прологарифмовані з метою підвищення нормальності розподілу залишків та мінімізації стандартних помилок моделі. Усі математичні розрахунки здійснено в програмі Eviews.

Однією з основних вимог до побудови економетричної моделі є використання стаціонарних часових рядів. Для перевірки наявності одиничних коренів в панельних даних використовують різноманітні тести: Левіна-Ліна-Чу, Хадрі, Песаран та Чін, панельних аналогів тестів Дікі-Фуллера.

Перевірка наявності одиничного кореня в панельних даних передбачає тестування нульової гіпотези, яка передбачає, що ряд є стаціонарним за умови $p<0,05$. Результати перевірки тестів на стаціонарність представлено в таблиці 1.4, а проміжні результати на рисунках А.1-А.16, додатку А.

За результатами проведених двох тестів на перевірку стаціонарності встановлено, що за окремими змінними отримано протилежні результати. Зокрема, змінна «рівень доступу домогосподарств до інтернету (INT_H)» за результатами розрахунку Левіна-Ліна-Чу є стаціонарною, тоді як за критерієм Песаран та Чін стаціонарною стала тільки після взяття перших різниць. Таким чином, при подальших розрахунках використано результати двох тестів.

Для забезпечення конкурентних переваг на національному ринку фінансових послуг та сприяння впровадженню інноваційних рішень при реалізації фінансових послуг необхідно визначити найбільш значущі фактори впливу на розвиток фінансових технологій. Для вирішення цього завдання нами використано методи аналізу панельних даних.

Таблиця 1.4 – Результати тестування панельних даних на наявність одиничного кореня

Показник		Levin, Lin & Chu Test		IM, Pesaran and Shin Test		Висновок
		статистика	p-значимість	статистика	p-значимість	
INT_H	факт	-14,0791	0,0000*	-0,28284	0,3887	перший рівень інтегрування
	перші різниці	-	-	-5,44429	0,0000*	
IP_I	факт	-2,69251	0,0035	2,14886	0,9842	перший рівень інтегрування
	перші різниці	-20,4992	0,0000*	-4,66234	0,0000*	
EG_I	факт	-14,9320	0,0000*	-1,51229	0,0652	перший рівень інтегрування
	перші різниці	-	-	-20,4282	0,0000*	
TR_E	факт	-13,6501	0,0000*	-3,46928	0,0003*	відсутнє інтегрування
	перші різниці	-	-	-	-	
EMP	факт	-3,83240	0,0001*	1,30455	0,9040	перший рівень інтегрування
	перші різниці	-	-	-2,26104	0,0119*	
INR	факт	2,30322	0,9894	4,27265	1,0000	перший рівень інтегрування
	перші різниці	-18,7269	0,0000*	-7,92860	0,0000*	
FIN	факт	-28,9839	0,0000*	-5,78314	0,0000*	відсутнє інтегрування
	перші різниці	-	-	-	-	
CBB	факт	1,49475	0,9325	3,53027	0,9998	перший рівень інтегрування
	перші різниці	-9,39328	0,0000*	-1,96463	0,0247*	

* - ряд є стаціонарним.

Для здійснення розрахунків сформовано масив панельних даних за 6 років (2014-2019) у розрізі 23 країн ЄС, що дозволило за кожним із аналізованих показників отримати 138 спостережень (таблиця Б.1, додаток Б).

У роботі запропоновано використовувати 2 залежні змінні, що відображають стан розвитку фінансових технологій: рівень інтернет банкінгу (INR) та рівень використання фінансових послуг онлайн (FIN). Тоді як незалежними змінними, які доцільно включити в економетричну модель, виходячи з результатів побудови діаграми Парето (п. 2.3), є: рівень доступу домогосподарств до мережі Інтернет (INT_H), рівень інтернет-покупок (IP_I),

рівень електронного урядування (EG_I), частка підприємств, які проводили навчання інформаційно-комунікативним технологіям власного персоналу (TR_E), рівень зайнятого населення у сфері інформаційно-комунікативних технологій (EMP).

З урахуванням перевірки на стаціонарність вхідних змінних, отримаємо моделі наступного вигляду:

$$lnINR_{rt}(1) = a_r + a_1 lnINT\_H_{rt}\ (1) + a_2 lnIP\_I_{rt}\ (1) + a_3 lnEG\_I_{rt}(1) + a_4 lnEMP_{rt}(1) + a_5 lnTR\_I_{rt} + u_{rt} \quad (1.7)$$

$$lnFIN_{rt} = b_r + \beta_1 lnINT_{H_{rt}}(1) + \beta_2 lnIP_{I_{rt-1}}(1) + \beta_3 lnEG\_I_{rt} + \beta_4 lnEMP_{rt}(1) + \beta_5 lnTR_{I_{rt}}(1) + u_{rt} \quad (1.8)$$

де ar, br – фіксовані ефекти r-ї країни;

urt – випадкова величина; r = 1,…,23; t = 1,…,6.

Коефіцієнти логарифмічно-лінійних моделей (1.7) – (1.8) відображають ступінь еластичності за відповідними факторами та показують на скільки відсотків змінюється залежна змінна зі збільшенням незалежної змінної на 1% за умови, що всі інші фактори залишаються незмінними. У табл. 1.5 наведено результати оцінювання панельних регресій трьох типів: загальна модель панельних даних (pooled model), модель панельних даних з фіксованими ефектами (fixed effects models), модель панельних даних з випадковими ефектами (random effects models).

На основі даних таблиці 1.5 запишемо математичну формалізацію даних взаємозв’язків:

– загальна модель панельних даних:

$$lnINR_{rt}(1)_g = 1{,}081lnINT_{H_{rt}}\ (1) + 0{,}253lnIP_{I_{rt}}\ (1) + 0{,}024lnEG\_I_{rt}(1) - 0{,}024lnEMP_{rt}(1)\ - 0{,}075lnTR_{I_{rt}} + 0{,}047 \quad (1.9)$$

– модель панельних даних з фіксованими ефектами:

$$lnINR_{rt}(1)_f = 0{,}972lnINT_{H_{rt}}\ (1) + 0{,}279lnIP_{I_{rt}}\ (1) + 0{,}087lnEG\_I_{rt}(1) + 0{,}051lnEMP_{rt}(1)\ - 0{,}065lnTR_{I_{rt}} - 0{,}056 \quad (1.10)$$

– модель панельних даних з випадковими ефектами:

$$lnINR_{rt}(1)_r = 1{,}079lnINT_{H_{rt}}\ (1) + 0{,}253lnIP_{I_{rt}}\ (1) + 0{,}025lnEG\_I_{rt}(1) - 0{,}024lnEMP_{rt}(1)\ - 0{,}075lnTR_{I_{rt}} + 0{,}047 \quad (1.11)$$

Таблиця 1.5 – Результати оцінювання впливу чинників цифровізації на рівень інтернет банкінгу

	Загальна модель панельних даних		Модель панельних даних з фіксованими ефектами		Модель панельних даних з випадковими ефектами	
	значення коефіцієнта	p-value	значення коефіцієнта	p-value	значення коефіцієнта	p-value
const	0,046715	0,1635	-0,056131	0,6680	0,046549	0,1641
ln INT_H (1)	1,081665	0,0008*	0,972218	0,0047*	1,079119	0,0007*
ln IP_I (1)	0,252677	0,0067*	0,278634	0,0045*	0,253241	0,0061*
ln EG_I (1)	0,024138	0,7541	0,086752	0,2903	0,025464	0,7392
ln ECM	-0,023603	0,2560	0,051821	0,5907	-0,023506	0,2578
ln TR_E (1)	-0,075184	0,1482	-0,065020	0,2554	-0,074868	0,1470
Пооказники адекватності						
R-squared	0,381578		0,516559		0,379703	
Adjusted R-squared	0,352948		0,364782		0,350985	
F-statistic	13,32762		3,403392		13,22200	
Prob (F-statistic)	0,00000		0,000009		0,000000	

* позначається значущість параметра на рівні надійності 0,95

За результатами проведених розрахунків встановлено, що незалежно від типу регресійної панельної моделі з поміж п’яти незалежних змінних статистчино значущими на рівні надійності 0,95 є: рівень доступу домогосподарств до мережі Інтернет (INT_H) та рівень інтернет-покупок (IP_I). Крім цього, дані фактори мають позитивний вплив на розвиток фінансових технологій в країнах ЄС. Зокрема, збільшення рівня доступу домогосподарств та інтернет-покупок на 1% зумовлює зростання розрахунків з використанням інтернет-банкінгу на 1,08% та 0,25% відповідно. Скоригований коефіцієнт детермінації за розглянутими моделями коливається в межах 0,35, тобто включені значущі факторні змінні лише на 35% пояснюють динаміку результативного показника. Водночас, згідно з F-критерієм Фішера, отримані економетричні моделі є статистично значимими, оскільки prob < 0,05.

Для визначення найбільш адеватної моделі доцільно скоритатися наступними статистичними критеріями: критерій відношення правдоподібності (Likelihood Ratio test) та тест Хаусмана.

Загальна модель нехтує ефектами неоднорідності, які явно враховані в моделі фіксованих ефектів. Для порівняння даних двох моделей використовують критерій відношення правдоподібності, що передбачає розрахунок критерію Фішера та Пірсона. При проведенні попарного порівяння загальної моделі та моделі з фіксованими ефектами висувається нульова гіпотеза, за якої наявність фіксованих ефектів у моделі є не значимою. Результати перевірки тести на специфікацію моделі представнено на рисунку 1.4.

Оскільки p-value як за критерієм Фішера (0,37) та Пірсона (0,17) більша за 0,05, тому приймаємо нульову гіпотезу, тобто включення фіксованих ефектів у модель недостатньо доцільно.

Для вибору моделі панельних даних з фіксованими чи випадковими ефектами доцільно використовувати тест Хаусмана, результати його розрахунку представлено на рисунку 1.5. Нульовою гіпотезою за тестом

Хаусмана є доцільність використовувати моделі з випадковими панельними даними.

Redundant Fixed Effects Tests
Test cross-section fixed effects

Effects Test	Statistic	d.f.	Prob.
Cross-section F	1.091456	(22,86)	0.3719
Cross-section Chi-square	28.071646	22	0.1733

Cross-section fixed effects test equation:
Dependent Variable: D(Y1)
Method: Panel Least Squares
Sample (adjusted): 2015 2019
Periods included: 5
Cross-sections included: 23
Total panel (unbalanced) observations: 114

Variable	Coefficient	Std. Error	t-Statistic	Prob.
D(X1)	1.081665	0.312531	3.460987	0.0008
D(X2)	0.252677	0.091339	2.766367	0.0067
D(X3)	0.024138	0.076862	0.314051	0.7541
X4	-0.023603	0.020670	-1.141893	0.2560
D(X5)	-0.075184	0.051627	-1.456275	0.1482
C	0.046715	0.033295	1.403058	0.1635

R-squared	0.381578	Mean dependent var	0.058347
Adjusted R-squared	0.352948	S.D. dependent var	0.081341
S.E. of regression	0.065431	Akaike info criterion	-2.564453
Sum squared resid	0.462368	Schwarz criterion	-2.420443
Log likelihood	152.1738	Hannan-Quinn criter.	-2.506008
F-statistic	13.32762	Durbin-Watson stat	1.571512
Prob(F-statistic)	0.000000		

Рисунок 1.4 – Результат тесту на специфікацію панельних ефектів (між загальною моделлю і моделлю з фіксованими ефектами) для результативної змінної – рівень інтернет банкінгу

Дані рисунку 1.5 засвідчують, що для опису обраних панельних даних більш доцільним є використання моделі з випадковими ефектами (p-value: 0,26 > 0,05). У моделі з випадковими ефектами передбачається, що індивідуальні відмінності носять випадковий характер. Цю модель можна розглядати як компроміс між загальною регресією, що накладає сильне обмеження гомогенності на всі коефіцієнти рівняння регресії, і регресією з фіксованими ефектами, яка дозволяє для кожного об’єкта вибірки ввести свою

константу і, таким чином, врахувати існуючу в реальності, але неспостережуваних гетерогенність.

Correlated Random Effects - Hausman Test
Equation: EQ05_Y1_2
Test cross-section random effects

Test Summary	Chi-Sq. Statistic	Chi-Sq. d.f.	Prob.
Cross-section random	6.445806	5	0.2652

Cross-section random effects test comparisons:

Variable	Fixed	Random	Var(Diff.)	Prob.
D(X1)	0.972218	1.079119	0.015965	0.3975
D(X2)	0.278634	0.253241	0.000888	0.3941
D(X3)	0.086752	0.025464	0.000828	0.0332
X4	0.051821	-0.023506	0.008787	0.4216
D(X5)	-0.065020	-0.074868	0.000597	0.6869

Рисунок 1.5 – Результат тесту Хаусмана на специфікацію панельних ефектів (між моделлю з фіксованими ефектами і моделлю з випадковими ефектами) для результативної змінної – рівень інтернет банкінгу

Одним із ключових етапів побудови економетричної моделі є перевірка її на адекватність. Для оцінки нормальності розподілу залишків панельної моделі можна проаналізувати гістограмму розподілу і результати тесту Бера-Жарка (рис. 1.6)

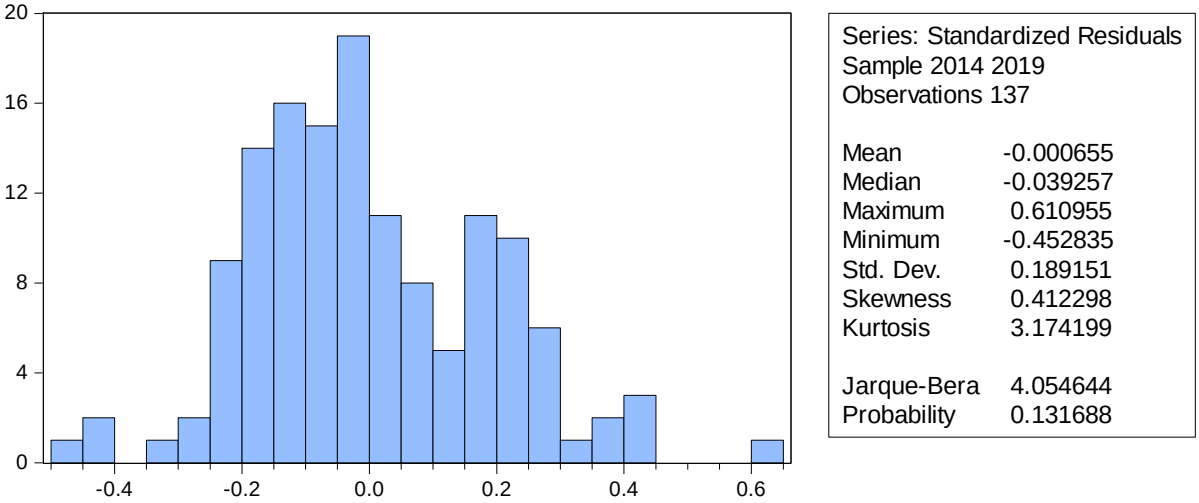


Рисунок 1.6 – Гістограма розподілу залишків

Дані рисунку 1.6 дозволяють стверджувати про наявність нормального розподілу залишків за побудованою моделлю. Оскільки рівень значущості критерію Жарка-Бера становить 0,132, що є більшим за 0,05.

Наступним критерієм є перевірка наявності кореляції в залишках на основі тестів Бреуша – Пагапа та Песарана (рис. 1.7).

Residual Cross-Section Dependence Test
Null hypothesis: No cross-section dependence (correlation) in residuals
Equation: EQ05_Y1_2
Periods included: 5
Cross-sections included: 23
Total panel (unbalanced) observations: 114
Note: non-zero cross-section means detected in data
Test employs centered correlations computed from pairwise samples

Test	Statistic	d.f.	Prob.
Breusch-Pagan LM	324.1426	253	0.1017
Pesaran scaled LM	2.140200		0.0823
Pesaran CD	1.896888		0.0578

Рисунок 1.7– Результат перевірки кореляції в залишках

Результати розрахунку тестів дозволяють прийняти нульову гіпотезу про відсутність кросс-секційної кореляції в залишках отриманої моделі (значення тестів Бреуша – Пагапа та Песарана більші за 0,05).

Для оцінки якості «підгонки» моделі під реальні дані можна переглянути спільні графіки фактичних і розрахункових значень, а також проаналізувати графік залишків (рис. 1.8).

Отже, для оцінювання впливу цифровізації та ступінь розвитку інтернет банкінгу доцільно використовувати модель панельних даних з випадковими ефектами, яка є адеватною. Зокрема, збільшення використання фізичними особами Інтернету та здійснення інтернет-покупок на 1% стимулює збільшення рівня інтернет банкінгу на 1,08 % та 0,25% відповідно.

Перейдемо до аналізу іншої результативної змінної (рівень використання фінансових послуг онлайн) та впливу факторів на неї (табл. 1.6).

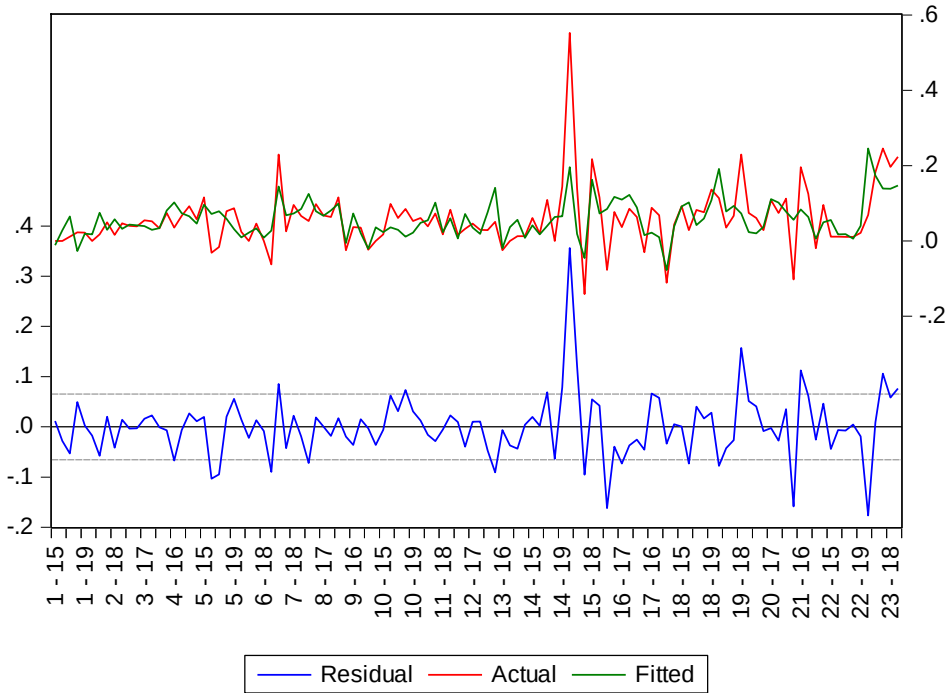


Рисунок 1.8 – Графік фактичних та розрахованих значень показника «рівень інтернет банкінгу»

Беручи до уваги дані таблиці 1.6, побудуємо наступні формалізовані зв'язки між досліджуваними процесами:

– загальна модель панельних даних:

$$lnFIN_{rt} = -0{,}991lnINT_{H_{rt}}(1) - 1{,}269lnIP_{I_{rt-1}}(1) + 0{,}951lnEG\_I_{rt} + 1{,}720lnEMP_{rt} - 0{,}416lnTR_{I_{rt}}(1) - 1{,}271 \quad (1.11)$$

– модель панельних даних з фіксованими ефектами:

$$lnFIN_{rt} = -2{,}247lnINT_{H_{rt}}(1) + 0{,}363lnIP_{I_{rt-1}}(1) + 0{,}488lnEG\_I_{rt} + 3{,}254lnEMP_{rt} - 0{,}636lnTR_{I_{rt}}(1) - 3{,}393 \quad (1.12)$$

– модель панельних даних з випадковими ефектами:

$$lnFIN_{rt} = -2{,}313lnINT_{H_{rt}}(1) + 0{,}235lnIP_{I_{rt-1}}(1) \quad (1.13)$$
$$+ 0{,}497lnEG\_I_{rt} + 2{,}256lnEMP_{rt} - 0{,}537lnTR_{I_{rt}}(1) - 2{,}043$$

Таблиця 1.6 – Результати оцінювання впливу чинників цифровізації на рівень використання фінансових послуг онлайн

	Загальна модель панельних даних		Модель панельних даних з фіксованими ефектами		Модель панельних даних з випадковими ефектами	
	значення коефіцієнта	p-value	значення коефіцієнта	p-value	значення коефіцієнта	p-value
const	-1,271235	0,0011*	-3,393063	0,0000*	-2,043231	0,0000*
ln INT_H (1)	-0,991123	0,7819	-2,247454	0.2253	-2.312744	0.2088
ln IP_I (1)	-1,269337	0,2266	0,363428	0.4899	0.234525	0.6542
ln EG_I (1)	0,950954	0,2814	0,488973	0.2780	0.497181	0.2671
ln ECM	1,720044	0,0000*	3,254621	0.0000*	2.255612	0.0000*
ln TR_E (1)	-0,416469	0,4818	0,636448	0.0444*	-0.537003	0.0834
Пооказники адекватності						
R-squared	0,474146		0,904986		0,355146	
Adjusted R-squared	0,449801		0,875156		0,325291	
F-statistic	19,47606		30,33819		11,89594	
Prob (F-statistic)	0,000000		0,000000		0,000000	

* позначається значущість параметра на рівні надійності 0,95

На відміну від онлайн банкінгу, значущими факторами впливу на рівень використання фінансових послуг онлайн є інші змінні – рівень електронної комерції та частка підприємств, які проводили навчання та підвищення кваліфікації свого персоналу інформаційно-комунікативним технологіям. З поміж трьох розглянутих моделей найвищий рівень адекватності за показником коефіцієнта детермінації є модель з фіксованими ефектами, тоді як за критерієм Фішера – всі моделі є статистчино значущі.

З метою проведення науково обгрунтованого вибору між даними моделями використоно формалізовані тести (рис. 1.9).

Наявний рівень значущості (критерій Фішера та Пірсона = 0,000) дозволяє відхилити нульову гіпотезу про відсутність в моделі фіксованих

панельних ефектів. Крім цього, здійснемо перевірку доцільності застосування моделі з фіксованими або випадковими ефектами (рис. 1.10).

Redundant Fixed Effects Tests
Equation: EQ05_Y2_2
Test cross-section fixed effects

Effects Test	Statistic	d.f.	Prob.
Cross-section F	17.725756	(22,86)	0.0000
Cross-section Chi-square	195.054050	22	0.0000

Рисунок 1.9 – Результат тесту на специфікацію панельних ефектів (між загальною моделлю і моделлю з фіксованими ефектами) для результативної змінної – рівень використання фінансових послуг онлайн

Correlated Random Effects - Hausman Test
Equation: EQ05_Y2_2
Test cross-section random effects

Test Summary	Chi-Sq. Statistic	Chi-Sq. d.f.	Prob.
Cross-section random	13.579582	5	0.0185

Cross-section random effects test comparisons:

Variable	Fixed	Random	Var(Diff.)	Prob.
D(X1)	-2.247454	-2.312744	0.041466	0.7485
D(X2)	0.363428	0.234525	0.002024	0.0042
D(X3)	0.488973	0.497181	0.002010	0.8547
X4	3.254621	2.255612	0.182365	0.0193
D(X5)	-0.636448	-0.537003	0.002865	0.0632

Рисунок 1.10 – Результат тесту Хаусмана на специфікацію панельних ефектів (між моделлю з фіксованими ефектами і моделлю з випадковими ефектами) для результативної змінної – рівень використання фінансових послуг онлайн

Результати розрахунку тесту Хаусмана вказують на необхідність використання саме моделі панельних даних з фіксованими ефектами, оскільки p-value 0,018 < 0,05. Наявність фіксованих ефектів у моделі вказує на наявність сутєєвих відмінностей в вільних коефіцієнтах, що відображають особливості кожної країни в провадженні цифрових продуктів в економічне життя.

З метою визначення ступеня впливу факторів цифровізації на рівень використання фінансових послуг онлайн для кожної країни додамо фіктивні змінні (приймають значення «0» або «1»). Фіксовані ефекти країн оцінюють вплив не вимірювальних чинників, які впливають на залежну змінну (рівень використання фінансових послуг онлайн). Оскільки будь-яка економетрична модель містить загальний перетин (c), то визначені значення фіксованих ефектів для кожної країни відображають відмінності у відповідних перетинах (табл. 1.7).

Таблиця 1.7 – Проміжні результати з розрахунку фіксованих ефектів країн порівняно з середнім по ЄС

Країна	Умовне позначення	Фіктивні змінні			p-значимість
		початкове значення	розрахунок	значення константи	
Фінляндія	-	-3,640	-	-3,640	0,001*
Франція	d2	0,098	-3,640+0,098	-3,542	0,792
Німеччина	d3	1,124	-3,640+1,124	-2,516	0,003*
Італія	d4	0,301	-3,640+0,301	-3,339	0,479
Латвія	d5	0,201	-3,640+0,201	-3,439	0,692
Нідерланди	d6	0,364	-3,640+0,364	-3,276	0,198
Польща	d7	0,084	-3,640+0,084	-3,556	0,866
Іспанія	d8	0,399	-3,640+0,399	-3,241	0,341
Швеція	d9	0,573	-3,640+0,573	-3,067	0,013*
Великобританія	d10	0,140	-3,640+0,140	-3,500	0,583
Австрія	d11	-0,145	-3,640-0,145	-3,785	0,651
Бельгія	d12	-0,289	-3,640-0,289	-3,929	0,323
Естонія	d13	-0,769	-3,640-0,769	-4,409	0,003*
Ірландія	d14	-1,340	-3,640-1,340	-4,980	0,000*
Хорватія	d15	0,026	-3,640+0,026	-3,614	0,953
Литва	d16	0,656	-3,640+0,656	-2,984	0,226
Люксембург	d17	-0,036	-3,640-0,036	-3,676	0,889
Угоршина	d18	-0,390	-3,640-0,390	-4,030	0,323
Португалія	d19	0,552	-3,640+0,552	-3,088	0,226
Словенія	d20	-0,481	-3,640-0,481	-4,121	0,205
Словачиина	d21	0,200	-3,640+0,200	-3,440	0,670
Норвегія	d22	1,124	-3,640+1,124	-2,516	0,000*
Туреччина	d23	3,310	-3,640+3,310	-0,330	0,001*
Середнє значення				-3,393	-

Дані таблиці 1.7 вказують, що індивідуальні фіксовані ефекти мають від’ємні значення по всім країнам ЄС, що свідчитть про неврахування певних чинників, що стримують розвиток фінансових послуг онлайн. Крім цього,

варто відмітити, що статистчино значимими індивідуальними ефектами є значення по таких країнах як: Фінляндія, Німеччина, Швеція, Естонія, Ірландія, Горвегія, Туреччина.

Заключним етапом побудови економетричних моделей є перевірки їх на адекватність. Крім показників детермінації та критерія Фішера для визначенн відсутності автокореляції в залишках моделі використовується панельний аналог тесту Дарбіна-Уотсона

Для оцінки нормальності розподілу залишків панельної моделі можна проаналізувати гистограмму розподілу і результати тесту Бера-Жарка (рис. 1.11).

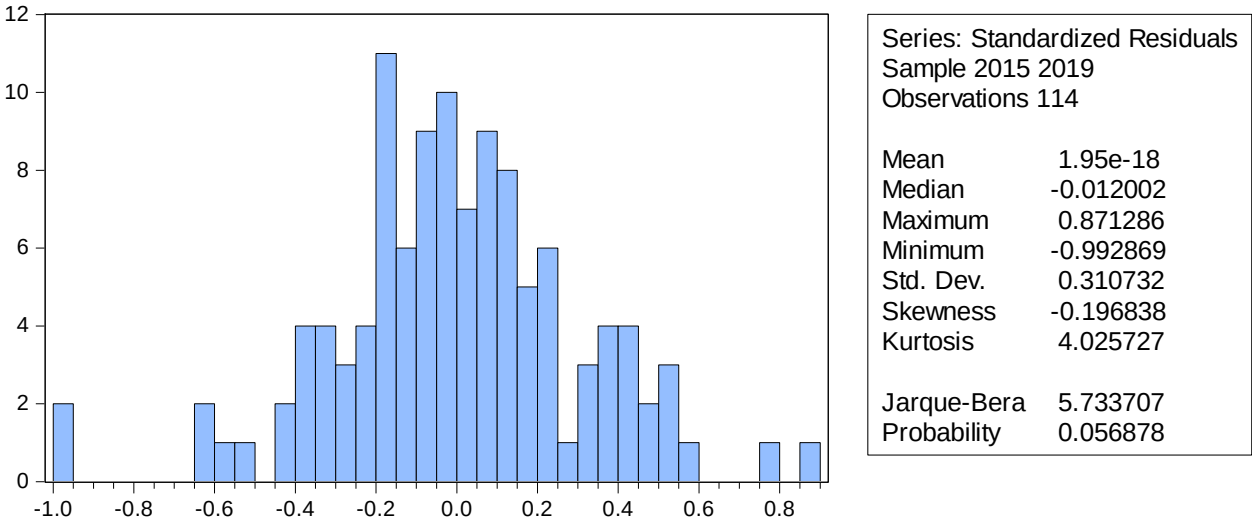


Рисунок 1.11 – Результати перевірки нормальності розподілу залишків моделі

Нульова гіпотеза про відповідність розподілу нормальному перевіряється на основі статистики Жарка-Бера із зазначенням відповідного рівня значущості. Оскільки рівень значущості за досліджуваною моделлю становить 0,057 (більше за 0,05), тоді можемо стверджувати про наявність нормального закону розподілу залишків.

Розрахунок статистичних тестів для перевірки серійної кореляції в залишках другої моделі підтвердив відчутність даної проблеми, що свідчить про адекватність отриманих даних (рис. 1.12).

Residual Cross-Section Dependence Test
Null hypothesis: No cross-section dependence (correlation) in residuals
Equation: EQ05_Y2_DUMMY
Periods included: 5
Cross-sections included: 23
Total panel (unbalanced) observations: 114
Test employs centered correlations computed from pairwise samples

Test	Statistic	d.f.	Prob.
Breusch-Pagan LM	432.5747	253	0.1254
Pesaran scaled LM	6.960594		0.1125
Pesaran CD	1.19052		0.0458

Рисунок 1.12 – Результат перевірки кореляції в залишках

Для візуального представлення фактичних та розрахункових значень рівня використання фінансових послуг онлайн в країнах ЄС побудовано графік, який засвідчує достатньо високу відповідність між цими значеннями (рис. 1.13).

Таким чином, за результататми проведених розрахунків виявлено, що для відображення залежності мід рівнем використання фінансових послуг онлайн та індикаторами цифровізації доцільно використовувати модель панельних даних з фіксованими ефектами. Коефіцієнт детермінації критерій Фішера, показник Жака-Берра, а також тести для перевірки кореляції засвідчують, що модель є адеватною, тому її будемо використовувати для формування висновків. В країнах ЄС зростання рівня зайнятості у сфері інформаційно-комунітивних технологій та частки компаній, які займалися підготовкою та перепідготовкою свого персоналу цифровим навичкам на 1% призводило до зростання отримання фінансових послуг онлайн на 3,25% та 0,63 % відповідно. Отже, ключову роль у розвитку цифрових фінансових послуг належить людському ресурсу, а саме рівня його кваліфікації та навичок.

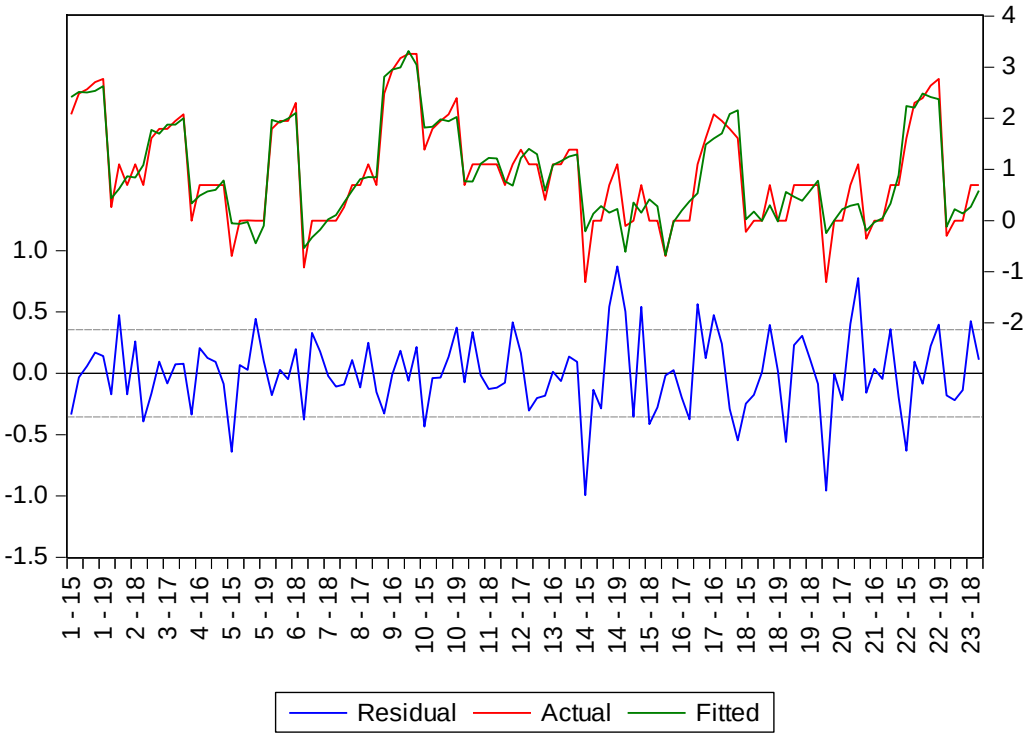


Рисунок 1.13 – Графік фактичних та розрахованих значень показника «рівень використання фінансових послуг онлайн»

Для визначення ступеня залежності між розвитком цифровізації економіки та поширенням кібератак вирішено використати модель розподіленого лагу. Для вирішення поставленої задачі сформовано статистичну базу дослідження за період 2011-2019 рр., яка містить дані щодо 11 незалежних змінних та 1 залежної змінної (кількість випадків з кібершахрайства) (таблиця 1.2).

Важливою передумовою побудови моделі розподіленого лагу є перевірка змінних на наявність мультиколінеарності між ними. Результати побудови кореляційної матриці представлено в таблиці 1.9.

Дані таблиці засвідчують, що між більшістю аналізованих факторних змінних існує тісний лінійний зв’язок (більше за 0,7). У зв’язку з цим для подальших розрахунків вирішено включити тільки 2 змінні: частка підприємств, які проводили навчання та підвищення кваліфікації персоналу

інформаційно-комунікативним технологіям (TR_E) та частка підприємств, які здійснюють e-commerce продажі (ECM_E).

Таблиця 1.9 – Кореляційна матриця

	INT_H	IP_I	EG_I	EMP	TR_E	ECM	ECM_E	INT_I	INT_EM	IIP	WEB
INT_H	1,000	0,994	0,968	0,801	0,737	0,962	0,822	0,972	0,960	0,879	0,960
IP_I	0,994	1,000	0,951	0,796	0,762	0,978	0,818	0,974	0,957	0,899	0,970
EG_I	0,968	0,951	1,000	0,730	0,660	0,900	0,779	0,913	0,888	0,803	0,878
EMP	0,801	0,796	0,730	1,000	0,615	0,778	0,820	0,835	0,886	0,606	0,822
TR_E	0,737	0,762	0,660	0,615	1,000	0,852	0,456	0,728	0,741	0,836	0,684
ECM	0,962	0,978	0,900	0,778	0,852	1,000	0,788	0,964	0,955	0,939	0,943
ECM_E	0,822	0,818	0,779	0,820	0,456	0,788	1,000	0,853	0,896	0,639	0,881
INT_I	0,972	0,974	0,913	0,835	0,728	0,964	0,853	1,000	0,974	0,914	0,972
INT_EM	0,960	0,957	0,888	0,886	0,741	0,955	0,896	0,974	1,000	0,853	0,963
IIP	0,879	0,899	0,803	0,606	0,836	0,939	0,639	0,914	0,853	1,000	0,873
WEB	0,960	0,970	0,878	0,822	0,684	0,943	0,881	0,972	0,963	0,873	1,000

При побудові економетричної моделі вирішено включити наступні лаги: 1 рік, 2 роки. Результати визначення параметрів регресійної моделі на основі методу найменших квадратів подано на рисунках 1.14 -1.15.

ВЫВОД ИТОГОВ

Регрессионная статистика	
Множественный R	0,8939
R-квадрат	0,7990
Нормированный R-квадрат	0,5980
Стандартная ошибка	3559,58
Наблюдения	7

Дисперсионный анализ

	df	*SS*	*MS*	*F*	*Значимость F*
Регрессия	3	151101568	50367189,5	3,975125	0,14339802
Остаток	3	38011780	12670593,5		
Итого	6	189113349			

	Коэффициенты	*дартная ош*	*статистик*	*-Значение*	*Нижние 95%*	*Верхние 95%*	*Нижние 95,0%*	*ерхние 95,0%*
Y-пересечение	-11118,272	32956,292	-0,337	0,758	-115999,903	93763,359	-115999,903	93763,359
TR_E	-1367,139	1080,043	-1,266	0,295	-4804,317	2070,038	-4804,317	2070,038
TR_E-1	725,337	1312,894	0,552	0,619	-3452,876	4903,551	-3452,876	4903,551
TR_E-2	1691,828	1146,176	1,476	0,236	-1955,815	5339,471	-1955,815	5339,471

Рисунок 1.14 – Результати побудови регресійної моделі для показника «TR_E»

ВЫВОД ИТОГОВ

Регрессионная статистика	
Множественный R	0,98
R-квадрат	0,97
Нормированный R-квадрат	0,94
Стандартная ошибка	1377,17
Наблюдения	7,00

Дисперсионный анализ

	df	*SS*	*MS*	*F*	*Значимость F*
Регрессия	3	183423573,6	61141191,2	32,237402	0,00877908
Остаток	3	5689775,246	1896591,75		
Итого	6	189113348,9			

	Коэффициенты	*Стандартная ошибка*	*t-статистика*	*P-Значение*	*Нижние 95%*	*Верхние 95%*	*Нижние 95,0%*	*Верхние 95,0%*
Y-пересечение	-42844,1044	9911,8826	-4,3225	0,0228	-74388,1387	-11300,0701	-74388,1387	-11300,0701
ECM_E	734,4458	250,1330	2,9362	0,0607	-61,5890	1530,4805	-61,5890	1530,4805
ECM_E-1	1245,1854	323,0702	3,8542	0,0309	217,0318	2273,3389	217,0318	2273,3389
ECM_E-2	705,2095	465,1681	1,5160	0,2268	-775,1629	2185,5819	-775,1629	2185,5819

Рисунок 1.15 – Результати побудови регресійної моделі для показника «ECM_E»

Побудовані дві моделі розподіленого лагу засвідчують доцільність використання лише другої. Перша модель (незалежна змінна: TR_E, рис. 1.14) є статистично незначимою за критерієм Фішера, а також відсутні значимі параметри (на основі критерію Стьюдента), і тому результати розрахунків не доцільно використовувати для формування науково обґрунтованих рішень.

Друга регресійна модель має кращі показники якості: по-перше, коефіцієнт детермінації становить 0,97; по-друге, порівняння залишкової дисперсії з дисперсією середнього арифметичного за допомогою F критерію Фішера також вказує на адекватність побудованої моделі (p-value < 0,05); по-третє, критерій Стьюдента та його p-значимість вказує на наявність статистично значимих параметрів.

На основі даних рисунку 1.15 представимо регресійну модель наступного виду:

$$CC = -42844{,}1 + 734{,}45ECM\_E_0 + 1234{,}185CM\_E_1 + 705{,}2095ECM\_E_2 \quad (1.14)$$

На основі співвідношень

$$\beta_0 = c_0$$
$$\beta_1 = c_0 + c_1 + c_2$$
$$\beta_2 = c_0 + 2c_1 + 4c_2$$

розраховують параметри моделі з розподіленим лагом:

$\beta_0 = c_0$= 734,45

$\beta_1 = c_0 + c_1 + c_2$ = 734,45+1234,185+705,209 = 2684,84

$\beta_2 = c_0 + 2c_1 + 4c_2$ = 734,45+2*1234,185+4*705,209 = 6045,66

Таким чином, модель з розподіленим лагом має наступний вигляд:

$$CC = -42844{,}1 + 734{,}45X_t + 2684{,}84X_{t-1} + 6045{,}66X_{t-2} \qquad (1.15)$$

Беручи до уваги, що статистично значимим є значення рівня e-commerce продажів з лагом в 1 рік, то зробимо наступний висновок: зростання рівня електронної комерції на 1% в поточному році у Бельгії призводить до збільшення масштабів кібератак в цій країні через 1 рік на 8731 випадків. Побудована дана економетрична модель є адекватною, оскільки коефіцієнт детермінації становить 0,98, фактичне значення критерію Фішера (34,3) більше за критичне (19,3).

Отримані емпіричні результати щодо визначення залежності в розвитку цифрових та фінансових технологій на прикладі 23 європейських країн можуть бути враховані Україною при розбудові цифрової економіки та суспільства. Цифровий розвиток у сфері фінансових відносин в Україні дещо відстає від європейських тенденцій, що пояснюється низьким рівнем цифрової грамотності населення та їх недовіра до інноваційних фінансових послуг, відставання в науково-технічному розвитку, недостатній розвиток інформаційної інфраструктури.

Підсумовуючи результати побудованих економетричних моделей встановлено, що найбільш значущими чинниками, що стимулюють розвиток фінансових технологій та їх використання населенням є рівень доступу до мережі інтернет, розвиток електронної комерції та розвиток цифрових навичок та компетенцій.

Таким чином, застосування цифрових фінансових технологій, з одного боку, сприяє інтенсивному розвитку фінансових відносин, підвищенню фінансової інклюзії та посилення конкуренції на ринку фінансових послуг, з іншого - появі нових ризиків та загроз інформаційної безпеки. Розвиток цифрових технологій призводить до зростання масштабів кіберзагроз, які потребують оперативного і своєчасного виявлення, оцінки та розробки відповідних заходів по їх запобіганню або мінімізації можливих наслідків.

1.3. **Критерії неформальних фінансових транзакцій за посередництва фінансових установ**

Протягом останнього десятиріччя з розвитком технологій, що використовуються у фінансовому секторі, розширенням комплексу послуг, що надаються економічними агентами, також удосконалювались шахрайські схеми для здійснення фінансових злочинів. А проведення незаконних фінансових транзакцій вже стало серйозною проблемою більшості економік країн світу. Так як вони підривають фундаментальні основи економічної системи та негативно впливають на розвиток національної економіки. І хоча фахівцями всього світу спрямовуються постійні зусилля для зупинення нелегальних фінансових операцій, протидії та боротьби з фінансово-економічними злочинами, наразі вони все ще залишаються досить серйозною проблемою для розвитку економіки та забезпечення економічної безпеки. Наявні не вирішені проблеми фінансової злочинності потребують розроблення комбінацій методик та моделей, що зможуть, враховуючи певні чинники та пріоритети, ефективно виявляти на ранніх етапах можливі фінансові

порушення. А це можливо досягти шляхом побудови ефективних причинно-наслідкових моделей, які зможуть пов’язати та об’єднати причини та наслідки фінансових транзакцій і фінансових злочинів у єдиний комплекс результативних дій.

Для побудови моделі оцінювання причинно-наслідкових зв’язків між фінансовими транзакціями та фінансовими злочинами, необхідно розуміти, які саме фінансові транзакції можуть використовуватись фінансовими злочинцями. Спостерігаються певні характеристики фінансових транзакцій, що можуть бути пов’язані з фінансовими злочинами. Такі фінансові транзакції, в залежності від їх характерних особливостей, групуються за наступними критеріями:

1. Поведінка клієнта: клієнт не надає необхідну для економічного агенту інформацію; клієнт надає неповну інформацію; клієнт надає недостовірну, сумнівну, неправдиву інформацію; клієнт не надає підтверджуючі документи; надана клієнтом контактна інформація щодо телефонів,адрес, електронної пошти є недійсною; дані від клієнта відрізняються від наявних в публічних джерелах; вік клієнта не відповідає характеру фінансових транзакцій; професія клієнта не характерна фінансовій операції; рівень доходу клієнта не відповідає сумі фінансової транзакції; клієнт не спроможний чітко сформулювати характер його діяльності; клієнт не розуміє характеру фінансових транзакцій; клієнт безпідставно поводиться нетипово, незвично, підозріло, нервово; клієнт безпідставно вимагає терміново провести транзакцію; клієнт підозріло цікавиться вимогами фінансового моніторингу; клієнт пропонує винагороду за проведення фінансової транзакції; клієнт відмовляється від здійснення фінансової транзакції через вимогу надати додаткові документи; клієнт вимагає обслуговуватись у конкретного працівника економічного агенту, відмовляючись від здійснення фінансової транзакції за відсутності такого працівника; у клієнта відкрита необґрунтовано велика кількість рахунків; незрозумілий характер мети відкриття рахунків; невідповідність між сумами податків та обсягів операцій; виникають підозри з приводу виконання операції

на користь невідомої третьої особи, або здійснення такою особою контролю за проведенням транзакції; законний представник клієнта умисно не контактує з працівниками економічного агенту; одна особа розпоряджається не пов'язаними рахунками; клієнт указує адресу доставки карти, що не пов'язана з клієнтом.

2. Безпосередньо фінансові транзакції: проведення значного обігу коштів по рахунку протягом дня при малих залишках коштів на кінець та початок дня; фінансові транзакції не відповідають діяльності клієнта; стрімкі скачки у сумах коштів по рахунках клієнта; часті перекази без відкриття рахунку; зарахування частих маленьких сум, з наступним їх сукупним перерахуванням іншій особі; рух коштів по рахунку передбачає тільки безготівкові зарахування з їх послідуючим готівковим виведенням з рахунку; здійснення готівкових транзакцій на значну суму, що не відповідають основному КВЕДу клієнта; здійснення транзакцій по картковим рахункам в великій кількості; проведення фінансових транзакцій по угодам відступлення прав вимоги; видаткові фінансові транзакції по підкріпленню каси по угодам інкасації у великих обсягах, з наступною видачею кредитів фізичних осіб, при чому кошти заходять на рахунок у великих сумах як оплата по угодам відступлення прав вимоги; безготівкове перерахування з рахунку коштів для для видачі кредитів фізичним особам, обсяги яких необгрунтовано більші за середньоринкові; видача декільком фізичним особам короткострокових кредитів на значні суми від однієї юридичної особи, при чому кошти фізичними особами одразу знімаються готівкою, а потім немає платежів по погашенню таких кредитів, а згідно наявних даних ці фізичні особи не мають достатніх коштів і доходів на погашення кредитів; отримання фізичною особою кредиту на велику суму, що більша за доходи фізичної особи, з подальшим погашенням кредиту не за рахунок коштів фізичної особи, а інших осіб; надходження на рахунок неприбуткової юридичної особи виключно державних коштів; відсутність інкасації виручки у клієнта, основним КВЕДом якого є роздрібна торгівля; більшість надходжень на рахунок складають кошти

від онлайн-систем, але при цьому клієнт не працює в інтернет-торгівлі чи онлайн-діяльності; проведення розрахунків від комерційної діяльності через рахунок фізичної особи; відмінності між реквізитами платежу та підтвержуючими документами; штучне поповнення та збільшення статутного капіталу шляхом поступового періодичного перерахування коштів на рахунок юридичної особи; здійснення операцій з купівлі чи продажу активів, отримання чи виплата заборгованостей за правочинами, надання чи повернення фінансової допомоги щляхом періодичного обігу одієї суми по рахунку клієнта; здійснення обслуговування по фінансовим транзакціям протягом одного дня умисно у різних працівників економічного агенту; перерахування коштів з рахунку юридичної особи на окремі рахунки фізичних осіб працівників чи пов'язаних з працівниками осіб, що не є виплатою заробітної плати чи інших зрозумілих виплат; партнери клієнта мають негативну репутацію; відправник та отримувач коштів не володіють елементарною інформацією один про одного; повернення коштів банком-отримувачем; безпідставна відмова у наданні відомостей по учасникам фінансової транзакції; виплата переказів у відділеннях, що територіально розміщені поряд з кордонами країн, що мають високий ризик тероризму; частий обіг позикових коштів від осіб, що не є групою пов'язаних осіб; неконкретизоване призначення платежу; прибуткові та видаткові операції мають невідповідне призначення; періодичні платежі особам, що не мають очевидного зв'язку з господарською діяльністю клієнта; надходження коштів від неприбуткової установи з наступною терміновою їх витратою на придбання активів; зв'язок фінансової транзакції з купівлею чи продажем товарів подвійного використання; застосування POS-терміналу клієнта третіми особами; придбання клієнтом необгрунтованої кількості миттєвих неперсоніфікованих карток; незрозумілі, не притаманні для певного виду господарської діяльності суми та обсяги фінансових транзакцій; фінансові транзакції з відшкодування коштів особам, від яких оплати фактично не поступали; переказ коштів юридичною особою-резидентом на рахунок

юридичної особи-нерезидента, відкритий в банку в Україні; одержання коштів юридичною особою-нерезидентом від юридичної особи-резидента на рахунок,відкритий в банку в Україні; партнери по зовнішньоекономічним контрактам мають негативну оцінку; проплата по зовнішньоекономічним контрактам, по яким вже виявлені порушення; нечітка сутність фінансових транзакцій з-за кордону чи за кордон; закордонні перекази протягом одного дня різними особами, але зі схожими реквізитами; збір коштів різними неприбутковими організаціями для подальшого перерахування певним особам-нерезидентам; отримання коштів із-за кордону з подальшим перерахуванням цих коштів за кордон (у ту ж країну), чи на ім'я тієї ж особи за кордон (в іншу країну).

3. Фінансові транзакції страхових компаній: необгрунтоване збільшення розміру страхової суми; обсяг страхових сум неспівставний з можливим ризиком; суми страхових внесків та страхових премій сплачуються незрозуміло більші за вказані в угоді; великі готівкові обсяги сплати страхових премій; почастинна виплата страхового відшкодування готівкою; готівковий одноразовий страховий внесок згідно угоди на страхування життя; розторгнення страхової угоди достроково з наступним перерахуванням третій особі коштів; треті особи сплачують страхові внески та страхові премії; необгрунтовано великі суми виплат (за надані послуги) фізичним особам-підприємцям; необгрунтовано великі суми агентської винагороди по договору доручення; угоди з явно невигідними для сторін умовами; значні зміни по раніше укладеним угодам за незначний термін; сума застрахованого майна невідповідна до фінансових доходів клієнта; страхування об'єкта по ризикам, що не є для нього притаманними; повторне страхування фінансових ризиків особи, яка мала страхове відшкодування у минулому; страхування фінансових ризиків особи, яка мала страхове відшкодування у минулому; страхування фінансових ризиків осіб, які несуть фінансові ризики по незастрахованим особам; в малий термін після страхування відбувається страховий випадок; недійсна, підроблена документація щодо сплати страхових внесків, страхових

премій, страхових виплат; заключення короткострокового депозитного договору з кінцевою датою – останнім днем кварталу; здійснення дострокового розторгнення депозитної угоди після останнього дня кварталу; обмежений список підтверджуючих документів для сплати відшкодування по страховій угоді; фінансові транзакції перестрахування особи, у якої суми руху коштів за минулі періоди значно менший; перестрахування осіб з незадовільним фінансовим становищем; перестрахування особи, що знаходиться у нетиповій для такої угоди державі; перестрахування осіб з країн перестрахування осіб яких у минулому не здійснювалось; перестраховик не може виконати фінансові зобов'язання власними коштами.

4. Готівкові фінансові транзакції: готівкове внесення виручки по проданим активам на рахунок без підтверджуючих документів; часті дрібні фінансові транзакції по внесенню на рахунки готівки у різних відділеннях банку для переказу коштів на один рахунок; дрібні фінансові транзакції значної кількості по внесенню на рахунки готівки у одному відділенні банку одночасно різними особами з метою переказу коштів на один рахунок; зняття з рахунку великих готівкових сум для розрахунків готівкою з партнерами без підтверджуючих документів; часті дрібні фінансові транзакції по зняттю з рахунків готівки у одному відділенні банку одночасно різними особами; невеликі фінансові транзакції по зняттю готівки з рахунку у різних відділеннях банку; готівкові фінансові транзакції по зняттю великої суми коштів з рахунку, який був неактивним тривалий час; готівкові фінансові транзакції щодо зняття значної суми коштів з рахунку, на який кошти зайшли з-за кордону; неодноразові готівкові фінансові транзакції на значні круглі суми; фінансові транзакції щодо повного зняття готівки одразу з рахунків різних клієнтів через один банкомат; валютні фінансові транзакції готівкою щодо купівлі, продажу, конвертації; невідповідність сум транзакцій готівкою по клієнтському рахунку його КВЕДу та обсягам господарської діяльності; не притаманний для КВЕДу клієнта значний обіг по рахунку готівкових коштів; постійний обмін значної кількості дрібних готівкових коштів на крупні;

постійні фінансові транзакції по внесенню на рахунки дрібних сум значної кількості з їх наступним зняттям з рахунку однією суттєвою сумою; обіг коштів по рахунку клієнта з ознаками циклічності; проведення фінансових транзакцій готівкою таким чином, щоб уникнути обов'язкові вимоги до порогових фінансових транзакцій; виконання готівкових фінансових транзакцій через термінали самообслуговування чи банкомати у великих обсягах протягом одного дня.

5. Кредитні фінансові транзакції: байдужість особи до умов кредиту, відсоткової ставки, розмірів платежів, переплати по кредиту, штрафних санкцій та ін.; необгрунтована оплата кредиту третьою особою; нецільове використання кредитних коштів; спрямування кредитних коштів на цілі, що не відповідають діяльності клієнта; економічне незрозуміла мета отримання кредиту; необгрунтований кредит під депозит на значну суму; забезпеченням по кредиту є майно не пов'язаних з клієнтом третіх осіб; погашення простроченого кредиту за рахунок коштів, які отримані клієнтом з невідомих джерел; погашення довгострокового кредиту у дуже малий термін часу.

6. Зовнішньоекономічні фінансові транзакції: місце доставки товару згідно зовнішньоекономічного контракту знаходиться у країні підвищеного рівня ризику фінансування тероризму, відмивання нелегальних коштів; країна транзиту товару згідно зовнішньоекономічного контракту належить до країн підвищеного рівня ризику фінансування тероризму, відмивання нелегальних коштів; незрозуміле проходження товар транзитом через певні країни; незрозуміле ускладнення структури фінансової транзакції; економічно необгрунтований імпорт чи експорт товарів; необгрунтовано висока чи низька ціна на товар чи послугу; недостовірна інформація стосовно кількості експортних чи імпортних товарів; неправдиві дані по різновиду товарів, що імпортуються чи експортуються; підозріло часті чи досить суттєві зміни до умов акредитиву.

7. Фінансові транзакції з цінними паперами: фінансові транзакції з купівлі/продажу фінансових інструментів згідно неринкових цін; регулярне

здійснення фінансових транзакцій щодо фінансових інструментів в невеликий проміжок часу, по неринковій ціні, з конкретно обраними контрагентами; фінансові транзакції на великі суми щодо купівлі чи продажу цінних паперів, що є неліквідними; фінансові транзакції у значних сумах по купівлі чи продажу цінних паперів, по яким складно встановити ринкову ціну; регулярне здійснення збиткових фінансових транзакцій купівлі-продажу цінних паперів за короткий проміжок часу по ціні покупки досить високій, а ціні продаж досить низькій; регулярне здійснення фінансових транзакцій купівлі-продажу цінних паперів за короткий проміжок часу при ціні продаж суттєво вищою за ціну покупки; економічно недоцільні операції з купівлі/продажу цінних паперів; необгрунтовано складний, заплутаний чи економічно недоцільний характер фінансових транзакцій з цінними паперами; значні суми фінансових транзакцій з купівлі або продажу цінних паперів закритого випуску з невідомим емітентом; суттєві обсяги фінансових транзакцій з купівлі або продажу цінних паперів закритого випуску з емітентом, пов’язаним з клієнтом; невиправдано стрімке зростання портфеля цінних паперів протягом короткого проміжку часу; позабіржові фінансові транзакції з купівлі чи продажу цінних паперів без проведення оплати проти поставки; одержання чи переказ цінних паперів від одного контрагента на постійній основі не пов’язаним між собою клієнтам; нетиповий термін розрахунку (більше двох тижнів); відсутність по рахунку клієнта, який постійно одержує перекази з інвестиційного прибутку, фінансових транзакцій по перерахування відповідних сум коштів на придбання цінних паперів брокеру; явні невідповідності, неточності у підтверджуючих документах клієнта по фінансовим операціям з цінними паперами; не достовірний вигодоодержувач за операціями з цінними паперами, проведення транзакції на користь невідомої третьої особи; наявні від суб’єкті фінансового моніторингу, держаної служби фінансового моніторингу, правоохоронних органів, офіційні запити щодо загроз проведення транзакції з метою легалізації незаконних доходів.

8. Депозитарні послуги: використання сейфа за довіреністю; один клієнт користується трьома і більше сейфами одночасно; нетипова поведінка клієнта при користуванні депозитарієм; різкі очевидні зміни у характері та строках відвідування клієнтом депозитарію; знаходження у депозитарії необгрунтовано великий проміжок часу; використання сейфу юридичною особою чи підприємцем, для господарської діяльності якого не притаманне користування такою послугою; клієнт спочатку відвідує депозитарій, і одразу після цього вносить на рахунок готівкові кошти.

9. Фінансові транзакції online: використання IP-адреси не пов'язаними між собою клієнтами при здійсненні операцій за допомогою Інтернет-клієнт-банку; доступ до Інтернет-клієнт-банку клієнта третьої невідомої банку особи; використання Інтернет-клієнт-банку користувачем за межами України без повідомлення про це банку.

10. Ситуативні фінансові транзакції: перерахування коштів на відрядження суб'єктом господарювання на рахунки фізичних осіб, при чому такі фізичні особи не працюють, задіяні у кримінальних справах; відкриття на неіснуючих робітників зарплатних карток чи відкриття каток на працівників фіктивного суб'єкта господарювання, з наступним регулярним зарахуванням на ці рахунки значних сум оплати праці, а потім їх зняття готівкових коштів з цих рахунків у банкоматі чи у касах банку; зняття готівкових коштів на подальше придбання сільськогосподарських товарів коротким терміном зберігання і можливістю досить швидкого їх списання як прострочених, при чому такі товари потім купуються за довіреністю у значної кількості сільськогосподарських суб'єктів у далеко розташованих місцевостях на незначні суми, що є доволі складним для перевірки відповідними структурами; операції зняття з рахунку коштів на не конкретизовані господарські витрати, придбання чітко не казаних товарів, послуг, товарно-матеріальних цінностей, справжня мета яких є виведення безготівкових коштів у готівкові; операції зі зняття готівкових коштів згідно вкладного договору з фізичною особою, видача дивідендів, виплата безвідсоткової фінансової допомоги, що

проводяться в короткий строк після укладання угоди; специфічні операції з видачі коштів з платіжних карток (метою зняття готівкових коштів є подальша купівля цінних паперів суб'єктів, що насправді є фіктивними; спочатку кошти безготівково заходять на рахунок як поворотня фінансова допомога, а потім знімаються готівкою; зняття готівкових коштів з рахунку фізичною особою як особисті заощадження; відкриття та наступне зняття готівкових коштів з корпоративних карток у різних регіонах на паливо, сільськогосподарську продукцію, але справжньою метою таких операцій є оперативний доступ до готівки); видача коштів з призначенням на інші цілі без конкретизації; виплата орендної плати за паї, без вказання кому, в яких сумах, згідно яких договорі та ін.; видача коштів за металобрухт, макулатуру, перевірити який майже неможливо; виплата коштів на оплату неуточнених послуг; виплата коштів на благодійну допомогу; проведення операцій з ознаками розбиття операцій на менші суми з етою уникнути законодавчих обмежень щодо фінансового моніторингу та інші.

11. Схемні фінансові транзакції:

- Переказ коштів з рахунку суб'єкта господарювання в одному банку на рахунок цього ж суб'єкта господарювання в іншому банку, при чому призначення платежу – переказ коштів на власний рахунок → переказ суб'єкт господарювання переказує кошти ряду своїм працівникам – фізичним особам на корпоративні карти як фінансову допомогу → фізичні особи виводять кошти з рахунку у готівковій формі.
- Переказ коштів між рахунками ряду суб'єктів господарювання як платіж за металобрухт, сільськогосподарські товари, товарно-матеріальні цінності, фінансова допомога, будівельні товари → кошти на рахунка накопичуються у загальні суми → готівкові кошти на загальну суму знімаються по довіреності у касах банку чи банкоматах (при чому переважна частина суб'єктів господарювання нещодавно створені; посадові особи та засновники це одна особа; між посадовими та довіреними особи простежується родинний зв'язок; особи, на яких надано довіреність, офіційно є засновниками, керівництвом,

бухгалтерами інших суб’єктів господарювання; особа, що діє по довіреності, офіційно не працевлаштована у суб’єкта господарювання; податкові платежі не сплачено, офіційно зафіксованих доходів немає у поданій звітності; операції по зняттю готівкових коштів проводились в той же день, коли кошти зайшли на рахунок; присутнє готівкове зняття коштів однією особою через каси банку, банкомати).

- Переказ коштів від одних суб’єктів господарювання, ряду інших суб’єктів господарювання (при чому у суб’єктів господарювання посадова особа та засновник є однією особою, чи статутний капітал яких є доволі малим, чи мають несплачені податки, чи незадекларовані доходи), з певним різним призначенням за послуги, за газ, за пшеницю, фінансова допомога → зняття таких коштів на придбання сільськогосподарських товарів або перерахування як фінансову допомогу певним фізичним особам з їх подальшим готівковим виведенням.
- та інші.

Так, коректне оцінювання причинно-наслідкових зв'язків, що виникають між фінансовими транзакціями та фінансовими злочинами у системі фінансово-економічних взаємовідносин економічних агентів, суб’єктів фізичних та юридичних осіб, регулюючих та контролюючих органів, як на мікро, так і на макро рівні, побудова ефективних моделей оцінки таких зв’язків, має відповідати певним особливостям, характеристикам та вимогам. Це дозволить максимально об'єктивно ідентифікувати, визначати, відображати наявні процеси, дії, що відбуваються в цій системі, усвідомлювати можливі наслідки, забезпечити захист від загроз, і в кінцевому результаті формувати певні вектори та напрямки мінімізації ризиків, розвитку ринку фінансів, національної економіки, стабілізації економічної системи взагалі.

2 КІБЕРШАХРАЙСТВА У СФЕРІ ФІНАНСОВИХ ПОСЛУГ: ТРЕНДИ ТА ЗАКОНОМІРНОСТІ

2.1. Тенденції та закономірності поширення кіберзлочинності: бібліометричний аналіз

Забезпечення кібербезпеки є постійно зростаючою проблемою для фінансових установ та національних фінансових регуляторів. На сьогодні протидія кіберзагрозам є однією із головних тем для обговорення на міжнародних економічних форумах і конференціях, дана проблематика широко висвітлена у працях зарубіжних вчених.

Кібершахрайство та легалізація доходів, набутих злочинними способами, представляє загрозу економічній безпеці будь-якої країни, вона набуває глобального характеру, оскільки різні схеми відмивання грошей мають міжнародний характер та містять зв’язок з організованою злочинністю. Саме тому розвиток сучасної економічної науки неможливий в межах ізольованої території окремої країни. Виходячи з цього, основою бібліометричного аналізу виступила міжнародна база даних наукових публікацій Scopus.

З метою проведення більш ґрунтовного дослідження визначення підходів до протидії кіберзагрозам у фінансовому секторі проведено бібліометричний аналіз за допомогою інструментарію VOSViewerv.1.6.10), що дозволяє ідентифікувати взаємозв’язки між об’єктами, проводити кластеризацію і візуалізацію наукометричних даних. Об’єктом бібліометричного аналізу обрано 3328 наукові статті, які відповідають одночасному врахуванні в пошуковому запиті таких категорій як «cyber» та «financial», за період 1993–2021 рр. у виданнях, що індексуються наукометричною базою даних Scopus. Дослідження засвідчило, що зростання кількості публікацій, присвячених дослідженню інформаційним питанням у фінансовому секторі, почалося з стрімкого зростання у 2013 році та залишається актуальним й дотепер. У 2020 році опубліковано 328 публікації з

даної проблематики, проіндексованих науковометричною базою Scopus, що у 5,6 рази більше порівняно з 2013 роком. За результатами аналізу частоти використання ключових слів з цієї проблематики у наукових статтях виокремлено три кластери: кластер 1 –кібербезпека та складові її забезпечення (червоний колір, рис. 1), кластер 2 – ідентифікація кіберзагроз (зелений колір, рис. 1), кластер 3 – концепція Industry 4.0 та її вплив на сферу фінансових послуг (синій колір, рис. 2.1).

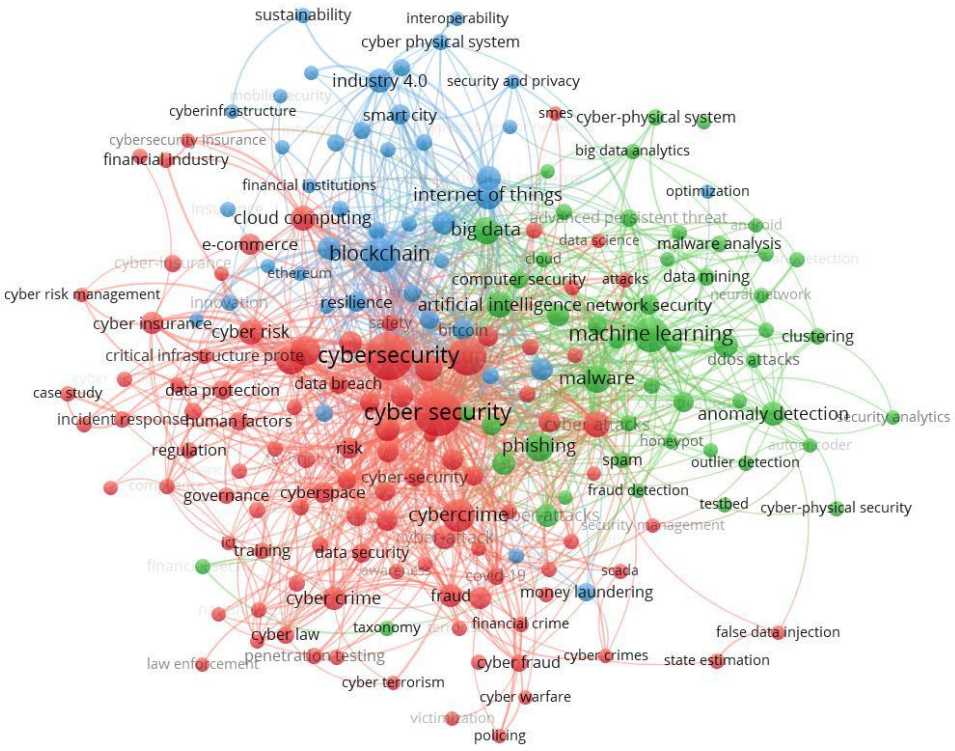


Рисунок 2.1 – Результати бібліометричного аналізу наукових праць з питань кіберзахисту у фінансовому просторі за 1992–2021 рр. у виданнях, що індексуються наукометричною базою даних Scopus (інструментарій VOSViewerv.1.6.10)

Крім цього, проведено аналіз міжнародних науково-дослідних центрів, які займаються вивченням даної проблематикою, за географічною ознакою. Третина публікацій з даної проблематики (547 публікації) опублікована науковцями США, тоді як 10,6% публікацій – Індії, 8,5 % – Великобританія, близько 5% – Австралія та Китай. Дані цифри наочно демонструють, що

протидія кіберзагрозам залишається пріоритетним для будь-яких країн світу незалежно від рівня економічного її розвитку.

У роботі [38] представлено результати опитуваннння керівників інформаційних служб та служб інформаційної безпеки, що дозволило виокремити основні виклики, з якими стикаються малі, середні та великі підприємства в галузі фінансових послуг щодо безпеки даних та надання відповідних інструментів і стратегій для їх захисту.

На сьогодні активно впроваджують методи машинного навчання у системи захисту інформації та забезпечення кібербезпеки, які дозволяють ефективно вирішувати завдання аналізу, класифікації та прогнозування широкого класу даних. У роботі [39] проаналізовано сфери практичного застосування нейронних мереж та генетичних алгоритмів в системі управління інформаційною безпекою комерційних банків. У роботі [40] побудовано фазові профілі кібершахраїв на основі аналізу моделей їх атак шляхом використання техніки розподільної семантики обробки природної мови. А. Бердюгін та П.Ревенков [41] розробили за допомогою Borland Delphi програмне забезпечення для кількісної оцінки ймовірності ризику кібератак на технології електронного банківського обслуговування.

У роботі [42] обґрунтовано необхідність посилення інформаційної безпеки серед працівників фінансових установ. Yerdon [43] запропоновано використовувати активні індикатори відстеження очей для визначення кібершахраїв з числа працівників великих компаній.

Однією з найбільш поширених кібератак є фішинг, метою якого є викрадення конфіденційної персональної та фінансової інформації. Науковцями [44] запропоновано модель класифікатора фішингової електронної пошти, яка застосовує алгоритми глибокого навчання з використанням згорткової мережі графів (GCN). Експериментальні тести підтвердили, що класифікатор ідентифікував фішингові листи з точністю 98,2%.

Найчастішою причиною зараження шкідливим програмним забезпеченням і порушення конфіденційності є соціальні мережі [45].

На думку П. Андреу і С. Аніфантакі [46] одним із факторів стрімкого поширення кіберзагроз є низький рівень цифрової та фінансової грамотності, а також недостатня обізнаність населення про кібератаки та їх потенційні руйнівні наслідки. Зокрема, у роботі [47] визначено набір навичок кібербезпеки не-ІТ-спеціалістів, які дозволяють зменшити ризики інформаційній безпеці компанії.

Науковцями С. Твенебоа-Кодуа & С. Тосун [48], М. Аркурі [49] оцінено вплив кібератак на динаміку зміни вартості цін на акції компаній залежно від їх галузевої приналежності. Доведено, що кібератака на фінансові компанії призводить до значної волатильності їх акцій протягом тривалого періоду часу [48].

Один із напрямів бібліометричного аналізу наукових досліджень є огляд публікаційної активності в сфері «ефективність ідентифікації кібершахрайств» (рис. 2.2) [50, 2].

Аналізуючи результати змістовно-контекстуального блоку бібліометричного аналізу зауважимо, що основний масив наукових досліджень сконцентрований на ідентифікації взаємозв’язків між ефективністю кібершахрайств і протидією відмиванню коштів, здобутих злочинним шляхом (жовтий кластер), злочином й оцінкою ризику (фіолетовий кластер), коштами, здобутих злочинним шляхом (блакитний кластер), блокчейном і системою управління (червоний кластер), комп’ютерною злочинністю (зелений кластер), фінансовими установами (оранжевий кластер), а також безпекою даних (синій кластер) [2].

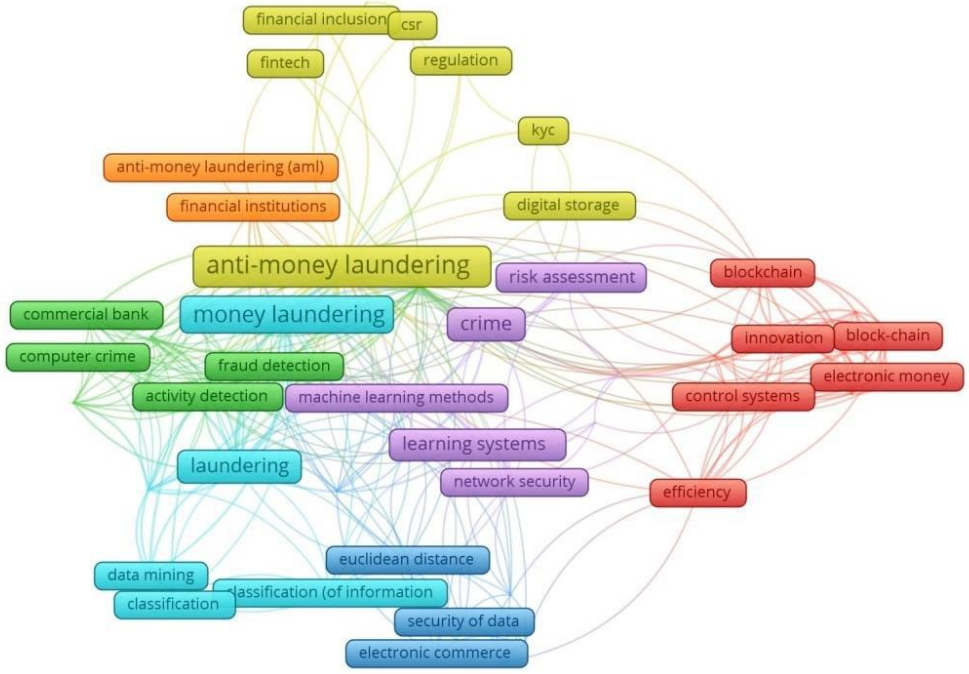


Рисунок 2.2 – Наукова бібліографія поняття «efficiency cyber fraud» (ефективність кібершахрайств) із застосуванням програми VOSviewer 1.6.15 за період з 2010 по 2020 рр.

Отже, основоположними категоріями у досліджені ефективності кібершахрайств є такі категорії як «протидія відмиванню коштів», «кошти, здобуті злочинним шляхом», «злочин» тощо. Це доводять також дані, зображені на рисунку 2.3.

На основі даних рисунку 2.3 зазначимо, що основний взаємозв'язок ефективності кібершахрайств та ефективості протидії відмиванню коштів відбувається за рахунок реалізації наступних ланцюгів: через здійснення протидії легалізації кримінальних доходів у фінансовій сфері (жовтий кластер); через кіберзлочини в сфері електронної комерції (червоний кластер); через кібератаки на персональні комп'ютери фізичних й юридичних осіб (зелений кластер) [2].

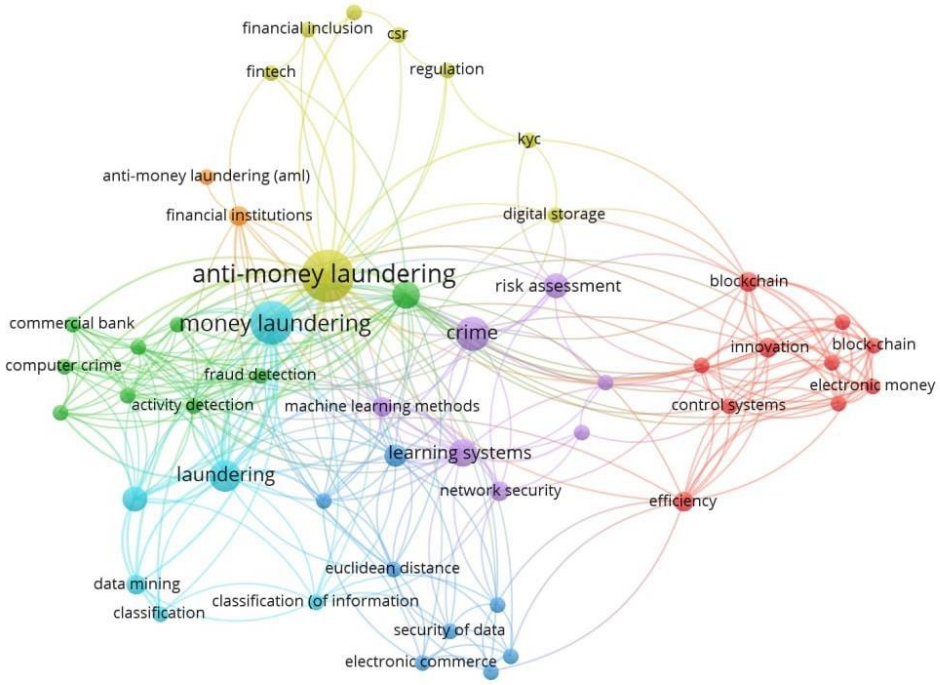


Рисунок 2.3 – Наукова бібліографія перетину понять «efficiency cyber fraud» (ефективність кібершахрайств) та «efficiency anti-money laundering» (ефективність протидії відмиванню коштів) за 2010-2020рр.

Розширюючи дослідження, проаналізуємо контекстуально-часовий блок бібліометричного аналізу (рисунок 2.4). Насиченість кольору на рисунку 2.4 змінюється від темно-фіолетового кольору (ранні публікації) до жовтого кольору (сучасні публікації).

Отже, за результатами контекстуально-часового аналізу з питань ефективності кібершахрайств встановлено три етапи зміни векторів дослідження, зокрема: у 2010–2013 роках науковці намагалися чітко зрозуміти та визначити як трактувати поняття «кібершахрайство», його види. Упродовж 2014–2018 років дослідників хвилювали питання протидії кібершахрайствам, оцінки ризиків його виникнення та встановлення контролю за фінансовими інститутами в рамках протидії легалізації коштів, здобутих злочинним шляхом. У 2019–2020 рр. з розвитком електронних коштів і блокчейну основна увага почала приділятися фінансовим технологіям і протидії вчинення кібершахрайств у сучасних реаліях [2].

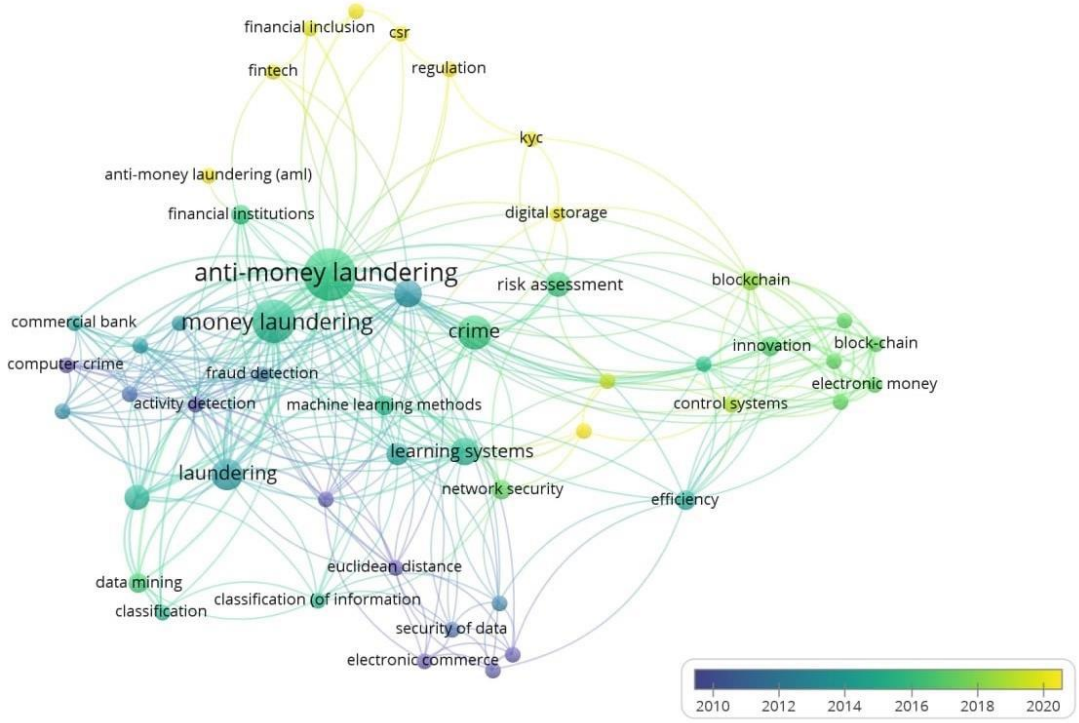


Рисунок 2.4 – Візуалізаційна карта контекстуально-часового виміру досліджень з питань ефективності кібершахрайств за 2010–2020 рр. у виданнях бази даних Scopus

2.2. **Сучасні тенденції поширення кіберзлочинності у фінансовій сфері в Україні та світі**

Фінансовий сектор здійснює обслуговування економічних відносин широкого кола учасників: державні та приватні установи та організації, їх працівників та клієнтів, інших фінансових посередників тощо. Від усіх цих учасників до фінансових установ потрапляє персональна інформація, комерційні дані, фінансова інформація тощо. Але, враховуючи сучасні технологічні можливості, існують особи та/або угрупування, що прагне скористатися такими ресурсами у незаконних цілях, виникає загроза того, що конфіденціальна інформація може бути зламана та потрапити до злочинців шляхом здійснення кіберзлочинів. А з огляду на стрімке використання цифрових продуктів в умовах пандемії, то проблема кіберзлочинності дедалі

загострюється і постає однією з головних загроз репутації, безпеці та економіці нації [51].

Динамічна цифровізація економіки робить банківські та небанківські фінансові установи більш вразливими до кіберзлочинності. Банки – це фактично «кровоносна система» національної економіки, через яку здійснюється обслуговування інтересів держави (виконання державного і місцевих бюджетів, отримання міжнародної допомоги, надання субсидій тощо), суб'єктів господарювання різних галузей економіки, а також громадян суспільства. З урахуванням цього, банківські установи акумулюють значну за обсягом інформацію від своїх клієнтів. У разі порушення інформаційної безпеки фінансових установ конфіденційні дані можуть бути використані для здійснення протиправної діяльності або продані на темних веб-майданчиках, що може призвести до втрати ділової репутації як фінансових установ, так і їх клієнтів [52].

У 2020 році збитки від кіберзлочинів у США оцінюються в 4,2 млн дол США, що вдвічі більше порівняно з 2018 роком (2,7 млн дол США). При цьому впродовж останніх років фінансові послуги були та залишаються основним таргетом для кіберзлочинців. IBM щорічно визначає індекс загроз (X-Force Threat Intelligence Index), який відображає ландшафт кіберзагроз у світі (табл. 2.1).

На основі даних про атаки та інциденти з порушення інформаційної безпеки з керованих мереж X-Force, а також про публічно розкриті кіберзлочини фахівцями IBM встановлено, що найбільш вразливими у 2020 році були сфери фінансів, виробництва та енергетики.

У 2019 р. 39% громадян ЄС, які користувалися Інтернетом, зіткнулися з проблемами безпеки у віртуальному просторі. Значення даного показника значною мірою коливається в різних державах-членах: більше 50% у Великобританії та 10% у Литві [54]. З урахуванням зазначених тенденцій, країни ЄС активно вкладають кошти для удосконалення інфраструктури,

проведення просвідницьких заходів щодо підвищення рівня цифрової культури серед населення та бізнесу.

Таблиця 2.1 – Рейтинг вразливості сфер діяльності до кіберзлочинів у період з 2018 по 2020 рр.

	2018	2019	2020	Зміна, 2020/2018
Фінансові послуги	1	1	1	-
Виробництво	5	8	2	-3
Енергетика	10	9	3	-7
Роздрібна торгівля	4	2	4	-
Професійні послуги	3	5	5	+2
Адміністративні послуги	7	6	6	-1
Охорона здоров'я	8	10	7	-1
Медіа	6	4	8	+2
Транспорт	2	3	9	+7
Освіта	9	7	10	+1

Джерело: складено авторами на основі даних [53]

Забезпечення безпеки інформаційних технологій фінансових установ та їх баз даних є постійно зростаючим викликом для топ-менеджменту як фінансових установ, так і національного регулятора. Хоча програмне забезпечення поступово стає все більш безпечним, а розробники створюють нові підходи до кібербезпеки, зловмисники також удосконалюють технології здійснення зловмисних діянь. З метою протидії кіберзагрозам у фінансовому секторі економіки доцільно проаналізувати найбільш поширені способи здійснення кібератак, інструменти монетизації викрадених даних, а також основних кіберзлочинців та їх мотивів.

Найбільш поширеними формами здійснення кібератак у фінансовому секторі є програма –вимагач (ransomware), атака ланцюга поставок (supply chain attack) прихований майнінг (cryptojacking), а також програми для відволікання уваги служб безпеки від справжнього епіцентру кібератаки (destractive attack) [55].

Одним з найбільш розповсюджених методів для викрадення грошей безпосередньо з рахунків компаній - це BEC-афера (Business Email Compromise). Принцип роботи BEC-афери наступний: кіберзлочинець вводить

в оману співробітника компанії, який має доступ до конфіденційної інформації, з вимогою зробити переказ коштів на рахунок, який начебто належить клієнту, або контрагенту компанії, проте кошти перенаправляються на рахунок кримінальної організації. У 2020 році збитки від BEC-афер та EAC-афер (Email Account Compromise), які є аналогом BEC-афер для фізичних осіб, у США оцінені на рівні 1,8 млрд дол США (або 36% від загальної суми збитків від кіберзлочинів), тоді як у 2019 році – 1,7 млрд дол США (або 48,57% від загальної суми) [56, 57].

У переважній більшості випадків кібератаки у фінансовому секторі здійснюються за участю таких суб'єктів як [58, 52]:

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

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

– держава та її шпигуни, які здійснюють незаконну діяльність з метою оборони, встановлення геополітичних інтересів, впливу на громадську думку на національному на міжнародному рівнях та інше.

У таблиці 2.2 представлено найбільші кіберзлочинні угруповання, які атакують фінансові установи в світі.

Нині для легалізації доходів, отриманих внаслідок кіберзлочину, в переважній більшості використовується криптовалюта. У 2018 році в Європі за допомогою криптовалют було легалізовано 4 млрд фунтів стерлінгів. Криптовалюта за своєю суттю має низький рівень регулювання і не контролюється центральним органом, і тому фінансові транзакції не можуть бути ретельно відслідковані [4].

Для виявлення, знешкодження, мінімізації та попередження кіберризиків, науково-практичним світовим співтовариством вживаються різноманітні заходи для боротьби з можливими кібератаками. А ефективність

вжиття механізмів протидії кібершахрайствам напряму залежить, в першу чергу, від виявлення закономірностей здійснення кібератак з досвіду країн світу.

Таблиця 2.2 – Найбільші кіберзлочинні угруповання, які здійснюють атаки на фінансові установи, у світі [59]

Назва	Рівень складності кібератак	Жертви	Особливості кібератак
Money Taker (Російська Федерація)	група використовує власні інструменти кібератак, шкідливе програмне забезпечення, яке працюватиме і після перезавантаження. здійснює налаштування загальнодоступних інструментів для своїх потреб.	банки, компанії, що надають послуги та/або технології фінансовим установам	більше 20 успішних атак на банки, фінансові установи та юридичні компанії в США, Великобританії та Росії.
Carbanak (Російська Федерація)	угруповання використовує шкідливе програмне забезпечення, яке надає широкий спектр можливостей: авторизація, зчитування даних банківських карток, особистої інформації.	Банки, фінансові компанії, компанії з електронної комерції / роздрібної торгівлі	понад 300 успішних атак на банки, фінансові установи та роздрібних торговців, у тому числі на систему Oracle
Lazarus Group (Північна Корея)	група має потужні можливості, а саме технології ухилення корпоративних систем кіберзахисту, трирівневі атакуючі сервери, зашифровані комунікації.	Банки, фінансові компанії, урядові структури	атака на Sony Pictures, розробник програми, атака на SWIFT (1 млн дол США), Центральний банк Бангладеша (81 млн дол США) ті інші.

На сьогоднішній день при виявленні певних закономірностей фахівцями проводиться обробка баз даних великих розмірів, що потребує розробки певних моделей, здатних опрацьовувати суттєві інформаційні ресурси. А одним з найефективніших вирішень цього питання є використання асоціативних правил та їх пристосування до вивчення досліджуваних питань.

Асоціативні правила – це дуже потужна технологія, що дозволяє виявляти взаємозв'язки між пов'язаними подіями або елементами. Вони

описуються у вигляді: $X \to Y, X \cap Y \to \emptyset$. При чому, будь-яке асоціативне правило можна представити двома основними характеристиками [60]:

- підтримка (опора) $supp(X \to Y)$ асоціативного правила $X \to Y$ виступає значенням, що дорівнює відношенню кількості записів $X \cup Y$ в базі даних D, до загальної кількості записів у базі даних;

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

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

– міжвимірні асоціаціативні правила, тобто правила між атрибутами різних вимірів (формула 2.1)[61]:

$$(A_I^x \in D_I) \wedge \ldots \wedge (A_J^y \in D_J) \to A_K^z \in D_K, \quad (2.1)$$

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

$D_I - I^{th}$ - є розмірністю,

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

m_i - кількість атрибутів I^{th}-виміру; A_I^X - певний атрибут I^{th}-виміру.

– внутрішньовимірної асоціаціативні правила, тобто правила асоціації в межах одного виміру (формула 2.2) [61]:

$$(A_I^x \in D_I) \wedge \ldots \wedge (A_I^y \in D_I) \to (A_I^z \in D_I) \wedge \ldots \wedge (A_I^v \in D_I), \quad (2.2)$$

де I = 1..n; де n - кількість розмірів,

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

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

– гібрідні асоціативні правила, тобто можливі залежності між вимірами, при чому певні операнди можуть представляти атрибути одного виміру (формула 2.3) [61]:

$$(A_I^x \in D_I) \wedge \ldots \wedge (A_J^y \in D_J) \rightarrow (A_J^y \in D_J) \wedge \ldots \wedge (A_K^z \in D_K), \qquad (2.3)$$

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

Розглянемо отримані закономірності здійснення кібератак в країнах ЄС на основі використання асоціативних правил у вигляді наступної послідовності етапів [51]:

1 етап. Формування вхідної структури даних здійснення кібератак на основі застосування методу логічного узагальнення. На даному етапі проводиться збір та систематизація даних щодо характеристик кібератак протягом 2005-2020 рр. (табл. 2.3).

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

в обслуговуванні. Дані кібератаки були здійснені на об’єкти різних сфер: публічний та приватний сектор, військовий сектор, громадянське суспільство.

Таблиця 2.3 – Фрагмент вхідної структури даних здійснення кібератак

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

Наступним кроком є проведення поглибленого аналізу кібератак на території Європейського Союзу на основі використання асоціативних правил. Для реалізації даного етапу використано програмний продукт STATISTICA 10. Отримані результати представимо у вигляді рисунку 2.5.

На основі даних, отриманих шляхом побудови асоціативних правил, представлених на рисунку 1, можна зробити наступні висновки: в 77,14% випадків шпіонаж здійснюється зловмисниками з Росії, у 88,24% - з Німеччини, у 93,75% - з Китаю. Встановлено, що 84,62% шпіонажу спостерігається у галузі приватного сектору, 82,05% - у публічній сфері. При цьому частка спостережень, для яких шпіонаж здійснюється з Росії, складає 43,55%. Частка спостережень, для яких шпіонаж здійснюється як з Німеччини, так і з Китаю, становить 24,19% вибірки. У 76% випадків шпіонаж здійснюється зловмисниками з Росії в сфері публічної діяльності. Переходячи

до аналізу частоти виявлених випадків здійснення кібератак, що є суттєвим доповненням до наведених вище асоціативних правил (рисунок 2.6).

Summary of association rules (cyber-operations (EC).sta)
Min: support = 20,0%, confidence = 10,0%
Max. size of an itemset = 10

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

Рисунок 2.5 – Результати аналізу кібератак на території Європейського Союзу за допомогою асоціативних правил

Frequent itemsets computed (cyber-operations (EC).sta)
Min: support = 10,0%, confidence = 10,0%
Max. size of an itemset = 10

	Frequent itemsets	Number of items	Frequency	Support(%)
1	(Espionage	1,00000	52,0000	83,8709
2	(Government	1,00000	39,0000	62,9032
3	(Military	1,00000	9,0000	14,5161
4	(EU)	1,00000	7,0000	11,2903
5	(Private sector	1,00000	26,0000	41,9354
6	(Civil society	1,00000	9,0000	14,5161
7	(Germany	1,00000	17,0000	27,4193
8	(France)	1,00000	7,0000	11,2903
9	(Espionage, France	2,00000	7,0000	11,2903
10	(Espionage, Germany	2,00000	15,0000	24,1935
11	(Espionage, Private sector, Germany	3,00000	7,0000	11,2903
12	(Espionage, Government, German	3,00000	8,0000	12,9032
13	(Espionage, Civil society	2,00000	7,0000	11,2903
14	(Espionage, Private sector	2,00000	22,0000	35,4838
15	(Espionage, Government, Private secto	3,00000	6,0000	9,6774
16	(Espionage, EU	2,00000	7,0000	11,2903
17	(Espionage, Military	2,00000	7,0000	11,2903
18	(Espionage, Government	2,00000	32,0000	51,6129
19	(Government, Germany	2,00000	9,0000	14,5161
20	(Government, Civil society	2,00000	6,0000	9,6774
21	(Government, Private sector	2,00000	7,0000	11,2903
22	(Government, Military	2,00000	7,0000	11,2903
23	(Private sector, Germany	2,00000	8,0000	12,9032

Рисунок 2.6 – Частота виявлених випадків здійснення кібератак

Аналіз рисунку 2.6 дозволяє констатувати, що найбільша частка кіберзлочинів (62,90%) відбувається в державних структурах, наступна за

частотою галузь – приватний сектор (41,94%). Найменші частки кіберзлочинів відбуваються у військовій та суспільній сферах і становить 14,52%.

Графічне представлення причинно-наслідкових зв'язків між кібератаками проведено на основі застосування методів візуалізації та графічного дизайну. У рамках даного етапу побудовано граф виявлених на другому етапі асоціативних правил, представлений на рисунку 2.7, який дозволяє отримати візуальне представлення сутності (вісь Head означає причину, вісь Body – наслідок), ступеня підтвердженості виявлених зв'язків (колір відповідного еліпса), а також частки досліджуваної сукупності, для якої відповідне асоціативне правило характерне (величина еліпсу).

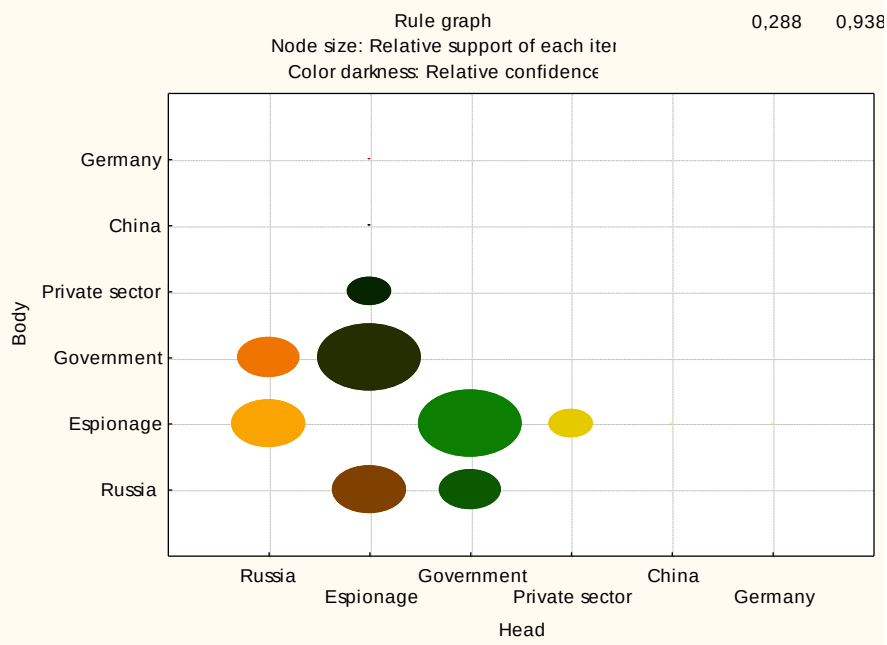


Рисунок 2.7 – Граф асоціативних правил

Переходячи до аналізу рисунку 2.7 та 2.8, то найбільшою за частотою виявлених випадків здійснення кібератак (83,87%) є шпіонаж. Серед країн, які стали жертвами кіберзлочинів, необхідно відмітити Німеччину, на частку якої припадає 27,42% випадків, в той час як для Франції даний показник на рівні 11,29% (що відбулось за рахунок шпіонажу). У середньому 11,29% країн ЄС стали постраждали від здійснення кібератак у період з 2005 по 2020 рр.

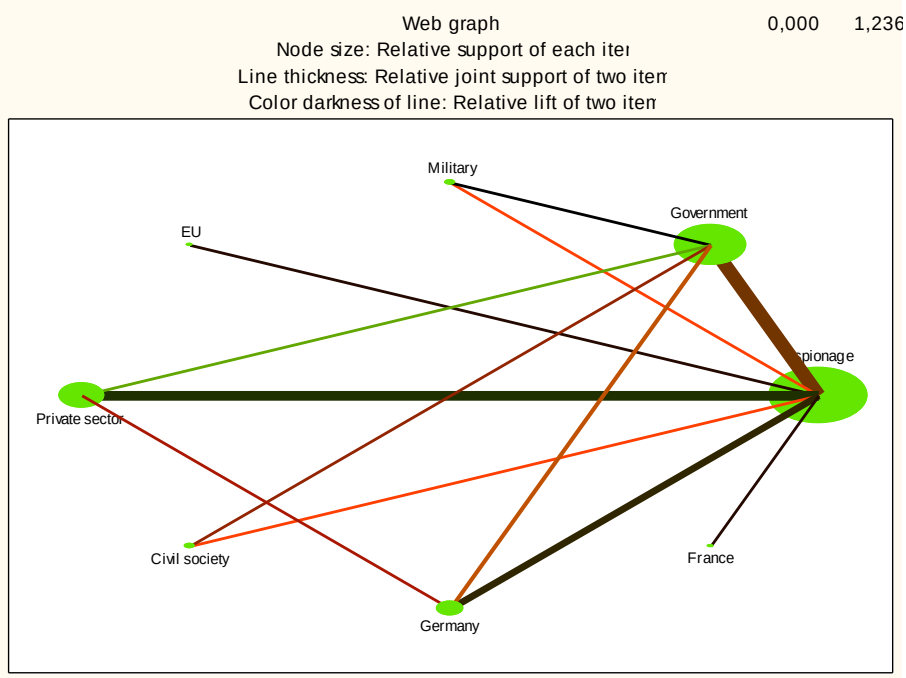


Рисунок 2.8 – Веб-граф підтримки виявлених асоціативних правил в розрізі здійснення кібератак в межах країн ЄС

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

Таким чином, обрана методологія дозволяє обробляти великі бази даних шляхом формування певних економічних алгоритмів, вирішення яких сприяє пошуку розв’язку поставленого завдання з незначними часовими витратами. Це в подальшому надасть можливість країнам приймати ефективні рішення для передбачення кіберзагроз, протидії кібератакам та забезпечення національної безпеки країн ЄС.

2.3. **Визначення детермінантів поширення кібершахрайств та незаконних фінансових операцій**

Карантинні заходи, спричинені пандемією, спровокували збільшення розрахунків в мережі Інтернет, зростання обсягів електронних фінансових послуг, нарощення використання криптовалют та альткоїнів як платіжного засобу та інвестиційного інструменту. Дані тенденції вказують на прискорення темпів цифровізації економіки та трансформації підходів до організації бізнес-процесів. За цих умов цифрова трансформація фінансових відносин відкриває як нові можливості для підвищення ефективності фінансових установ і зниження їх витрат за рахунок оптимізації транзакцій, так і загрози для стабільного їх функціонування – поширення кібератак та зростання частоти їх здійснення. У 2020 році в Україні зафіксовано близько мільйона випадків, пов’язаних з кіберзагрозами, сформовано достатньо сприятливі умови для “відмивання” брудних грошей (67 позиція з поміж 141 країни світу за даними Базельського індексу протидії легалізації), що має значущий дестабілізаційний ефект на функціонування фінансового сектору та враховуючи кроссекторальність фінансових відносин виступає загрозою для національної безпеки держави [52]. Не зважаючи на велику кількість публікацій, присвячених окресленій проблематиці, у науковій літературі досі не здійснена спроба формалізації детермінант поширення кібер шахрайства у сфері фінансових послуг.

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

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

– приведення вхідних показників до єдиного співтавного вигляду;

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

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

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

– побудова SVM-моделі машинного навчання двох типів (epsilon-SVM regression та nu-SVM regression) в розрізі чотирьох специфікацій опорних векторів: лінійні, поліноміальні, радіально -базисні функції (RBF) та сигмоподібні.

Перший етап передбачає проведення збору та систематизації статистичних даних, що характеризують фактичні кібератаки, проведені у 2020 році. Об'єктом дослідження слугували 21 країна Європи. Джерелом первинної інформації слугували дані компанії Comparitech [62]. Для відображення інтенсивності здійснення кібератак у розрізі країн Європи використано наступні індикатори: частка мобільних пристроїв, заражених шкідливим програмним забезпеченням, % (I_1); частка користувачів, атакованих вірусами троян через інтернет банкінг, % (I_2); частка користувачів, атакованих мобільними троянами-вимагателями, % (I_3); частка користувачів, атакованих банківським шкідливим програмним забезпеченням, % (I_4); частка користувачів, атакованих троянськими програмами-вимагателями, % (I_5); частка комп'ютерів, заражених принаймні однією атакою зловмисного програмного забезпечення (в Інтернеті), % (I_6); частка комп'ютерів, які стикаються принаймні з однією локальною атакою шкідливого програмного забезпечення, % (I_7); частка мобільних користувачів, атакованих через веб-джерела, % (I_8); частка атак на Telnet протокол, % (I_9); частка атак з боку криптомайнерів, % (I_{10}); частка атак на SSH протокол, % (I_{11}); частка спам-

листів за країною відправника (за рік), % (I_{12}); частка країн, на які націлені зловмисні розсилки (щороку), %(I_{13}); частка комп'ютерів, атакованих фішингом (щорічно), % (I_{14}); загальна кількість виявлених шкідливих файлів, пов'язаних із Covid 19 (I_{15}).

Зведена статистична інформація щодо випадків кібершахраства у розрізі різних методів для країн Європи представлена у додатку В (таблиця В.1), а основні результати подано в таблиці 2.7.

На основі аналізованих у таблиці 2.4 видів кібератак, зауважимо, що найбільшими країнами-жертвами у 2020 році були Іспанія, Португалія та Латвія, тоді як найменша кількість кібератак зафіксована у таких країнах як Данія, Швеція та Ірландія. Зокрема, 19,73% комп'ютерів у Португалії були атаковані таким інтернет-шахрайством як фішинг, тоді як у Данії – лише 3,26%. Перехід на дистанційний режим роботи та інтенсивне користування електронними послугами, спричиненого пандемією COVID-19, призвів до збільшення масштабів кібершахрайства у світі. Щодо країн Європи, то найбільша кількість виявлених шкідливих файлів, пов'язаних із андемією Covid 19 виявлена у Іспанії, Італії та Німеччині.

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

Таблиця 2.4 – Інформація щодо стану кіберзлочинності в європейських країнах у 2020 році у розрізі методів та способів їх здійснення

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

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

$$k_{cj} = \frac{I_{cj} - \overline{I_j}}{\sigma_j} \quad (2.4)$$

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

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

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

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

Використовуючи формулу 2.4, розраховано стандартизовані значення показників, що характеризують рівень кіберзагроз в країнах Європи, подано в таблиці 2.5.

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

$$IK_c = \sum_{j=1}^{J} \sum_{j=1}^{J} \left(k_{cj}\right)^2 \quad (2.5)$$

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

Результати обчислень за формулою (2.5) візуалізуємо на рисунку 2.9, де представимо динаміку індексу кіберзагроз у розрізі розглянутих країн Європи станом на 2020 рік, у тому числі з урахуванням впливу пандемії на захищеність інформаційного простору.

Таблиця 2.5 – Стандартизовані значення детермінант поширення кіберзагроз станом на 2020 рік

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

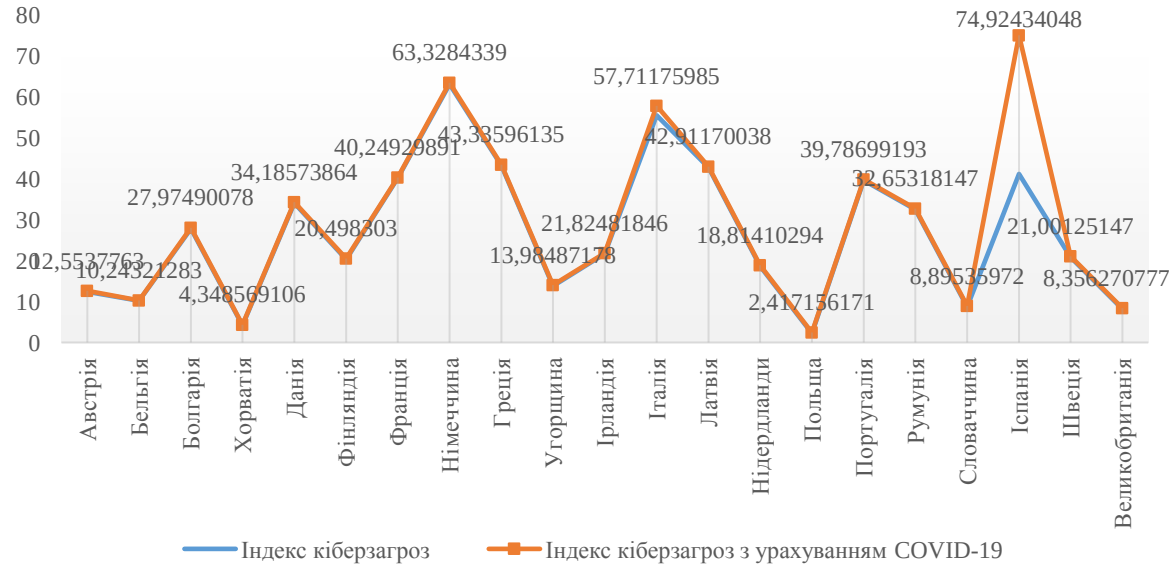


Рисунок 2.9 – Динаміка індексу кіберзагроз у розрізі країн Європи, а також з урахуванням впливу пандемії Covid 19 станом на 2020 рік

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

З метою детального аналізу динаміки інтегрального оцінювання рівня кіберзагроз у розрізі країн Європи розглянемо таблицю частот (рисунок 2.10). Так, найбільша кількість країн серед розглянутої множини характеризуються рівнем індексу кіберзагроз в межах від 0 до 10, від 10 до 20 та від 20 до 30 (по 4 країни, тобто 19,05% вибірки відповідно), що свідчить про низький рівень досліджуваного показника. Лише незначна кількість країн (всього 3 серед досліджуваної множини країн Європи) з рівнями від 50 до 60, від 60 до 70 та від 70 до 80, що свідчить про високий рівень кібернебезпеки.

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

Рисунок 2.10 – Таблиця частот індексу кіберзагроз на множині розглянутих країн світу станом на 2020 рік

Третім етапом запропонованого підходу є визначення детермінант поширенння кіберзагроз. У межах даної роботи для математичної формалізації

детермінант поширення кібершахрайств запропоновано використати наступні змінні:

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

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

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

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

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

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

Станом на 2020 рік значення вищеперерахованих показників у розрізі країн Європи подано в таблиці 2.11.

Таблиця 2.11 – Детермінанти поширення кіберзагроз кіберзагроз на множині розглянутих країн світу станом на 2020 рік

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

Джерело: складено на основі даних [63]

Провести більш детальний ґрунтовний детермінант поширення кіберзагроз дозволить побудова діаграма (рис. 2.11), яка свідчить про найбільшу волатильність індикатора Z1 (частка населення, яка користується послугами онлайн банкінгу), значення якого за 21 країнами світу коливається в межах від 11 до 95. В той же час, найменшу волатильність має індикатор Z5 (індикатор онлайн діяльності), що приймає значення в межах від 33 до 69. Зазначені висновки можна також зробити, проаналізувавши описові статистики детермінант поширення кіберзагроз у розрізі країн Європи станом на 2020 рік, представлені на рисунку 2.12.

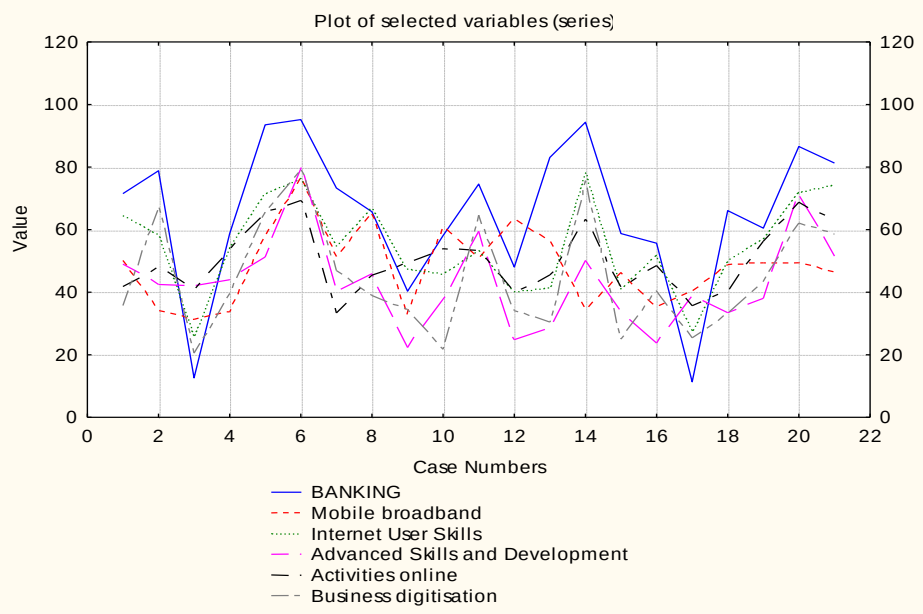


Рисунок 2.11 – Варіація значень детермінант поширення кіберзагроз на множині розглянутих країн світу станом на 2020 рік

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

Рисунок 2.12 – Описові статистики детермінант поширення кіберзагроз на множині розглянутих країн світу станом на 2020 рік

На основі рисунку 2.12 можна стверджувати, що серед розглянутих 7 детермінант поширення кіберзагроз в розрізі лише 3 (рівень розвитку мобільного широкосмугового доступу, рівень навичок населення в Інтернеті, обсяг онлайн діяльності) спостерігається однорідність розглянутої вибірки країн, оскільки значення коефіцієнту варіації не перевищує рівня 33%. В розрізі інших детермінант, а особливо інтегрального індексу кібербезпеки спостерігається досить висока нерівномірність та різновекторність країн.

Наступним етапом запропонованого науково-методичного підходу є побудова SVM-моделей машинного навчання двох типів (epsilon-SVM regression та nu-SVM regression) в розрізі чотирьох специфікацій опорних векторів: лінійні, поліноміальні, радіально -базисні функції (RBF) та сигмоподібні на базі даних вибіркової сукупності країн світу. Для реалізації даного етапу розглянемо спочатку математичне підґрунтя побудови та специфікацію зазначених моделей.

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

$$y = f(x) + noise \tag{2.5}$$

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

Тип SVM регресії 1. Для цього типу SVM модель:

$$\frac{1}{2}w^T w + C\sum_{i=1}^{N}\xi_i + C\sum_{i=1}^{N}{\xi_i}^* \to min \tag{2.6}$$

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

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

Тип SVM регресії 2. Для цього типу SVM модель:

$$\frac{1}{2}w^T w - C\left(v\varepsilon + \frac{1}{N}\sum_{i=1}^{N}(\xi_i + \xi_i^*)\right) \to min \tag{2.7}$$

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

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

$$\phi = \begin{Bmatrix} x_i \cdot x_j \quad Linear \\ (\gamma x_i \cdot x_j + coefficient)^d \quad Polynomial \\ exp\left(-\gamma(x_i - x_j)^2\right) \quad RBF \\ tanh(\gamma x_i \cdot x_j + coefficient) \quad Sigmoid \end{Bmatrix} \tag{2.8}$$

де d - ступінь поліноміального ядра;

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

коефіцієнт - коефіцієнт для поліномінального та сигмоподібного ядер;

Отже, побудуємо 8 SVM-моделей машинного навчання: двох типів (epsilon-SVM regression та nu-SVM regression) в розрізі чотирьох специфікацій опорних векторів: лінійні, поліноміальні, радіально -базисні функції (RBF) та сигмоподібні на базі даних вибіркової сукупності країн Європи. На базі порівняння фактичних та прогнозних рівнів досліджуваних детермінант поширення кібербезпеки та інтегрального індексу кіберзагроз для тестової вибірки країн обчислимо середнє квадратичне відхилення (остання графа таблиці 2.6). Таким чином, найбільш точною виступає сигмоїдної nu-SVM регресійна модель машинного навчання, яка має наступні характеристики:

SVM: Regression type 2 (C=10,000, nu=0,500), Kernel: Sigmoid (gamma=0,167, coefficient=0,000) Number of support vectors= 9 (3 bounded).

Таблиця 2.6 – Порівняння 8 побудованих SVM-моделей

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

Джерело: авторська розробка

Наступним етапом є проведення визначення детермінант поширення кіберзагроз на основі методів машинного навчання SVM за допомогою сигмоїдної nu-SVM regression моделі, яка була ідентифікована як найбільш точна та адекватна на базі країн світу тестової сукупності. Отримані результати представимо у наведених нижче рисунках 2.13-.2.15.

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

Рисунок 2.13 – Специфікація SVM-моделі кіберзагроз на множині розглянутих країн світу станом на 2020 рік

Аналіз рисунку 2.14 дозволяє констатувати наступні характеристики сигмоїдної nu-SVM regression моделі машинного навчання: кількість незалежних змінних в моделі 6, тип моделі - nu-SVM regression, Kernel type – сигмоїдна, кількість опорних векторів, які дозволяють здійснити алгоритм розпізнавання образів – 9, серед яких граничними є 3.

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

Рисунок 2.14 – Специфікація SVM-моделі визначення детермінант поширенння кіберзагроз

Аналіз рисунку 6 дозволяє констатувати наступне: серед 9 побудованих опорних векторів, найбільшу за абсолютним значенням вагу мають 2, 5 та 7 вектори. Саме тому, для визначення детермінант поширенння кіберзагроз обчислимо в розрізі кожного опорного вектора середнє арифметичне значення

за трьома обраними опорними векторами. Отже, отримаємо наступний рейтинг важливості детермінант поширенння кіберзагроз:

– частка населення, яка користується онлайн банкінгом (Z1) – 0,49;
– індикатор рівня навичок в Інтернеті (Z3) – 0,42;
– індикатор онлайн діяльності (Z5) – 0,41;
– індикатор ділової онлайн активності (Z6) – 0,21;
– індикатор поглиблених навичок та вмінь (Z4) –0,18;
– індикатор розвитку мобільного широкосмугового доступу (Z2) – 0,14.

У полі «Резюме» у верхній частині діалогового вікна «Результати» наведено специфікацію SVM-моделі, включаючи кількість опорних векторів та їх типи, а також ядра та їх параметри. Крім цього, відображаються й інші специфікації, створені в діалоговому вікні «Машини опорних векторів»: список залежних і незалежних змінних, значення навчальних констант (ємність, епсилон і nu), результати перехресної перевірки (якщо застосовно), а також статистику регресії для навчальних, тестових та загальних вибірок, таких як середній квадрат помилки, коефіцієнт стандартного відхилення та коефіцієнти кореляції (рисунок 2.15).

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

Рисунок 2.15 – Показники точності SVM-моделі визначення детермінант поширенння кіберзагроз

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

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

2.4. **Визначення взаємозв'язку між FinTech інноваціями та ризиком поширення кібершахрайства та здійснення незаконних транзакцій за посередництва фінансових установ**

В останні роки фінансові інноваційні технології, а особливо FinTech інновацій набули особливого розвитку та поширення. Так, світові інвестиції у інновації FinTech за останнє десятиріччя зросли більш ніж у три рази. Застосування FinTech інновацій передбачає розвиток найсучасніших технологічних можливостей: вбудовані мобільні системи обліку та обчислень даних, мобільні мережі, хмарні ресурси та обчислення, мобільна робота з великими базами даних, системи швидкого та комплексного аналізу великих масивів інформації. Важливе значення також має застосування FinTech для безперебійного вбудованого, дистанційного, online надання фінансових послуг та продуктів [65].

І хоча більшість світової спільноти вбачає в інноваціях FinTech значні переваги, не потрібно забувати і про виникаючі несприятливі наслідки

використання FinTech у фінансовій сфері. Так як інноваційні досягнення можуть застосовуватись і злочинною сферою та шахраями для вчинення фінансово-економічних правопорушень. Отже, серед проблемних аспектів застосування FinTech інновацій можна виділити посилення небезпеки мережевих атак, поява загроз конфіденційності, вчинення протиправних фінансових та кібернетичних дій, а також організація та здійснення легалізації незаконних доходів, виявлення та розробка шахрайських схем обігу коштів, і навіть фінансування тероризму та розповсюдження зброї масового знищення [64, 65, 66].

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

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

Одним із таких методів можна виділити сплайн-моделювання - один з найефективніших сучасних способів побудови багатокомпонентних математичних функцій та рівнянь, тривимірних 3D моделей, де сплайни представляють собою компонентні математичні функції, базові тривимірні криві, певний фундаментальний будівельний матеріал для побудови різноманітних складних функцій, тривимірних моделей. Створення сплайн-моделі передбачає побудову відповідного сплайн-каркасу, який далі виступає основою для формування почастинно заданої функції, сукупності декількох функцій, що задані множинністю значень, тривимірної геометричної поверхні, дуже складних тривимірних геометричних форм і об'єктів, тривимірних моделей [68]. Самі сплайн-лінії визначаються тривимірною сукупністю

контрольних позицій точок у просторі, що задають форму та гнучкість кривої. Базовими інструментами сплайн-моделювання є алгебраїчні многочлени, математичні змінні, найпростіші функції, сплайн-примітиви (найпростіші об’єкти, з яких формується сплайн-модель), такі як: Arc, Circle, Donut, Ellipse, Helix, Line, NGon, Rectangle, Section, Star, Text та інші більш складні сплайн-елементи. Сплайн-моделювання характеризується рядом переваг: універсальність, широке застосування, можливість використання у різноманітних обчислювальних програмних комплексах, комп’ютерному моделюванні, високі обчислювальні спроможності, наявність апроксимативних властивостей, велика точність, у випадку необхідності масштабування у будь-яких межах якість сплайн-об’єкту не погіршується, гнучке налаштування, на будь-якому етапі є можливість зміни форм сплайн-об’єктів, простота реалізації обчислювальних функцій [69].

Для досягнення мети дослідження пропонується виконати три етапи.

На першому етапі науково-методичного підходу до застосування багатомірних адаптивних регресивних MAR-сплайнів до визначення впливу факторів фінансових технологій, фінансового моніторингу як банків так і страхових компаній, обсягів торгів на біржі на фінансові правопорушення, кібернетичні правопорушення та на легалізацію кримінальних доходів формується вхідна інформаційна база дослідження. Вона містить п’ять регресорів: X1 - Показник розвитку фінтех, який представлений питомою вагою кількості абонентів мережі інтернет в чисельності населення України [69], X2 - Кількість повідомлень про підозрілі операції, взятих на облік Держфінмоніторингом [70], X3 - Загальний обсяг торгів на біржі за період, X4 - Показник діяльності страхових компаній, X5 - Показник діяльності банків; та три регресанти: Y1 - Кількість кримінальних правопорушень за статтями 222 (Шахрайство з фінансовими ресурсами) та 222-1 (Маніпулювання на фондовому ринку України) Кримінального кодексу України, досудове розслідування у яких проводилося у звітному періоді, Y2 - Кількість кримінальних правопорушень за статтями 361 (Несанкціоноване

втручання в роботу електронно-обчислювальних машин (комп’ютерів), автоматизованих систем, комп’ютерних мереж чи мереж електрозв’язку), 361-1 (Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут), 361-2 (Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп’ютерах), автоматизованих системах, комп’ютерних мережах або на носіях такої інформації), 362 (Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп’ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї), 363 (Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється), 363-1 (Перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку) Кримінального кодексу України, досудове розслідування у яких проводилося у звітному періоді, Y3 – Кількість кримінальних правопорушень за статтею 209 (Легалізація (відмивання) доходів, одержаних злочинним шляхом) Кримінального кодексу України, досудове розслідування у яких проводилося у звітному періоді [71]. Для дослідження пропонується побудувати окремо сплайн-модель в розрізі кожного із зазначених регресантів, беручи в якості регресорів один і той же набір показників. В якості часового діапазону дослідження запропоновано обрати квартальні дані з 1 кварталу 2013 р. по четвертий квартал 2020 р. (рис. 2.16, 2.17)

На другому етапі науково-методичного підходу до застосування багатомірних адаптивних регресивних MAR-сплайнів до визначення впливу факторів фінтех, фінансового моніторингу як банків так і страхових компаній, обсягів торгів на фінансові правопорушення, кібернетичні правопорушення,

легалізація кримінальних доходів проводиться дослідження динаміки поведінки як регресора, так і факторів. Для реалізації даного етапу побудуємо відповідні діаграми за допомогою інструментарію Statistics, Advanced Linear/Nonlinear Models, Time Series/Forecasting, Time Series ARIMA dialog. Даний етап виступає підготовчим для проведення безпосереднього сплайн-моделювання в розрізі визначення специфікації шуканої функціональної залежності.

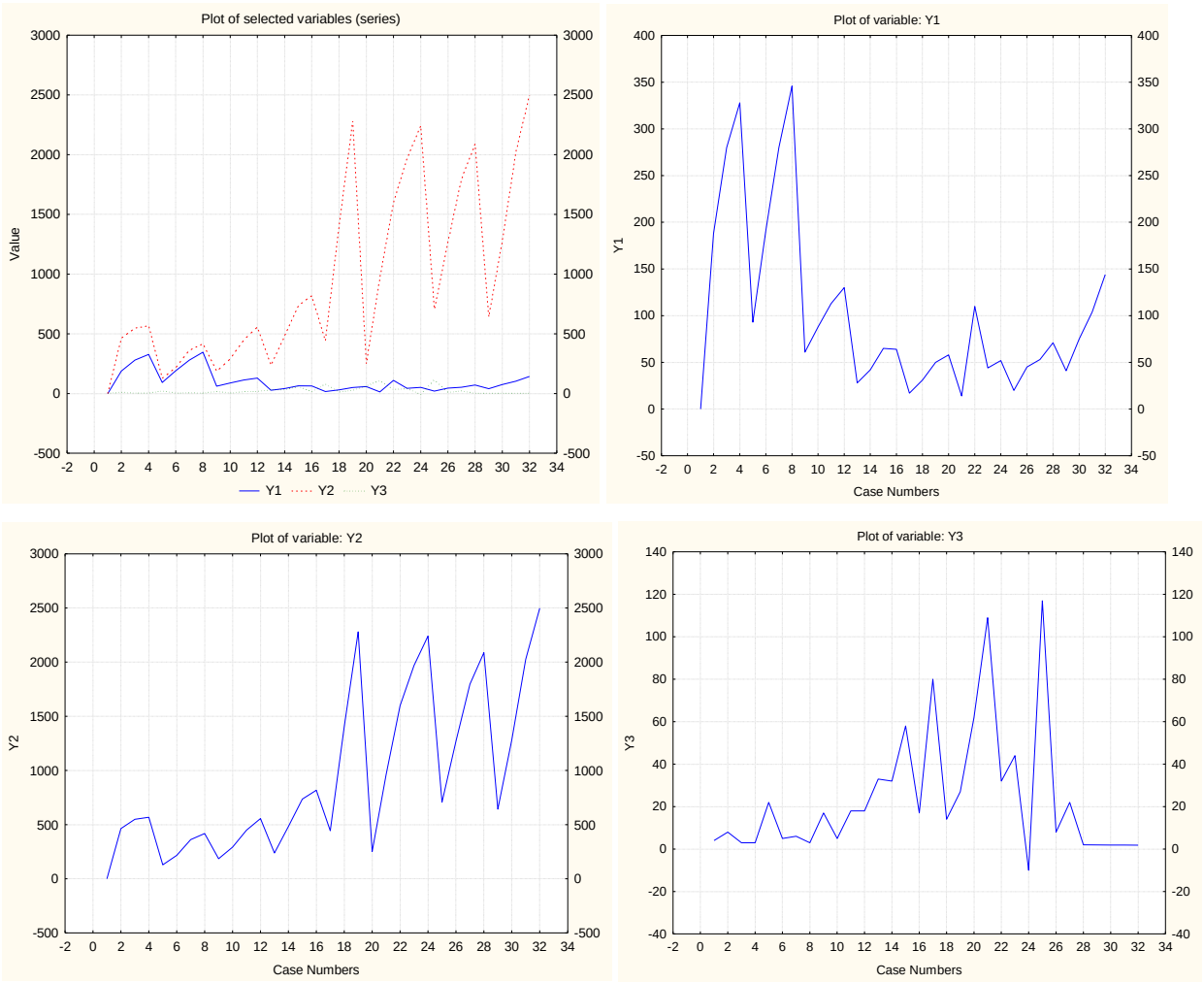


Рисунок 2.16 – Графіки динаміки регресанів визначення впливу факторів фінтех, фінансового моніторингу як банків так і страхових компаній, обсягів торгів на фінансові правопорушення, кібернетичні правопорушення, легалізація кримінальних доходів

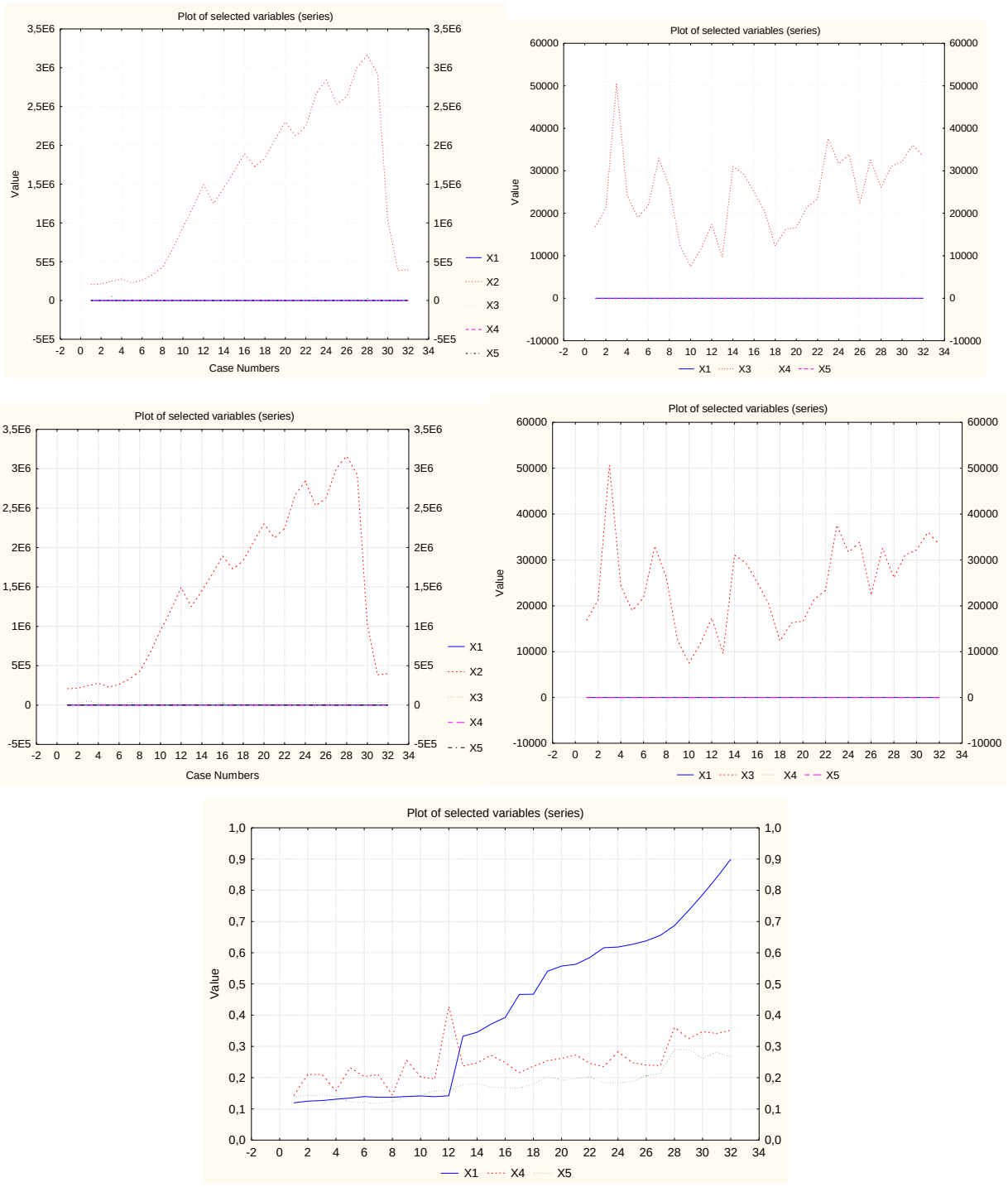


Рисунок 2.17 – Графіки динаміки регресорів визначення впливу факторів фінтех, фінансового моніторингу як банків так і страхових компаній, обсягів торгів на фінансові правопорушення, кібернетичні правопорушення, легалізація кримінальних доходів

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

Багатомірні адаптивні регресивні MAR-сплайни – це непараметрична процедура формалізації залежності по набору базисних функцій та коефіцієнтів, які повністю визначаються вхідним масивом даних. В основі даної процедури лежить підхід, у відповідності з яким множина значень вхідних змінних (регресорів) розбивається на області зі своїми специфічними рівняннями регресії та класифікації. Саме зазначений підхід дозволяє отримати адаптивні моделі, які дозволяють отримати достовірні прогнози та використовується у випадках наявності точок переключення регресії та формалізації немонотонного характеру залежності між ефектами та відгуками, які важко апроксимувати параметричними моделями.

Базисні функції багатомірних адаптивних регресивних MAR-сплайнів до та після точки переключення регресії описуються наступним чином:

$$(x-t)_+ = \begin{cases} x-t, if\ x > t \\ 0, if\ x \le t \end{cases} \qquad (2.10)$$

$$(x-t)_- = \begin{cases} t-x, if\ x < t \\ 0, if\ x \ge t \end{cases}$$

де t – точка перегину кусочної функції.

Базисні функції у MARSplines (Multivariate Adaptive Regression Splines) у програмі Statistics зазвичай формалізуються у вигляді наступних математичних співвідношень:

$$(x-t)_+ = \max(0; x-t) \qquad (2.11)$$
$$(x-t)_- = \max(0; t-x)$$

У випадку формалізації багатомірної залежності для кожної компоненти вектора регресорів будуються базисні функції виду (2.10) та (2.11), які і визначають набір базисних функції, побудованих на основі множини вхідних даних:

$$B = \{(x_i - t)_+, (t - x_i)_-\}_{\substack{t \in \{x_{1i},\ldots,x_{Ni}\} \\ i=1,\ldots,n}} \qquad (2.12)$$

Загальне рівняння багатомірних адаптивних регресивних MAR-сплайнів для m ненульових членів-складових записується у вигляді комбінації зваженої суми базисних функцій та їх добутків:

$$y = f(X) = \alpha_0 + \sum_{j=1}^{m} \alpha_j \cdot B_j(X) \qquad (2.13)$$

де α_0 – константа, вільний член;

α_j – константа, параметр багатомірного адаптивного регресивного рівняння;

m – загальна кількість базисних функцій;

X – векторів вхідних регресорів;

$B_j(X)$ – j-та базисна функція із множини B або добуток двох чи більшої кількості таких функцій.

Основний принцип побудови багатомірних адаптивних регресивних MAR-сплайнів передбачає визначення не лише базисних функцій, але і термів, які визначають кількість різних комбінації базисних функцій з урахуванням звернень до кожного із релевантних факторів-регресорів.

При побудові регресивних MAR-сплайнів отримаємо наступні параметри (рисунок 2.18): кількість незалежних змінних – 5, кількість залежних змінних – 1, кількість термів – 5, кількість базисних функцій – 5, порядок взаємодії (кількість складових добутку базисних функцій) – 2, а також кількість звернень до факторів-регресорів: найбільша – 2 до X1, X2, далі 1 – X3, крім того незначущими виявлено фактори X2 та X5.

Model specifications	Model Summa Value
Independents	5
Dependents	1
Number of terms	5
Number of basis functions	5
Order of interactions	2
Penalty	2,00000
Threshold	0,00050
GCV error	3153,12

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

Рисунок 2.18 – Параметри специфікації моделі та кількість звернень до релевантних факторів-регресорів

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

Рисунок 2.19 – Коефіцієнти моделі та терми моделі впливу впливу факторів фінтех, фінансового моніторингу як банків так і страхових компаній, обсягів торгів на фінансові правопорушення у вигляді багатомірних адаптивних регресивних MAR-сплайнів

Таким чином, враховуючи представлені вище коефіцієнти, терми та параметри модель впливу фінтех, фінансового моніторингу як банків так і

страхових компаній, обсягів торгів на фінансові правопорушення, кібернетичні правопорушення, легалізація кримінальних доходів у вигляді багатомірних адаптивних регресивних MAR-сплайнів набуває вигляду:

$$Y1 = -1{,}53418216810049e+001 - 2{,}20013777098280e+003*\max(0;\ 2{,}39473128974892e-001-X4) + 2{,}28135475716692e-001*\max(0;\ X3-7{,}46462968235000e+003)*\max(0;\ 2{,}39473128974892e-001-X4) + 3{,}30135483180817e+002*\max(0;\ 5{,}57544361572743e-001-X1) + 2{,}50799012955197e+002*\max(0;\ X1-3{,}71405276737145e-001) \quad (2.14)$$

Аналізуючи рівняння 2.14, робимо висновок, що діяльність страхових компаній веде до зменшення фінансових кримінальних правопорушень, за умови що показник діяльності страхових компаній буде менший за 0,2395, в іншому випадку, окремо діяльність страхових компаній не буде мати впливу. Мультиплікативний додатній ефект на фінансові правопорушення будуть мати загальний обсяг торгів на біржі з діяльністю страхових компаній, якщо обсяг торгів буде перевищувати 7464,63, а показник діяльності страхових компаній буде меншим за 0,2395. Додатній вплив на кількість фінансових правопорушень буде мати рівень розвитку фінтех, при тому, якщо значення показника буде від 0,3714 до 0,5575 то вплив буде у вигляді підсумку двох термів, а якщо перевищить значення у 0,5575 одиниць, то тільки одного.

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

Адекватність побудованої моделі у вигляді багатомірних адаптивних регресивних MAR-сплайнів підтверджено: мінімальним значенням загального критерію якості моделі – узагальненого ковзного середнього помилки (GCV error), яке приймає значення 3153,12 (рисунок 2.18); коефіцієнт детермінації

набуває значення 0,803, що свідчить про високу якість моделі (рисунок 2.20); несуттєве відхилення фактичних та прогнозних значень кількості фінансових правопорушень, по яких було провадження у звітному періоді.

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

Рисунок 2.20 – Регресивні статистики залежності фінансових правопорушень від факторів у вигляді багатомірних адаптивних регресивних MAR-сплайнів

Переходячи до практичної реалізації моделі в розрізі залежності кібернетичних правопорушень від 5 факторів у вигляді багатомірних адаптивних регресивних MAR-сплайнів отримаємо наступні параметри (рисунок 2.21): кількість незалежних змінних – 5, кількість залежних змінних – 1, кількість термів – 8, кількість базисних функцій – 14, порядок взаємодії (кількість складових добутку базисних функцій) – 3, а також кількість звернень до факторів-регресорів: найбільша – 5 до X1, далі 4 – X3, 3 – X2, 2 – X5, крім того незначущим виявлено фактор X4.

	Model Summary (Spreadsheet9.s
Model specifications	Value
Independents	5
Dependents	1
Number of terms	8
Number of basis functions	14
Order of interactions	3
Penalty	2,00000
Threshold	0,00050
GCV error	218725,
Prune	Yes

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

Рисунок 2.21 – Параметри специфікації моделі та кількість звернень до релевантних факторів-регресорів

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

Рисунок 2.22 – Коефіцієнти моделі та терми моделі впливу факторів фінтех, фінансового моніторингу як банків так і страхових компаній, обсягів торгів на кібернетичні правопорушення у вигляді багатомірних адаптивних регресивних MAR-сплайнів

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

$$Y2 = 3{,}97130455471352e+002 + 3{,}38716423357658e+004*\max(0; X1-3{,}71405276737145e-001) + 1{,}10777191998577e+005*\max(0; X5-1{,}83132301034698e-001) - 3{,}44120331174238e-002*\max(0; X1-3{,}71405276737145e-001)*\max(0; X2-1{,}83693800000000e+006) + 2{,}11976578551327e-006*\max(0; X1-3{,}71405276737145e-001)*\max(0; X2-1{,}83693800000000e+006)*\max(0; X3-7{,}46462968235000e+003) - 2{,}15529085157748e-006*\max(0; X2-2{,}09449000000000e+005)*\max(0; X3-7{,}46462968235000e+003)*\max(0; X5-1{,}83132301034698e-001) - 1{,}78240383752107e+000*\max(0; X1-3{,}71405276737145e-001)*\max(0; \quad (2.15)$$

X3-7,46462968235000e+003) - 1,37560299832438e+000*max(0; X1-3,71405276737145e-001)*max(0; 2,61731749103700e+004-X3)

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

Адекватність побудованої моделі у вигляді багатомірних адаптивних регресивних MAR-сплайнів підтверджено: мінімальним значенням загального критерію якості моделі – узагальненого ковзного середнього помилки (GCV error), яке приймає значення 218725 (рисунок 2.22); коефіцієнт детермінації набуває значення 0,886, що свідчить про високу якість моделі (рисунок 2.23); несуттєве відхилення фактичних та прогнозних значень (таблиця 2.8).

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

Рисунок 2.23 – Регресивні статистики залежності фінансових правопорушень від факторів у вигляді багатомірних адаптивних регресивних MAR-сплайнів

Таблиця 2.8 – Фактичні та прогнозні значення, залишки та квадрат залишків кібернетичних правопорушень

	Y1 Pred	Y1 Res	Y1 Res Sqd		Y1 Pred	Y1 Res	Y1 Res Sqd
I 2013	397,130	-397,130	157712,6	I 2017	670,291	-227,291	51661,2
II 2013	397,130	65,870	4338,8	II 2017	986,612	417,388	174212,4
III 2013	397,130	151,870	23064,4	III 2017	2145,180	134,820	18176,5
IV 2013	397,130	170,870	29196,4	IV 2017	568,492	-317,492	100800,9
I 2014	397,130	-268,130	71893,9	I 2018	1326,433	-364,433	132811,5
II 2014	397,130	-181,130	32808,2	II 2018	1500,751	97,249	9457,4
III 2014	397,130	-35,130	1234,1	III 2018	1500,714	468,286	219292,0
IV 2014	397,130	20,870	435,5	IV 2018	2307,715	-66,715	4451,0
I 2015	397,130	-212,130	44999,3	I 2019	753,345	-46,345	2147,9
II 2015	397,130	-105,130	11052,4	II 2019	1108,891	162,109	26279,2
III 2015	397,130	51,870	2690,4	III 2019	2293,327	-497,327	247333,7
IV 2015	397,130	158,870	25239,5	IV 2019	1858,931	229,069	52472,5
I 2016	397,130	-159,130	25322,5	I 2020	647,897	-4,897	24,0
II 2016	397,130	85,870	7373,6	II 2020	1475,864	-192,864	37196,5
III 2016	397,130	338,870	114832,6	III 2020	2266,093	-239,093	57165,7
IV 2016	421,703	396,297	157051,0	IV 2020	2133,804	364,196	132639,1

Переходячи до практичної реалізації моделі в розрізі залежності обсягів легалізації кримінальних доходів від 5 факторів у вигляді багатомірних адаптивних регресивних MAR-сплайнів отримаємо наступні параметри (рисунок 2.21): кількість незалежних змінних – 5, кількість залежних змінних – 1, кількість термів – 3, кількість базисних функцій – 3, порядок взаємодії (кількість складових добутку базисних функцій) – 2, а також кількість звернень до факторів-регресорів: найбільша і однакова – 1 до X1, X2, X3, незначущими виявлено фактори X4 та X5.

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

Y3 = 3,29291807569567e+001 - 1,77427285069972e-005*max(0; 1,83693800000000e+006-X2) + 1,50318465753288e+001*max(0; X1-5,57544361572743e-001)*max(0; 2,23304254185900e+004-X3) (2.16)

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

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

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

Рисунок 2.24 – Параметри специфікації моделі та кількість звернень до релевантних факторів-регресорів

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

Рисунок 2.25 – Коефіцієнти моделі та терми моделі впливу факторів фінтех, фінансового моніторингу як банків так і страхових компаній, обсягів торгів на кібернетичні правопорушення у вигляді багатомірних адаптивних регресивних MAR-сплайнів

Адекватність побудованої моделі у вигляді багатомірних адаптивних регресивних MAR-сплайнів підтверджено: мінімальним значенням загального критерію якості моделі – узагальненого ковзного середнього помилки (GCV error), яке приймає значення 767 (рисунок 2.24); коефіцієнт детермінації набуває значення 0,405, що свідчить про високу якість моделі (рисунок 2.26); несуттєве відхилення фактичних та прогнозних значень кількості правопорушень з метою легалізації кримінальних доходів (таблиця 2.9).

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

Рисунок 2.9 – Регресивні статистики залежності обсягів легалізації кримінальних доходів від факторів на у вигляді багатомірних адаптивних регресивних MAR-сплайнів

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

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

Таблиця 2.9 – Фактичні та прогнозні значення, залишки та квадрат залишків обсягів легалізації кримінальних доходів

	Y1 Pred	Y1 Res	Y1 Res Sqd		Y1 Pred	Y1 Res	Y1 Res Sqd
I 2013	4,0531	-0,0531	0,003	I 2017	30,9541	49,0459	2405,504
II 2013	4,1196	3,8804	15,058	II 2017	32,9292	-18,9292	358,314
III 2013	4,7558	-1,7558	3,083	III 2017	32,9292	-5,9292	35,155
IV 2013	5,2318	-2,2318	4,981	IV 2017	32,9292	29,0708	845,113
I 2014	4,3805	17,6195	310,446	I 2018	109,0000	-0,0000	0,000
II 2014	4,9814	0,0186	0,000	II 2018	32,9292	-0,9292	0,863
III 2014	6,2031	-0,2031	0,041	III 2018	32,9292	11,0708	122,563
IV 2014	7,9842	-4,9842	24,842	IV 2018	32,9292	-42,9292	1842,915
I 2015	12,1221	4,8779	23,794	I 2019	32,9292	84,0708	7067,903
II 2015	17,1412	-12,1412	147,408	II 2019	32,9292	-24,9292	621,464
III 2015	21,7675	-3,7675	14,194	III 2019	32,9292	-10,9292	119,447
IV 2015	26,8347	-8,8347	78,053	IV 2019	32,9292	-30,9292	956,614
I 2016	22,4964	10,5036	110,326	I 2020	32,9292	-30,9818	959,872
II 2016	26,1436	5,8564	34,297	II 2020	18,7450	-16,8488	283,884
III 2016	29,8826	28,1174	790,586	III 2020	7,1063	-5,2601	27,668
IV 2016	32,9292	-15,9292	253,739	IV 2020	7,4344	-5,6367	31,773

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

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

Для визначення взаємозв’язків між FinTech інноваціями, фінансовими злочинами, кіберзлочинами та легалізацією кримінальних доходів обрано структурне моделювання. Структурне моделювання передбачає собою методологію перевірки значної кількості можливих паралельно існуючих гіпотез щодо наявності причинно-наслідкових зв’язків, формування різних елементів в взаємопов’язану, комплексну, систематизовану структуру. При

чому структурна модель призначена для аналізу складних взаємозв’язків між категоріями, визначеними для дослідження. За допомогою структурного моделювання можливо точно врахувати складні взаємозв’язки між складовими моделі. І за умови використання належних граничних умов, структурна модель створює базу для здійснення аналізу широкомаштабних відповідей моделі з огляду локальних характеристик її структури. Тобто згруповане вивчення сукупності окремих факторів надає індивідуальні методології вирішення індивідуальних напрямів проблемних питань [65].

1 етап. Формування вхідних показників оцінювання взаємозалежності FinTech інновацій та фінансовими та кібернетичними злочинами за посередництва фінансових установ в розрізі наступних груп: фінтех складова, фінансові злочини, кіберзлочини та легалізація кримінальних доходів, враховуючи, що показник співвідношення фінансових активів до ВВП (FA/GDP) [64] буде включено до опису кожної із зазначених груп. Таким чином, для опису фінтех складової обрано наступні два показники: Fintech1 – кількість абонентів мобільного зв'язку на 1 тис. населення; Fintech2 - показник фінтех, питома вага абонентів інтернету в населенні України; фінансові злочини, відповідно: FC1 – кількість обліковано фінансових злочинів у звітному періоді (статті 222 та 222-1 ККУ); FC2 - кількість фінансових злочинів, які передано до суду з обвинувальним актом; кіберзлочини: CC1 - кількість обліковано кіберзлочинів у звітному періоді (статті 361,361-1, 361-2, 362, 363, 363-1 ККУ); CC2 - кількість фінансових злочинів, які передано до суду кіберзлочинів з обвинувальним актом; а також легалізація кримінальних доходів – такі показники, як; AML1 – кількість обліковано з легалізації кримінальних доходів (стаття 209 ККУ); AML2 – кількість фінансових злочинів, які передано до суду обвинувальних актів з легалізації кримінальних доходів. Розглянемо статистичну базу в розрізі вхідної бази дослідження у вигляді квартальних часових рядів з 2013 по 2020 рр. (таблиця 2.10) [70, 71].

Таблиця 2.10 – Вхідні показники оцінювання взаємозалежності FinTech інновацій та фінансовими та кібернетичними злочинами за посередництва фінансових установ

Квартал/Рік	FA/GDP	Fintech1	Fintech2	FC1	FC2	CC1	CC2	AML1	AML2
I 2013	6,539	1,344	0,119	0	0	0	0	4	1
II 2013	5,708	1,357	0,125	188	51	463	33	8	1
III 2013	5,237	1,364	0,127	280	109	549	200	3	1
IV 2013	5,224	1,375	0,131	328	164	568	247	3	1
I 2014	7,184	1,373	0,135	93	46	129	19	22	3
II 2014	6,144	1,381	0,140	191	115	216	77	5	1
III 2014	5,635	1,410	0,138	280	165	362	157	6	0
IV 2014	5,565	1,425	0,137	346	206	418	191	3	2
I 2015	7,885	1,436	0,140	61	28	185	35	17	2
II 2015	6,105	1,442	0,141	88	43	292	90	5	0
III 2015	4,976	1,429	0,139	113	61	449	218	18	1

Продовження таблиці 2.10

Квартал/Рік	FA/GDP	Fintech1	Fintech2	FC1	FC2	CC1	CC2	AML1	AML2
IV 2015	5,011	1,420	0,142	130	67	556	151	18	0
I 2016	6,704	1,339	0,333	28	8	238	109	33	0
II 2016	5,620	1,329	0,345	42	23	483	172	32	0
III 2016	4,596	1,348	0,371	65	20	736	307	58	1
IV 2016	4,419	1,332	0,393	64	26	818	455	17	1
I 2017	5,408	1,324	0,467	17	7	443	101	80	1
II 2017	4,850	1,326	0,467	31	11	1404	469	14	2
III 2017	3,950	1,316	0,541	50	21	2280	802	27	3
IV 2017	3,697	1,314	0,558	58	26	251	1002	62	3
I 2018	4,565	1,307	0,563	14	4	962	379	109	6
II 2018	3,964	1,302	0,585	110	11	1598	853	32	4
III 2018	3,358	1,295	0,616	44	20	1969	1036	44	3
IV 2018	3,254	1,279	0,618	52	27	2241	1314	-10	0
I 2019	4,160	1,277*	0,627	20	12	707	351	117	0
II 2019	3,600	1,274*	0,638	45	26	1271	796	8	2
III 2019	2,995	1,271*	0,656	53	35	1796	1142	22	1
IV 2019	3,158	1,269*	0,687	71	41	2088	1248	2	9
I 2020	4,457	1,266*	0,735*	41	31	643	301	1,947*	9,794*
II 2020	4,413	1,263*	0,786*	75	53	1283	611	1,896*	10,657*
III 2020	3,417	1,261*	0,841*	104	72	2027	990	1,846*	11,597*
IV 2020	3,344*	1,258*	0,899*	144	92	2498	1484	1,798*	12,620*

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

2 етап. Структурне моделювання взаємозалежності FinTech інновацій та фінансовими та кібернетичними злочинами за посередництва фінансових установ. На основі використання змінних, введених на першому етапі при

формалізації вхідної бази дослідження, виникає необхідність їх класифікації на екзогенні та ендогенні, а також визначенні на основі введених змінних латентних (неявно заданих) змінних, які і дозволять описати взаємозалежність FinTech інновацій та фінансовими та кібернетичними злочинами за посередництва фінансових установ. Так, всі приведені змінні на першому етапі – це спостережувані (явні) змінні, оскільки їх значення приведені у файлі даних [68, 69]. Але в моделі повинні бути присутні ще й латентні змінні, якими пропонується обрати: Fintech – рівень розвитку FinTech інновацій, FC – рівень розвитку фінансових злочинів, CC – рівень розвитку кібернетичних правопорушень, AML – рівень розвитку системи протидії легалізації кримінальних доходів. Явні змінні Fintech1, Fintech2, FC1, FC2, CC1, CC2, AML1, AML2 відносяться до ендогенних. Оскільки фінтах інновації впливають на фінансові та кібернетичні злочини та легалізацію кримінальних доходів, кібернетичні злочини впливають на фінансові злочини та легалізацію кримінальних доходів, а легалізація кримінальних доходів впливає на фінансові злочини, то латентну змінну Fintech можна вважати екзогенною, а латентні змінні FC, CC, AML – ендогенними.

Для побудови моделі структурних рівнянь взаємозалежності FinTech інновацій та фінансовими та кібернетичними злочинами за посередництва фінансових установ скористаємось програмним пакетом Statistica Portable командаю Statistics/Advanced Linear/Nonlinear Models/Structural Modeling. В результат отримаємо рисунок 2.27.

На основі даних рисунку 2.27, а саме параметрів лінійних однофакторних та багатофакторних регресійних моделей залежності між латентними змінними, а також залежності між явними та латентними змінними побудуємо шукану систему структурних рівнянь:

$$\begin{cases} \frac{FA}{GDP} = -16.622 \cdot Fintech \\ Fintech1 = -0.047 \cdot Fintech + 0.002 \\ Fintech2 = 0.252 \cdot Fintech + 0.003 \\ \frac{FA}{GDP} = FC + 6.146 \\ FC1 = 556.553 \cdot FC \\ FC2 = 290.105 \cdot FC + 292.109 \\ \frac{FA}{GDP} = CC + 6.146 \\ CC1 = 58.179 \cdot CC + 220119.130 \\ CC2 = 35.761 \cdot CC + 66949.988 \\ \frac{FA}{GDP} = AML + 6.146 \\ AML1 = 0.312 \cdot AML + 939.984 \\ AML2 = 0.431 \cdot AML + 7.568 \\ FC = -7.660 \cdot Fintech + 0.274 \cdot CC + 0.823 \cdot AML + 0.013 \\ CC = 10.055 \cdot Fintech + 0.234 \\ AML = 7.444 \cdot Fintech - 0.156 \cdot CC + 0.001 \end{cases} \quad (2.17)$$

Таким чином, на основі системи (2.17) можна зробити наступні висновки:

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

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

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

– якщо порівнювати темпи варіації фінансових правопорушень, кібернетичних правопорушень, фінтех інновацій та легалізації кримінальних доходів, необхідно відмітити, що лише при зростанні фінтех інновацій фінансові правопорушення будуть зменшуватись значно вищими темпами. В розрізі впливу кібернетичних правопорушень та легалізації кримінальних

доходів на фінансові правопорушення темпи варіації результативної ознаки будуть меншими за варіацію факторних;

– темп варіації кібернетичних правопорушень значно перевищує темп варіації фінтех інновацій, про що свідчить відповідний коефіцієнт передостаннього рівняння системи (2.17), а саме при зростання рівня фінтех інновацій на 1% рівень кібернетичних правопорушень буде зростати на 10,06%;

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

3 етап. Перевірка адекватності та точності моделі взаємозалежності FinTech інновацій та фінансовими та кібернетичними злочинами за посередництва фінансових установ. Для реалізації даного етапу визначимо базові сумарні статистики (рисунок 2.28), матрицю рефлектор (рисунок 2.29), а також перевірку відповідності залишків моделі нормальному закону розподілу (рисунок 2.30).

Як видно з рисунку 2 Maximum Residual Cosine (максимум косинуса залишків) прямує до 0, що свідчить що ітераційний процес завершився успіхом. Значення ICSF Criterion та ICS Criterion близькі до 0, що свідчить що побудована модель є стійкою до множення на постійний маштабуючий множник та до змін масштабу.

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

	Model Estimates (Spreadsheet1.sta)			
	Parameter Estimate	Standard Error	T Statistic	Prob. Level
(Fintech)-1->[FA/GDP]	-16,62	1,81	-9,17	0,00
(Fintech)-2->[Fintech1]	-0,047	0,01	-4,477	0,00
(Fintech)-3->[Fintech2]	0,252	0,03	7,327	0,00
(DELTA1)-->[FA/GDP]				
(DELTA2)-->[Fintech1]				
(DELTA3)-->[Fintech2]				
(DELTA1)-4-(DELTA1)	0,00	0,00		
(DELTA2)-5-(DELTA2)	0,002	0,001	3,742	0,00
(DELTA3)-6-(DELTA3)	0,003	0,00	0,742	0,458
(FC)-->[FA/GDP]				
(FC)-7->[FC1]	556,55	5063,45	0,11	0,912
(FC)-8->[FC2]	290,10	2639,42	0,11	0,912
(CC)-->[FA/GDP]				
(CC)-9->[CC1]	58,17	11,50	5,059	0,00
(CC)-10->[CC2]	35,761	0,00		
(AML)-->[FA/GDP]				
(AML)-11->[AML1]	0,312	0,956	0,326	0,744
(AML)-12->[AML2]	0,431	0,112	3,853	0,00
(EPSILON1)-->[FA/GDP]				
(EPSILON2)-->[FC1]				
(EPSILON3)-->[FC2]				
(EPSILON4)-->[CC1]				
(EPSILON5)-->[CC2]				
(EPSILON6)-->[AML1]				
(EPSILON7)-->[AML2]				
(EPSILON1)-13-(EPSILON1	6,146	2,21	2,77	0,006
(EPSILON2)-14-(EPSILON2	0,00	0,00		
(EPSILON3)-15-(EPSILON3	292,10	74,196	3,937	0,00
(EPSILON4)-16-(EPSILON4	220119,13	61580,76	3,574	0,00
(EPSILON5)-17-(EPSILON5	66949,98	19388,36	3,453	0,001
(EPSILON6)-18-(EPSILON6	939,984	238,78	3,936	0,00
(EPSILON7)-19-(EPSILON7	7,568	2,005	3,776	0,00
(ZETA1)-->(FC)				
(ZETA2)-->(CC)				
(ZETA3)-->(AML)				
(ZETA1)-20-(ZETA1)	0,013	0,383	0,035	0,972
(ZETA2)-21-(ZETA2)	0,234	1,678	0,139	0,889
(ZETA3)-22-(ZETA3)	0,001	0,151	0,007	0,995
(Fintech)-23->(FC)	-7,66	0,00		
(Fintech)-24->(CC)	10,055	1,858	5,412	0,00
(Fintech)-25->(AML)	7,444	0,00		
(CC)-26->(FC)	0,274	0,00		
(CC)-27->(AML)	-0,156	0,00		
(AML)-28->(FC)	0,823	0,113	7,259	0,00

Рисунок 2.27 – Фрагмент таблиці обчислених параметрів моделі взаємозалежності FinTech інновацій та фінансовими та кібернетичними злочинами за посередництва фінансових установ

	Basic Summary Statistics (Spr
	Value
Discrepancy Function	5,123
Maximum Residual Cosine	0,388
Maximum Absolute Gradient	159,12(
ICSF Criterion	1,818
ICS Criterion	0,858
ML Chi-Square	158,804
Degrees of Freedom	23,000
p-level	0,000
RMS Standardized Residual	0,548

Рисунок 2.28 – Показники адекватності та точності моделі

За допомогою Матриці-рефлектора (рисунок 2.29) проводимо перевірку моделі на інваріантність, тобто визначаємо стійкість моделі відповідно до зміни масштабу початкових даних.

	Reflector Matrix (Spreadsheet1.sta)								
	FA/GDP	Fintech1	Fintech2	FC1	FC2	CC1	CC2	AML1	AML2
FA/GDP	0,858	-0,002	0,009	6,928	3,585	56,325	37,076	-0,814	0,042
Fintech1	-2,611	0,605	0,761	-267,77	-184,68	587,515	438,344	48,854	1,242
Fintech2	0,147	0,134	0,294	251,025	103,283	1379,87	619,281	-120,76	-4,795
FC1	-0,000	-0,000	0,002	-0,192	-0,169	0,689	1,108	0,055	0,022
FC2	0,007	0,000	-0,003	-0,031	0,067	-4,129	-3,807	0,234	-0,064
CC1	0,001	-0,000	-0,000	-0,042	-0,018	0,067	-0,352	0,023	0,000
CC2	0,002	-0,000	-0,000	-0,080	-0,039	-1,154	0,068	0,038	0,001
AML1	0,001	0,000	-0,001	1,201	0,706	4,554	2,101	-0,001	0,025
AML2	-0,079	-0,001	-0,004	-9,472	-6,205	8,727	11,874	3,811	0,051

Рисунок 2.29 – Матриця-рефлектор

Для стійкої моделі характерна близькість елементів даної матриці один до одного. Аналіз матриці рефлектора взаємозалежності FinTech інновацій та фінансовими та кібернетичними злочинами за посередництва фінансових установ свідчить про стійкість побудованої моделі до зміни масштабу вимірювання початкових даних.

Проаналізувавши Normal Probability Plot (нормальний імовірнісний графік, рисунок 2.30), підтвердимо припущення про те, що залишки моделі є якісні та мають близький до нормального закон розподілу, так як на графіку вони розміщуються близько до прямої.

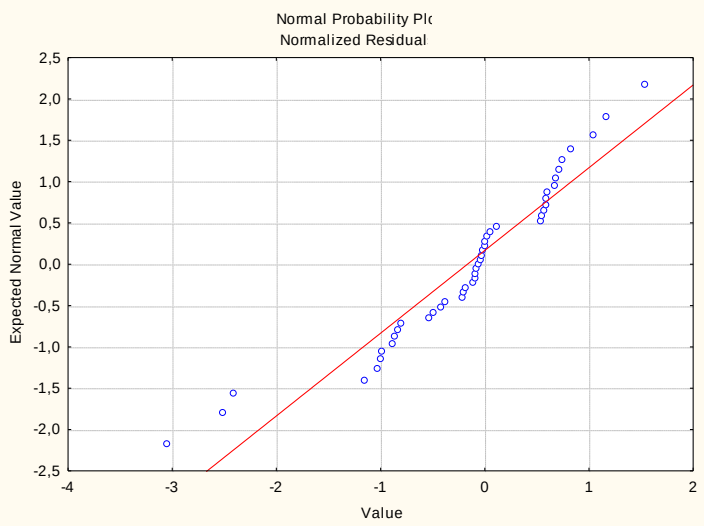


Рисунок 2.30 – Нормальний імовірнісний графік

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

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

3 ОСОБЛИВОСТІ ВІКТИСНОЇ ПОВЕДІНКИ СПОЖИВАЧІВ ФІНАНСОВИХ ПОСЛУГ У КІБЕРПРОСТОРІ

3.1. Психологічний аспект дослідження протидії віктимізації внаслідок кібершахрайства

Для сучасного суспільства природнім і доступним стає новий вимір діяльності – віртуальний. Це стосується не лише побутового рівня взаємодії, але і корелює із державною політикою реформ в Україні. Відповідно до даних опитування «Електронні послуги: досвід, довіра, доступність», проведеного Київським міжнародним інститутом соціології у 2020 р., більшість громадян України у віці від 18 до 29 років мають досвід користування електронними державними сервісами [73]. Високі темпи діджиталізації впливають на кожного в різний спосіб. Саме тому набуває значимості дослідження особливостей віртуального простору та можливих позитивних і негативних аспектів впливу на існуючі реальні соціальні проблеми.

Розвиток віртуальних технологій, окрім можливостей самореалізації індивіда у кіберпросторі в цілому, спровокував появу нових форм девіантної та делінквентної поведінки. Можна впевнено говорити про відтворення більшості відомих видів правопорушень у віртуальному просторі. Наприклад, порівняння кібершахрайства із аналогічними видами злочинів у реальному просторі свідчить про відтворення базових структурних елементів злочинного діяння. У 2017 році в Україні відбулася масштабна атака вірусом Petya: були вражені енергетичні компанії, українські банки, аеропорти в Києві та Харкові, Чорнобильська АЕС, урядові сайти, київський метрополітен і т. д. За даними експертів Міжнародного валютного фонду, економічні втрати від атаки вірусу Petya склали близько 850 млн. доларів [74].

Віртуалізація даного виду злочинної діяльності неминуче впливає на формування специфічних проявів кібершахрайство порівняно із шахрайською діяльністю. Загальновизнані наукові досягнення у визначенні психологічних особливостей шахрайської діяльності Ю.М. Антоняна, Б.С. Волкова,

П.С. Дагеля, О.А. Герцензона, О.В. Рудзитіса, О.О. Данилова, Є.Л. Доценко, О.В. Кравченко та багатьох інших дослідників. Однак актуальним питанням слід визнати аналіз різноманітних проявів кібершахрайства як своєрідного виду злочину. Метою даного дослідження є проаналізувати психологічні особливості шахрайства у кіберпросторі.

Внаслідок відсутності тривалого життєвого досвіду особливо актуальною проблема є для молоді, що перебуває на етапі формування світогляду. Довіра до інноваційних інструментів реалізації прав і свобод має ґрунтуватися на свідомому розумінні доступних меж захисту конфіденційних даних та відповідального ставлення до приватної інформації. Віктимізація є важливим фактором як у аналізі проблем психологічного, так і кримінологічного типу. Таким чином на зіткненні одвічно актуальної і відносно нової, сучасної проблематики виникає цікавий і практико затребуваний простір для досліджень.

Г. Біктагірова, Р. Валеєва, Н. Костюніна, Н. Калацкая, А. Дроздікова-Заріпова та інші дослідники підкреслюють динамічність як сутність віктимізації, адже це є певний процес. Віктимізацію визначають як процес і результат набуття статусу жертви в результаті впливів і впливів як зовнішніх, так і внутрішніх; перетворення людини на потерпілого [75]. Дослідження віктимізації вимагає врахування рівнів віктимізуючого впливу на особистості. Залежно від різних об'єктивних і суб'єктивних типово виділяють первинну, вторинну і третинну віктимізацію. На першому рівні перебувають безпосередньо потерпілі від несприятливих обставин. Жертвами вторинної віктимізації вважають референтне оточення потерпілого первинного рівня. На третинному рівні розглядають потерпілих від непрямого впливу чи негативних обставин, опосередковано спрямованих проти конкретної особи, наприклад, на рівні організації. Інколи виокремлюють також четвертий та п’ятий рівні, за яких йдеться про масштаб та кількість потерпілих, регіонального чи міжнародного рівня відповідно.

Віктимна поведінка внаслідок комплексу специфічних якостей особистості збільшує вірогідність віктимізації. Враховуючи цілісність особистості, слід говорити про єднання індивідуальних рис та соціальних впливів, які зумовлюють віктимні прояви. Віктимність розглядають як на рівні біологічних закономірностей розвитку, біологічну якість, так і як наслідок соціалізації, набуту рису [76]. Markus Kaakinen, Teo Keipi, Pekka Räsänen, and Atte Oksanen (2018) визначають зв'язок віктимності індивіда внаслідок кібершахрайства із рівенм суб'єктивного благополуччя. Внаслідок кроскультурного дослідження, проведеного у США, Великобританії, Німеччини та Фінляндії, визначено негативні кореляційні зв'язки між рівенм суб'єктивного благополуччя та вразливістю до кібершахрайства у разі відсутності активних джерел соціалізації за межами віртуального простору [77].

С.О. Гарькавець аналізує 4 форми віктимності особистості:

- віктимність шизоїдної особистості – проявляється у надмірному егоїзмі, зневажанні інтересів та цінностей інших. Також відзначається низький рівень розвитку емоційного інтелекту, а у конфліктах характеризується агресивним поводженням з опонентами. Цей тип переважає серед жертв кримінальних зіткнень та убивств;
- віктимність депресивної особистості – характеризується пасивними очікуваннями, невимогливістю до життя, підвищеною навіюваністю та залежністю від інших, а також слабкістю вольових проявів, різними проявами форм адикції;
- віктимність особистості з нав'язливістю – характеризується підвищеною агресивністю, емоційною збудливістю, догматичністю та авторитарністю, схильністю використовувати деструктивну фантазію, породжувати міжособистісні та внутрішньогрупові конфлікти. Незважаючи на те, що дана характеристика стеретипно ближча до уявлень про особистість злочинця, однак встановлено зв'язки такого типу поведінкових проявів зі зростанням віктимної вразливості;

‗ віктимність істеричної особистості – відзначаються надмірною наполегливістю щодо реалізації власних інтересів, нехтуванням правами оточуючих, марнославством, невизнанням власної провини та перекладенням її на інших. Особистість з істеричною віктимністю схильна до аморальних та асоціальних вчинків, що можуть у майбутньому стати причиною міжособистісних конфліктів [78].

Особливими характеристиками соціального віртуального простору є те, що у більшій мірі зберігається анонімність при взаємодії та у меншій ця взаємодія може бути контрольована правоохоронною системою. Особливо у період обмежень соціальної взаємодії, детермінованих пандемією. З часу запровадження карантинних обмежень в Україні зафіксовано понад 700 звернень щодо випадків кібер-шахрайства виключно з тематики протидії поширенню захворюваності на COVID-19, йдеться про маніпуляції щодо товарів індивідуального захисту, фейкову інформацію, СМС-розсилки та дзвінки, пов’язані із шахрайськими повідомленнями [79].

Для здійснення шахрайства, злочинець використовує психологічні засоби впливу на психіку жертви. Специфіка шахрайства полягає в переважанні методів активного психологічного впливу. Відповідно з дефініцією Г. О. Ковальова, за якою вплив – це цілеспрямований процес, в якому беруть участь дві або більше упорядкованих систем, в результаті якого спостерігаються будь-які зміни хоча б однієї з цих сторін. Психологічний вплив має певні ознаки, визначені Сергієм та Світланою Ніколаєнками як усвідомлення здійснення впливу, котрий передбачає певний результат; вплив на мислення, почуття, думки із застосуванням психологічних методів; цілеспрямованість; вольові зусилля людиною, яка виконує вплив; інформаційність впливу [80].

А. С. Булатов зауважує, що методи активного впливу на психічну активність мають зміст, котрий вигідний саме для маніпулятора. Суть здійснення маніпуляції полягає в тому, щоб створити певний дисбаланс у жертви і викликати внутрішній дискомфорт. Окрім того, щоб жертва не

встигла знайти способи вирішення поданої ситуації, маніпулятор попередньо надає ці способи вирішення, зазвичай надаючи вибір, котрий можна назвати «вибір без вибору», тобто створюється ілюзія кращого вибору для обох сторін, хоча насправді кожен із наданих варіантів вигідні лише для самого шахрая. Сутність маніпуляції може бути не лише дискомфортною для жертви, а й навіть нестерпною, що не надає їй можливості включитися в раціональне мислення. Існують певні мішені, на котрі спрямований активний вплив. За класифікацією О. В. Кравченко до цілей впливу шахраїв в першу чергу відносять:

1. Когнітивні структури (інформаційне забезпечення діяльності людини).

2. Психічні стани (емоційні, фонові, функціональні).

3. Спонукачі діяльності людини (потреби, схильності, інтереси).

4. Регулятори діяльності людини (норми, правила, самооцінка, самоповага, гордість тощо).

5. Операційний склад активності (стиль мовлення, поведінки, звички, навички, спосіб мислення тощо) [81].

Інформаційні технології частково змінили світосприйняття людини, спричинивши формування нового віртуального простору та суспільства. За законодавством України, кіберпростір є певним середовищем, що надає можливості для комунікації в результаті функціонування сумісних комунікаційних систем та забезпечення електронних комунікацій з використанням інтернету або інших мереж [82]. Дослідниця М. В. Палчинська визначає кіберпростір як особливу соціальну сферу, включену до системи існуючих соціальних відносин, не тільки як аналог, а і конкурент стосовно просторово-часових змін [83]. Типово кіберпростір порівнюють з міфологічним, так як він займає проміжну позицію між чуттєвим простором сприйняття і середовищем чистого пізнання. Як частина віртуального простору, кіберпростір є певним середовищем, що підтримується за

допомогою сумісних комунікаційних систем, доступ до якого може бути отриманий за допомогою інтернету чи аналогічних мереж.

За своєю сутністю віртуальний простір є інформаційним середовищем, тобто має високу залежність від інформаційних впливів. Характер подачі інформації може змінювати її сприйняття, так М. Маклюен відзначає, що засіб передачі повідомлення можна розглядати як окремий тип повідомлення [84]. Однак для розуміння цього необхідне застосування конкретних меж сприйняття та аналізу. Важливо зазначити, що реальний, фізичний простір у цілому, має більш виражені рамки соціального регулювання. Віртуальний простір менше регламентується законом у зв’язку з новизною та невизначеністю конкретних рамок дозволенного, а також більшою складністю у ідентифікації злочинця, що спричинює виникнення багатьох межових феноменів, що провокує розвиток кібершахрайства [85].

Г.М. Сащук характеристикою віртуальної культури називає мозаїчність, пов'язану з особливостями процесу пізнання, а також структурування та ціннісного відбору соціального досвіду життєдіяльності. Віртуальна культура поєднує випадкові елементи культур різних народів та епох.

Віртуалізація призводить до зниження критичності, тому позитивно відображається на потенціальній віктимізації. Анонімність може дезорієнтувати особистість у міжособистісних контактах, тоді як відкритість та незахищеність особистої інформації вже є фактором можливої віктимізації вже у психологічному розумінні.

Відсутність місцевих обмежень виключає фактор, розглянутий у реальній віктимізації. Віртуальний простір не має матеріального розміру та розташування. Великий обсяг інформації посилює можливості шахрайських впливів, провокує експлуатацію кліпової хаотичності. Як зауважують Я.В. Чаплак та І.М. Зварич, темпи кліпової хаотичності зростають, позначаючись на соціальній свідомості. Це створює підґрунтя маніпулювання людиною у віртуальному просторі [80].

У сучасному віртуальному просторі безліч феноменів, що можуть бути класифіковані як злочин, але при цьому залишаються діючими та достатньо популярними, наприклад «1XBET» або «треш-стріми». Порушення авторських прав, так зване «піратство», взагалі інтегроване в масову свідомість мешканців багатьох країн, у тому числі України. Крізь призму психічного сприйняття шахрайство у віртуальному просторі має схожі риси із звичайним, але відповідно до характеристики самого простору має більш масовий, так званий «стихійний» характер. Л.М. Прудка на основі аналізу праць У. Альбрехта, Дж. Венца та Т. Уільяма, відзначає, що шахраї, зокрема і ті, які орудують у кіберпросторі, не мають сутнісно відмінних психологічних особливостей від законослухняних громадян. Тобто, схильність до кібершахрайства не може бути визначена превентивним обстеженням. Хоча окремі дані щодо злочинця можуть бути отримані завдяки профайлінгу, наприклад, психологічний портрет шахрая представлений в основному авантюрним складом особистості.

Мотивами кіберзлочину можуть виступати, у першу чергу, корисливі, але їх також можуть доповнювати мотиви самоствердження, прагнення до влади, ігровий мотив. Залежно від домінування певного мотиву, кібершахраї виявляють типові моделі поведінки, демонструють раціональний підхід до здійснення шахрайства, що виражається у активному підготовчому етапі вчинення злочинного діяння та усвідомленні його наслідків або отримують задоволення від процесу злочинної діяльності [85].

Угорські дослідники N. Arató, A.N. Zsidó, K. Lénárd, B. Lábadi визначають, що більшість агресорів у кіберпросторі лишаються анонімними. Кіберпростір забезпечує більш широку аудиторію для шахрайства. Кібершахраї схильні вчиняти злочини щодо осіб, що мають проблеми з регулюванням своїх емоцій, підвищений рівень агресивності, депресивність, підвищену схильність до стресу [86].

О.П. Дзьобань розрізняє два типи сприйняття інформації людиною у віртуальному просторі. У першому варіанті увага людини концентрується на

чомусь логічному, всезагальному, абстрагованому. У другому варіанті йдеться про певне занурення у так зване «міфологічне» сприйняття, що зосереджене на чомусь конкретному, неповторному, емоційно-образному. Таким чином, другий тип у більшості випадків створює віртуальну реальність, тобто індивід віртуалізується. Віртуальна реальність характеризується більшою суб'єктністю, нелінійністю, зміщенням просторових та часових меж, зануреністю з боку віртуалізованої особистості, вона стає «співучасником» цього світу. Але цей вимір неоднорідний, він має безліч можливих варіацій, залежних від контексту, тому кожна із них, будучи відомою людині, може провокувати різні поведінкові або емоційні реакції.

Швидкість операцій є істотною відмінністю кіберпростору від реальності. Починаючи від, наприклад, пошуку цифрових та реальних продуктів, закінчуючи їх оплатою. Тобто, віртуальний простір має низку специфічних властивостей, що позначається на віктимізації особистості.

Віртуальна ідентичність відповідно до визначення, наданого соціологом А. Криловим є усвідомлюваним і створюваним у віртуальній реальності уявленням людини про саму себе. А. Краснякова підкреслює можливість продукування багатоманіття «Я»-образів у віртуальному просторі, що приводить до формування мінливої і нестабільної ідентичності [83].

Невирішеним лишається питання, чи може утворення віртуального образу «Я» напряму впливати на віктимність особистості у віртуальному просторі. Наприклад, якщо поведінка особистості з віктимною нав'язливістю є агресивною, але стримується найближчим соціумом, то реальне «я» може використовувати кіберпростір як спосіб компенсації, що зробить поведінку людини більш агресивною у віртуальному просторі (внаслідок відсутності контролю, певних рамок та за умови можливої відносної анонімності).

Віртуальна реальність проявляє і більш загальний, соціальний вплив. У ній стираються державні кордони, з'являються нові цінності, моделі поведінки, стереотипи. Віртуальній реальності, згідно О.П. Дзьобаню, також характерне зміщення реальності, що може нести як позитивний у соціальному

аспекті зміст – розширення життєвого досвіду, смислу, так і негативний – необмежена та неконтрольована, деструктивна творчість [84]. Попри те, що користування віртуальним і зокрема кіберпростором не означає неминучої віртуалізації індивіда, певною мірою можливості занурення зростають. Принаймні, у разі використання специфічного розважального, ігрового контенту. Враховуючи змінений стан волі та свідомості у віртуальній реальності, можливості активного впливу на людину, значно зростають. Водночас пересічне послугування віртуальним простором, відмежоване від віртуальної реальності, не створює очевидних передумов до послаблення захисних можливостей психіки.

Для визначення ризиків активних методів впливу на особистість у віртуальному просторі з боку кібершахраїв проведене двохетапне емпіричне дослідження, яким охоплено 211 осіб у віці від 18 до 24 років. До вибірки увійшли студенти закладу вищої освіти технічних та соціогуманітарних спеціальностей. Вікові межі вибірки визначило переконання, що молодь є однією із найбільш активних когорт серед користувачів кіберпростору, що детермінує ризики її віктимізації з боку кібершахраїв.

Методичну базу дослідження становлять: «Схильність до віктимної поведінки» О. О. Андроннікової, А. Асингера «Оцінка агресивності у відносинах», психогеометричний тест С. Делінгер [87], самостійно розроблений опитувальник. Метою останнього є визначення рівня активності і поінформованості молоді про феномен та особливості кібершахрайства, пов’язані з цим необхідні заходи кібербезпеки. Для опрацювання отриманих даних використані r-критерій Пірсона, t-критерій Стьюдента та φ-критерій Фішера.

Досліджуючи показники різних типів схильності до віктимної поведінки, визначено середньозважені показники норми (рис. 3.1). Узагальнююча шкала методики «рівень реалізованої віктимності» в сирих балах описує 6,5±2,74 б., що відповідає межі між низьким та нормальним проявами віктимності. Це свідчить про незавершеність процесів формування

способу поведінки, що дозволяє уникати небезпечних ситуації, досить поширену внутрішню готовність до віктимної поведінки у майбутньому.

За окремими типами віктимності середньогрупові показники не виходять за межі норми. Йдеться про схильність віктимізуватися через агресивну поведінку; внутрішню прийнятність агресивних дій, які можуть призвести до віктимізації; невисокі ризики віктимізації через демонстрацію гіперсоціальної поведінки або бездіяльності задля уникнення віктимізації.

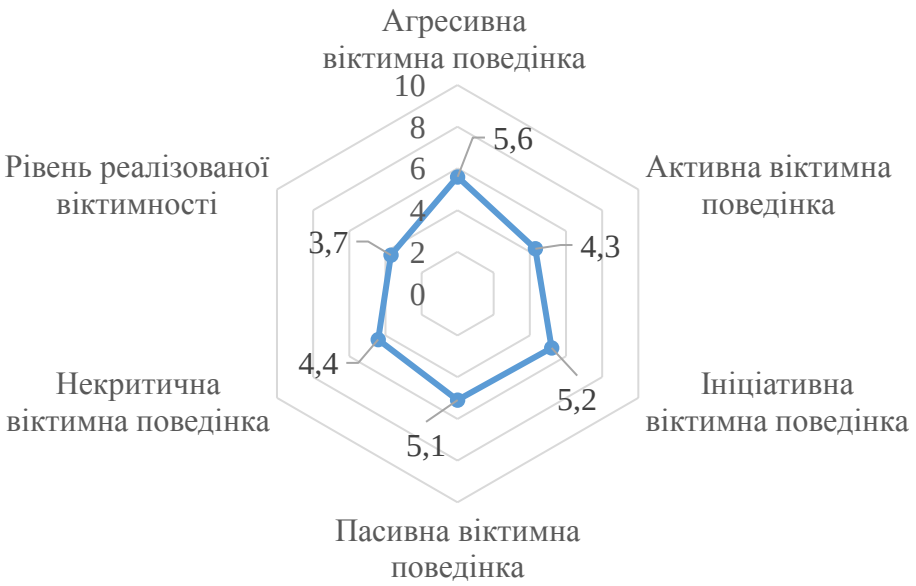


Рисунок 3.1 – Середньогрупові показники віктимності студентської молоді (стени)

Виявлено, що рівень агресивності студентської молоді також не перевищує показників норми (36,7±3,55), тобто агресивність для молоді є характеристикою, яка дозволяє людині діяти без надмірних негативних проявів проти інших.

Проведене дослідження підтвердило високу актуальність тематики, адже 93% опитаних обізнані із темою кібершахрайства, хоча лише 7% вибірки змогли вірно визначити перелік шляхів незаконного маніпулювання кібершахраїв. Єдине уявлення, можна визначити стійким, – щодо небезпеки переходу за сумнівними посиланнями, однак орієнтація у небезпеці подібної

поведінки не виключає подібних проявів. Третина студентів (33% вибірки) зазначили, що не звертають увагу на безпечність сайтів, якими вони користуються. Ще 28% опитаних впевнені у небезпеці сайтів, які вони відвідують. Менше половини опитаних студентів (39%) переконані, що послуговуються лише перевіреними ресурсами. Однак питання перевірки надійності видається суб'єктивним, адже значно вища частка студентів, які вказали, що користувалися так званими «піратськими» сайтами (88%). Лише 8% опитаних висловили відчуття безпеки щодо кібершахрайства.

Віртуальний простір використовується абсолютно усіма опитаними студентами. Більшість студентської молоді (89% опитаних) користуються мережею Інтернет кожного дня в навчальних, професійних і розважальних цілях. Уникають непродуктивного використання віртуального простору 7% респондентів, натомість виключно розважальне його призначення вбачають 4%.

94% опитаних студентів стикалися з шахраями в Інтернеті особисто або опосередковано через найближче коло спілкування. Користування недостатньо надійними та безпечними ресурсами віртуального простору є ознакою схильності до віктимної поведінки. Цей висновок підтверджує нерегулярність зміни паролів доступу, яку визнають 58% опитаних, готовність більшості (відповідно 88%) надіслати гроші у відповідь на прохання знайомих у соціальних мережах. 61% опитаних студентів низько оцінюють захищеність власних коштів на віртуальних рахунках, при цьому інакше сприймаючи карткові банкові рахунки. Суттєво вище особисте відчуття безпеки студенти демонструють до власних коштів, які зберігаються на карткових рахунках, ніж на віртуальних ($t_{емп} = 4.7$, $p^{0,01}$).

Суб'єктивне відчуття незахищеності поширене серед студентів у питанні безпеки персональних даних (63% опитаних) та інформації, яка пересилається віртуальними засобами (44% опитаних). Значна частка вибірки (21% опитаних) не довіряють обміну «купівля/продаж» у віртуальному

просторі. 25% опитаних мають сумніви щодо можливостей пошуку роботи в Інтернеті.

Цікаво, що тривалість користування мережею пов'язана із частотою зміни паролів (табл. 3.1). Однак причиною є не набуття навичок безпечного користування кібепростором, а зовнішні фактори: забування старих паролів (цей варіант як причину вказали 42 % опитаних); зафіксовані ознаки зовнішнього втручення (13%); особливості конкретних сайтів (11%). При цьому четверта частина досліджуваних (24%) довіряє таку інформацію, як паролі, сім'ї чи друзям.

Таблиця 3.1 – Взаємозв'язки проявів сприйняття кібершахрайства та особистісних рис і соціально-демографічних характеристик студентської молоді молоді

	1	2	3	4	5	6	7	8	9	10
1. Фігура [1]	1									
2. Час у кіберпросторі	-	1								
3. Частота і причини зміни паролів у кіберпросторі	-	,28**	1							
4. Оцінка ризиків у кіберпродажах	-	-	-	1						
5. Готовність відмовитися від кіберресурсів	-	-	-	-	1					
6. Користування «піратським» контентом	-	-	-	-	-	1				
7. Уявлення про шляхи кібершахрайства	-	-	-	-	-	-	1			
8. Досвід віктимізації від кібершахрайства	-	-,284**	-	-	-	-	-	1		
9. Стать	-	-	-,284**	-	-	-	-	-	1	
10. Напрям підготовки	-,22*	-	-,22*	-	-	-	-	-	,53**	1

Примітки: * p≥0,05; ** p≥0,01

[1] за психогеометричним тестом С. Делінгер.

Можна визначити існування загального уявлення про небезпеку кібершахрайства, зокрема, 92% вибірки висловили установку щодо відмови від користування підозрілими ресурсами, якщо вони пов'язаними із ризиками щодо персональних даних чи фінансів. У той же час ці уявлення варто визначити недостатньо чіткими, адже 14% опитаних готові публікувати у мережі будь-які персональні дані або не задумуються про безпеку цих даних. Більшість опитаних (70%) не має уявлення про ризики використання програмного забезпечення із джерел, подібних Play Маркет чи App Store. Третина респондентів (37%) не мають інформації щодо фінансових пірамід.

Виявлено зворотні кореляційні взаємозв'язки проявів агресивності та суб'єктивною схильністю до користуванням студентами перевіреними сайтами ($r=-0,18$, $p^{0,05}$). Встановлено позитивний кореляційний зв'язок між готовністю користуватися «піратськими» сайтами та ініціативним типом віктимної поведінки ($r=-0,19$, $p^{0,05}$), а також з некритичним типом віктимності ($r=-0,2$, $p^{0,05}$).

Зафіксовані відмінності $t_{емп}=2.6$ ($p^{0,05}$) між показниками віктимності студентів, які впевнені у безпеці пересилання даних Інтернет-засобами, (6,97±2,52) та тими, які має сумніви щодо безпеки даних при пересилці (5,65±2,78). Водночас переважно суб'єктивні переживання не впливають на віктимність особистості. За іншими параметрами порівняння статичні відмінності між показниками віктимності студентів, які мають сумніви щодо безпеки користування віртуальним простором, та тими, які впевнені у його відносній безпечності, не виявлені. Так само не впливає на ризики стати жертвою впевненість людини у знанні шляхів віртуального шахрайства. Рівень віктимності студентів, що мають дану впевненість, а також тих, хто висловлює сумніви, статистично не відрізняється.

Не виявлено відмінностей в рівні критичності оцінки рекламних продуктів у віртуальному просторі залежно від досвіду використання віртуальних продуктів, поширені рекламними засобами ($\varphi_{емп.}= 0.82$).

За методикою Деллінгера визначено домінування психотипу «коло», пов'язаного із комунікативною спрямованістю особистості, серед студентів соціогуманітарних спеціальностей ($\varphi_{емп.}$=1,69, p≥0,05), а серед студентів технічних спеціальностей – психотипу «трикутник», який пов'язують із лідерськими схильностями ($\varphi_{емп.}$=2,32, p≥0,01). Зазначимо, що цей результат слід у першу чергу пов'язувати із нерівномірним розподілом досліджуваних за статтю у підгрупах порівняння за ознакою напряму підготовки. Важливо, що результати дослідження свідчать про відсутність взаємозв'язків суб'єктивних проявів сприйняття кібершахрайства та так званою «суб'єктивною фігурою» С. Делінгер (табл. 3.1).

Отже, кібершахрайство, як злочин у межах віртуального простору, має специфічні прояви відносно аналогічного типу злочинів у реальному житті. Віртуальна взаємодія відзначається особливими ризиками деперсоніфікації користувачів, меншим ступенем регламентації та соціального контролю. Поширеність віртуальної взаємодії та її проникнення у різноманітні сфери соціального життя людини обумовлює зростання частоти, різноманіття та масштабів кібершахрайства [72].

3.2. **Визначення рівня кібервразливості споживачів фінансових послуг**

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

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

Національний банк України також посилює контроль за виконанням фінансовими установами заходів із забезпечення кіберзахисту та інформаційної безпеки. З прийняттям постанови Правління Національного банку України від 16 січня 2021 року № 4 [88] фінансові установи зобов'язані щорічно проводити самооцінку з оцінювання ризиків власної інформаційної безпеки та подавати дану інформацію до національного регулятора. Дані регуляторні заходи сприятимуть приведенню вітчизняного законодавства у сфері кіберзахисту фінансової системи до міжнародних стандартів та принципів, а саме Банку міжнародних розрахунків "Керівництво з кіберстійкості для інфраструктур фінансового ринку" [89] та Європейського центрального банку "Очікування з оверсайта щодо кіберстійкості інфраструктур фінансового ринку" [90] Крім цього, починаючи з серпня 2021 року Національний банк України та кіберполіція співпрацюватимуть для посилення ефективності протидії кіберзлочинам у фінансовій сфері.

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

У сучасних умовах фінансові установи деяких країн світу укладають попередню угоду зі своїми клієнтами, де чітко зазначається необхідний спосіб ідентифікації та аутентифікації клієнта при підтвердженні фінансової транзакції [91].

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

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

– збір та обробка статистичних даних, що прямо та опосередковано характеризують ступінь обізнаності клієнтів фінансових установ щодо ймовірних кібершахрайств та способів захисту від кіберзагроз при здійсненні фінансових транзакцій;

– визначення пріоритетності змінних, обраних на попередньому етапі;

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

Початковим етапом розробленого науково-методичного підходу є збір та систематизація індикаторів, що прямо та опосередковано характеризують вразливості споживачів фінансових послуг до кіберзагроз (проінформованість про ознаки підозрілих кібершахрайств, способи кіберзахисту, канали інформування про кібератаки). Джерелом первинних даних слугувало опитування громадян Європейського Союзу щодо їх ставлення до питань кібербезпеки, яке проводилося у 2020 році [54]. Для потреб даного дослідження відібрано 17 індикаторів, які виключно стосуються фінансових транзакцій та захисту персональних даних, а саме: частка населення, які

хвилюються безпекою онлайн-платежів (R1); частка населення, які мають хвилювання щодо несанкціонованого використання їх персональних даних (R2); частка населення, які змінювали протягом останніх 12 місяців пароль до інтернет-банкінгу (R3); частка населення, які зазначають низький рівень інформованості про ризики кіберзлочинності (R16); частка населення, яким відомо хоча б один спосіб повідомлення про кіберзлочин (R17), а також група показників, що відображають превентивні заходи громадян для підвищення їх рівня захисту віртуальному просторі (R4- R15): частка населення, яка зменшила кількість банківських операцій в Інтернеті (R4); частка населення, яка рідше вводить особисту інформацію на веб-сайтах (R5); частка населення, яка змінила налаштування безпеки (наприклад, у браузері, соціальній мережі, пошуковій системі) (R6); частка населення, яка відвідуєте лише ті веб-сайти, які знаєте і яким довіряє (R7); частка населення, яка використовує різні паролі для різних сайтів (R8); частка населення, яка не відкриваєте електронні листи від незнайовим людей (R9); частка населення, яка встановила актуальне антивірусне програмне забезпечення (R10); частка населення, яка скасувала онлайн-покупку через підозри щодо продавця або веб-сайту (R11); частка населення, яка використовує більш складні паролі, ніж раніше (R12); частка населення, яка використовує біометричні функції (наприклад, розпізнавання обличчя, відбиток пальця) (R13); частка населення, яка не підключається до Інтернету через незахищені точки доступу (R14); частка населення, яки не турбує безпека в Інтернеті (R15). Об’єктом дослідження обрано 30 країн Європи. Узагальнена інформація у розрізі 17 індикаторів станом на 2020 рік представлена в додатку, а основні результати подано в таблиці 3.2.

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

щодо несанкціонованого використання їх персональних даних при здійсненні розрахунків.

Таблиця 3.2 – Інформація щодо обізнаності громадян про кібератаки та способи захисту від них в європейських країнах у 2020 році

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

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

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

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

показників кібервразливості споживачів фінансових послуг при подальшому обчисленні єдиного інтегрального індексу кіберврзарливості, проводяться наступні проміжні кроки обчислень:

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

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

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

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

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

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

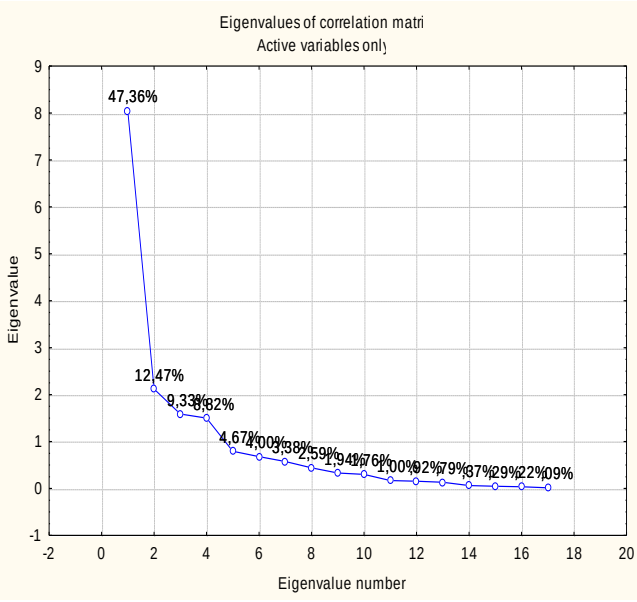
Дана умова введена в економетричну модель, оскільки вищезазначені індикатори (R4- R15) відображають ступінь використання превентивних заходів громадянами для підвищення їх рівня захисту віртуальному просторі.

- значення показників кібервразливості не повинні перевищувати і не повинні бути менше гранично допустимих рівнів:

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

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

Для встановлення гранично допустимих рівнів показників кібервразливості скористаємось методом головних компонент можливостями програмного пакету Statistica. За своєю сутністю метод полягає у виборі нової ортогональної системи координат у просторі спостережень. Як першу головну компоненту обирають напрям, вздовж якого масив спостережень має найбільшу дисперсію. Кожну наступну компоненту обирають також з умови максимізації частки дисперсії, що залишилася, вздовж неї, доповненої умовою ортогональності всім раніше обраним компонентам. При цьому із зростанням номера компоненти буде зменшуватися пов’язана з нею частка загальної дисперсії. Результати представимо на рисунку 3.2.



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

Рисунок 3.2 – Скріншот фрагмента програми Statistica графіку кам’янистого опису, власних значень кореляційної матриці та пов’язаних статистичних показників

На основі аналізу рисунку 3.2 можна зробити висновок про доцільність для оцінювання граничних обмежень показників кібервразливості враховувати перші чотири головні компоненти, представлені першими чотирма факторами, на варіацію яких припадає 77,98% загальної варіації, про що свідчить як графік кам'янистого осипу (лівий фрагмент рисунку 1), так і табличні значення власних значень факторів в розрізі показників (правий фрагмент рисунку 3.2). Враховуючи дані рисунку 1 та вкладу змінних на основі кореляції показників кібервразливості споживачів фінансових послуг (таблиця 3.3, графи 1-4), визначимо обмеження для визначення пріоритетності RO_i на сонові середньої арифметичної зваженої:

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

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

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

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

Результати обчислень за формулою (3.4) представимо у графі 5 таблиці 3.3.

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

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

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

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

Таблиця 3.3 – Вклад змінних на основі кореляції, обмеження пріоритетності та ваги показників кібервразливості споживачів фінансових послуг

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

Вирішення задачі оптимізації вагових коефіцієнтів показників кібервразливості споживачів фінансових послуг як задачі лінійного програмування пропонується провести за допомогою інструментарію «Пошук рішення» MS Excel, зокрема методу узагальненого знижуючого градієнту.

Результати проведених розрахунків представимо в графі 6 таблиці 3.3. Таким чином, найбільш впливовим при оцінюванні кібервразливості споживачів фінансових послуг є показник R2, на частку впливу якого припадає 11,1%. Наступними релевантними показниками виступають R1 та R16, вагові коефіцієнти впливу в розрізі яких сягають 10,4%.

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

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

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

k – константа, яка визначає кількість показників кібервразливості;

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

Результати проведених обчислень за формулою Кіні (3.6) систематизуємо в табличному вигляді, зокрема графах 1 та 2 таблиці 3.4.

Таблиця 3.4 – Абсолютний та відносний рівні кібервразливості споживачів фінансових послуг на множині відібраних 28 країн Європи

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

Абсолютне значення індексу кібервразливості споживачів фінансових послуг на множині розглянутих країн Європи не дозволяє об’єктивно оцінити та порівняти країни між собою, що призводить до необхідності визначення відносної оцінки кібервразливості споживачів фінансових послуг. Для цього визначимо відносний рівень кібервразливості споживачів фінансових послуг як співвідношення абсолютної оцінки до максимально можливого рівня, який спостерігається на досліджуваній множині значень складових показників. Отже, максимально можливе значення абсолютного індекса кібервразливості обчислимо наступним чином:

$$ICR_{max}(R_1, \dots, R_{17}) = \frac{1}{k}\left\{ \prod_{i=1\div 3,16} \left[1 + k \cdot w(\max_{i=1\div 17} R_i) \cdot \max_{i=1\div 17} R_i\right] \cdot \prod_{i=4\div 15,17} \left[1 + k \cdot w(\min_{i=1\div 17} R_i) \cdot (1 - \min_{i=1\div 17} R_i)\right] - 1 \right\} \quad (3.7)$$

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

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

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

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

Представимо результати проведених обчислень за допомогою формули (3.8) на рисунку 3.3.

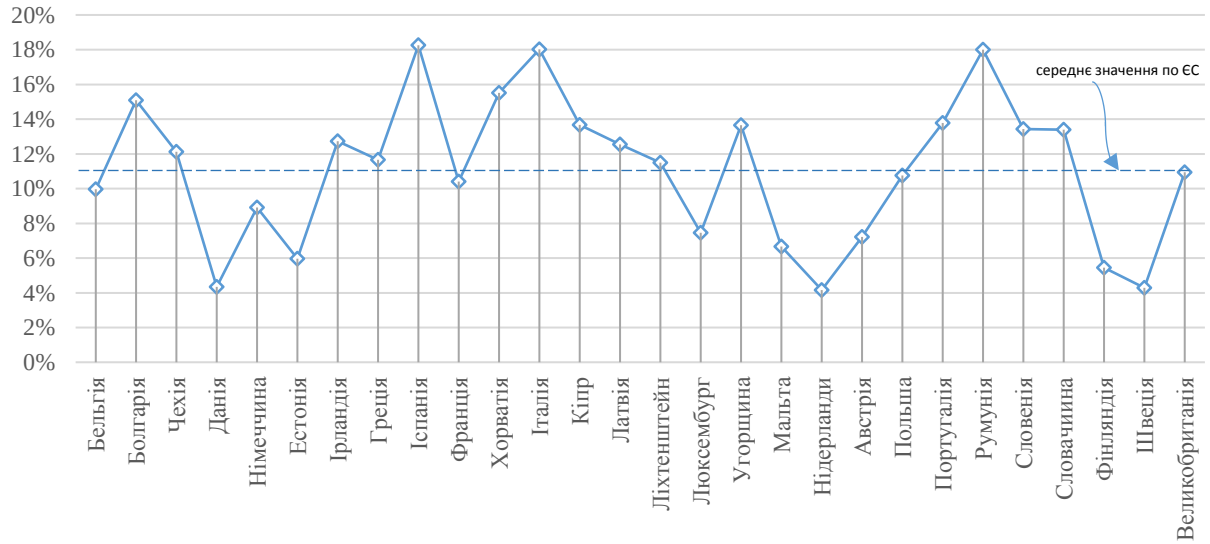


Рисунок 3.3 – Результати оцінювання рівня кібервразливості споживачів фінансових послуг у країнах Європи станом на 2020 рік

Проведене дослідження засвідчило, що рівень кібервразливості громадян ЄС становить у середньому 11%, що дозволяє стверджувати про усвідомленість населенням європейський країн наявних загроз у віртуальному

просторі, способів захисту від кіберзлочинності. Проте рівень кібервразливості споживачів фінансових послуг у розрізі країн ЄС не є однорідним, а саме найменшим ризик стати жертвою кібершахрайства мають громадяни таких країн як Данія, Нідерланди, Швеція. До країн з найвищими значеннями розрахованого рівня кібервразливості споживачів фінансових послуг (18%) належать: Іспанія, Італія, Румунія.

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

3.3. **Побудова фазового портрету потенційної жертви кіберзлочинності у сфері фінансових послуг**

Активізація зусиль щодо зменшення кількості кібержертв від фінансових операцій неможлива у відриві від наукового забезпечення системи кіберзахисту. Сучасний розвиток інформаційних технологій дозволяє акумулювати великі масиви даних, їх обробляти та отримувати науково обґрунтовані закономірності, які доцільно враховувати при формуванні системи попередження кіберзагроз у фінансовому секторі. Одним з провідних напрямків у вирішенні цього завдання є розробка фазового портрету ймовірної жертви кібершахрайства у фінансовій системі, що дозволяє ідентифікувати ознаки кіберзагрози на ранніх етапах, відповідно відреагувати на неї, тим самим нейтралізувати або мінімізувати негативні наслідки. Використання технології профайлінгу дозволяє оцінити та спрогнозувати поведінку споживача фінансових послуг в умовах зростаючого ризику кіберщахрайств

на основі систематизації та встановлення причинно-наслідкових зв'язків між найбільш інформативними персоніфікованими їх ознаками. Зауважисо, що технологій профайлінгу є досить поширеною практикою в діяльності правоохоронних органів для встановлення типових психотипів злочинців.

Для його побудови використано дані соціологічного опитування громадян Європейського Союзу станом на 2020 рік. Для аналізу обрано 25 країн світу. В основі побудови фазового портрету споживача фінансових послуг є індикатор «частка населення, які стикалися з кібершахрайствами у сфері фінансових послуг» у розрізі європейських країн, динаміка якого представлена на рисунку 3.4.

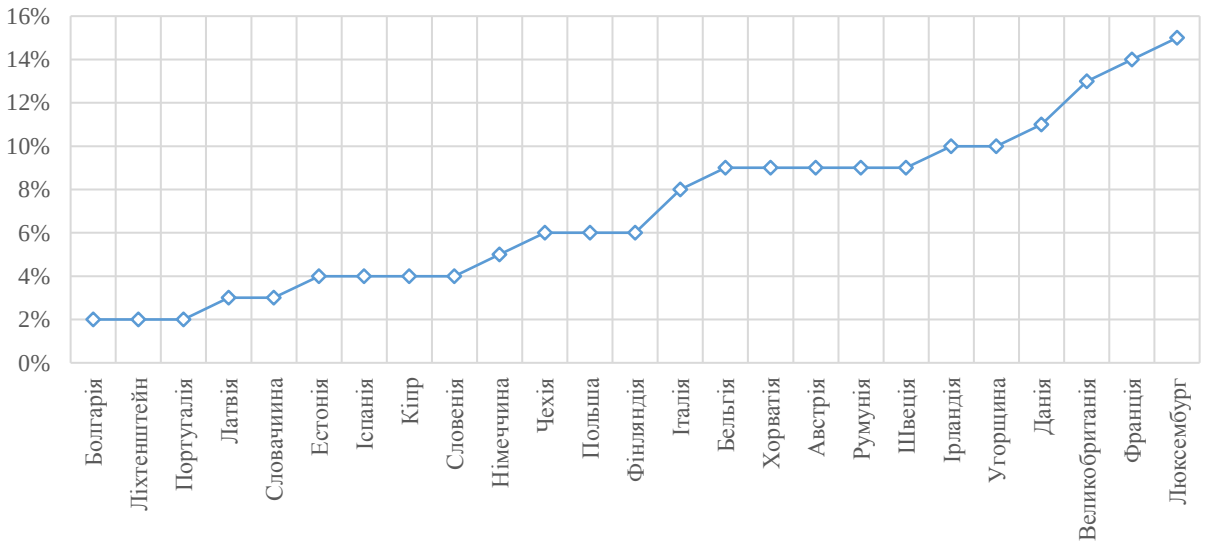


Рисунок 3.4 – Частка громадян країн Європейського Союзу, які стикалися з кібершахрайствами у сфері фінансових послуг у 2020 році, %

Дані рисунку 3.4 наочно демонструють, що до країн з найвищими показниками кібершахрайства у сфері фінансових послуг належить Люксембург (15%), Франції (14%), Великобританії (13%) та Данії (11%). У 2020 році у середньому кожний 10-й житель Європейського Союзу став кібержертвою при здійсненні фінансових транзакцій.

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

Таблиця 3.4 – Вхідні дані для побудови фазового портрету жертви кіберзлочинності

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

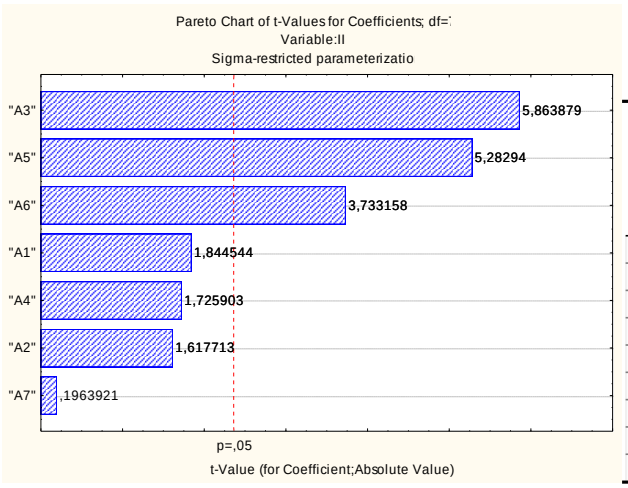
Сформована статистична база для побудови фазового портрету жертви кіберзлочинності подана в таблиці В.2, додатку В.

Наступним кроком є вибір найбільш релевантних індикаторів, що характеризують кібершахрайства при здійсненні фінансових транзакцій В

рамках даного етапу проведений одномірний тест значущості впливу різних інформаційних ознак на результативний показник – «особи, які стикалися з кібершахрайствами у сфері фінансових послуг» за допомогою сигма-обмеженої параметризації та діаграми Парето t-значень для коефіцієнтів GRM та ідентифіковано релевантні факторами віктимної поведінки споживача фінансових послуг (рисунок 3.5 – 3.9). Для реалізації даного етапу використовується інструментарій Statistics.

Інформаційна ознака «вік особи».

Дані стосовно опитування громадян Європейського Союзу щодо їх відношення до питань кібербезпеки акумулювалися у розрізі 7 градацій вікової структури. У 2020 році найвищі значення показника кіберзлочинності у сфері фінансових послуг (21%) зафіксовано для громадян Литви у віці 25-34 роки та громадян Італії у віці більше 75 років. Для визначення найбільш значущих інформаційних ознак «вік» з позиції стати кібержертвою побудовано діаграму Парето (рис. 3.5).

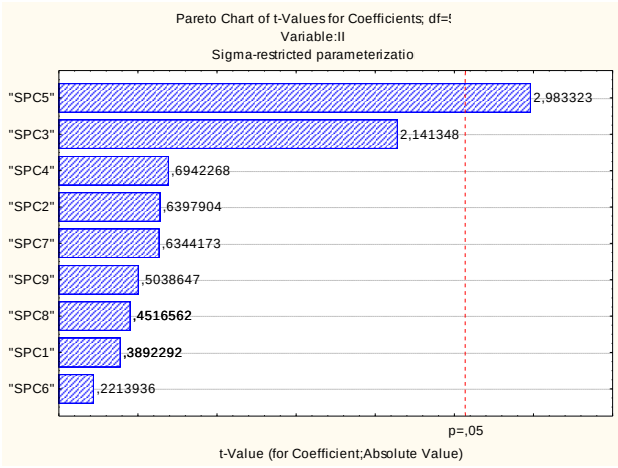


Univariate Tests of Significance fo(Spreadsheet3 a
Sigma-restricted parameterization
Effective hypothesis decomposition

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

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

На основі даних рисунку 3.5, в правому фрагменті якого приведені одномірні результати для оцінки ступеня та характеру взаємозв'язку між рівнем кібершахрайства у сфері фінансових послуг та віковою структурою, можна стверджувати, що статистично значущими виступають такі ефекти, як: особи у віці від 35 до 44 років (A3); від 55 до 64 років (A5); від 65 до 74 років (A6), оскільки рівні значущості p критерія Фішера менше 0,05. Найбільший вклад в загальну модель вносить ефект A3, оскільки сума квадратів відхилень SS, яка приймає значення 0,000697, має найбільше значення. Далі вклад статистично значущих ефектів розподіляється наступним чином: A5 та A6. Візуальним підтвердженням значущості даних трьох ефектів виступає діаграма Парето t-значень значущості (лівий фрагмент рисунку 3.5).



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

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

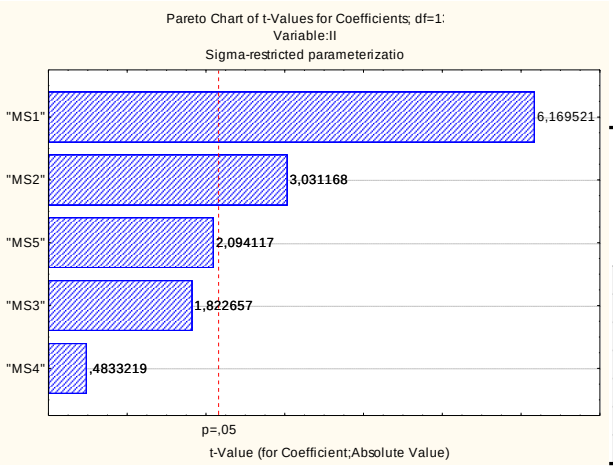
Рисунок 3.6 – Скріншот фрагменту діаграми Парето t-значень значущості (лівий фрагмент) та одномірного тесту значущості впливу інформаційної ознаки «сфера діяльності особи» на результативний показник (правий фрагмент)

Інформаційна ознака «сфера діяльності особи».

Найбільший рівень кібершахрайства серед споживачів фінансових послуг зафіксовано для наступних сфер їх діяльності: особи, які навчаються (17% – Угорщина); фрілансер (23% – Данія); управлінець (23% – Ірландія);

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

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



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

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

Рисунок 3.7 – Скріншот фрагменту діаграми Парето t-значень значущості (лівий фрагмент) та одномірного тесту значущості впливу інформаційної ознаки «сімейний статус» на результативний показник (правий фрагмент)

Інформаційна ознака «сімейний статус особи».

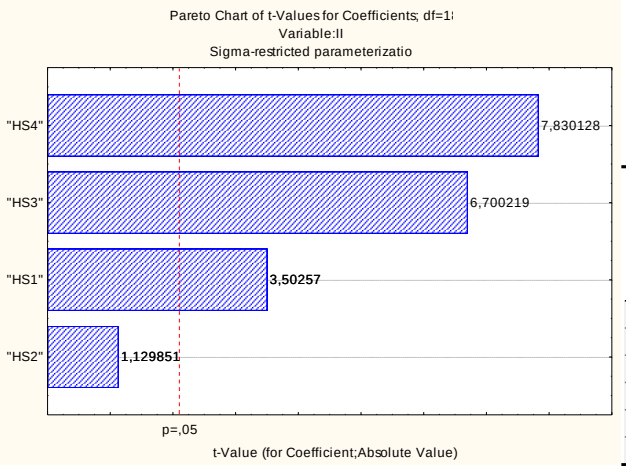
Серед європейських країн жертвами кіберзлочинності у середньому ставали 7% одружені/заміжні особи (тоді як у Франції – 16%, Латвія – 15%); 8% одинокий(-а), який(-а) проживає з партнером (Італія, Румунія – 14%); 7% неодружений/незаміжня (Латвія – 15%, Великобританія – 13%);

7% розлучений (-а) (Великобританія – 20%, Франція – 16%); 9% вдова/вдівець (Франція – 21%).

Оскільки рівень значущості p критерія Фішера менше 0,05 лише для двох показників (одружені/заміжні особи (MS1), одинокий(-а), який(-а) проживає з партнером (MS2)), то можемо стверджувати про необхідність їх подальшого врахування в наступних розрахунках при побудові фазового портрету кібержертви споживача фінансових послуг. Найбільший вклад в загальну модель вносить ефект MS1, оскільки сума квадратів відхилень SS має найбільше значення (0,001898). Візуальним підтвердженням значущості даних двох ефектів виступає діаграма Парето t-значень (лівий фрагмент рисунку 3.7).

Інформаційна ознака «стан сім'ї».

Домогосподарства, які мають дітей, частіше ставало жертвою кібершахрайства при користуванні фінансовими послугами. Результати відбору значимих інформаційних чинників «стан сім'ї» подано на рисунку 3.8.



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

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

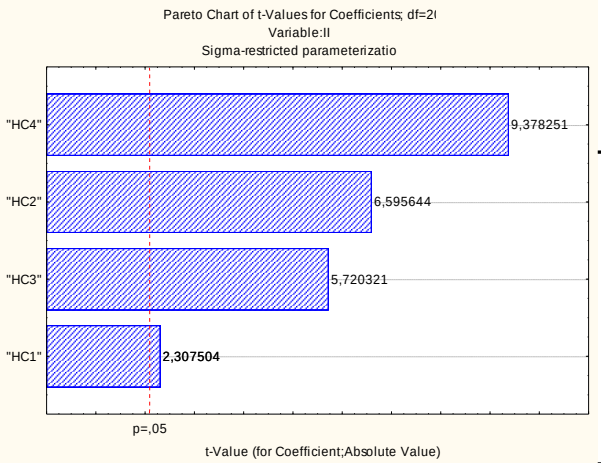
Рисунок 3.8 – Скріншот фрагменту діаграми Парето t-значень значущості (лівий фрагмент) та одномірного тесту значущості впливу інформаційної ознаки «стан сім'ї» на результативний показник (правий фрагмент)

На основі даних рисунку 3.8, зауважимо, що найбільш релевантними (рівень значущості p критерія Фішера менше 0,05) характеристиками

інформаційної ознаки «стан сім'ї» є одне домогосподарство без дітей (HS1); декілька домогосподарств без дітей (HS3); декілька домогосподарство з дітьми (HS4). Найбільший вклад в загальну модель вносить ефект HS4 - Household with children оскільки сума квадратів відхилень SS, яка приймає значення 0,002, має найбільше значення. Далі вклад статистично значущих ефектів розподіляється наступним чином: HS3 - Multiple Household without children, HS1 - Single Household without children. Графічне представлення отриманих результатів відображає діаграма Парето (лівий фрагмент рисунку 3.8).

Інформаційна ознака «склад сім'ї».

До топ європейських країн, особи яких ставали кібержертвами у сфері фінансових послуг залежно від складу їх сім'ї, відзначимо наступних: громадян Литви, які мають одну дитину (22%); громадян Данії, які мають троє дітей (20%); громадян Франції, які мають чотири та більше дітей (18%). Проведений аналіз відбору найбільш значущих складових інформаційної ознаки «склад сім'ї» підтвердив необхідність включення всіх елементів: HC1-HC4 (рис. 3.9).



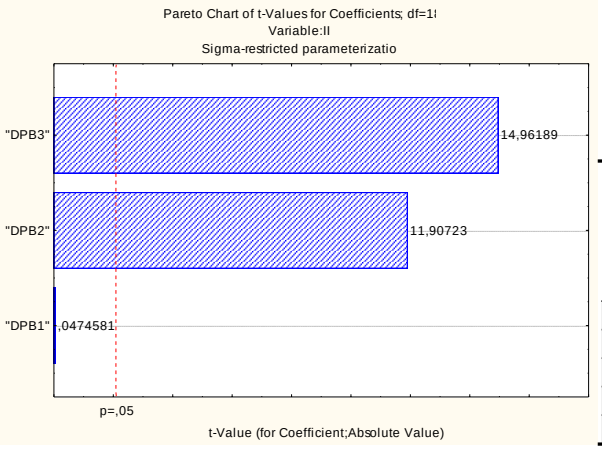
Univariate Tests of Significance fo (Spreadsheet3 a
Sigma-restricted parameterization
Effective hypothesis decomposition

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

Рисунок 3.9 – Скріншот фрагменту діаграми Парето t-значень значущості (лівий фрагмент) та одномірного тесту значущості впливу інформаційної ознаки «склад сім'ї» на результативний показник (правий фрагмент)

Інформаційна ознака «труднощі з оплатою рахунків».

За результатами аналізу даних опитування встановлено, що 12% середньостатистичних європейців мали труднощі з оплатою рахунків, та відповідно вони у більшій мірі схильні стати жертвою кібершахрайства. Побудована діаграма Парето та розрахований одномірний тест значущості (рис. 3.10) вказує, що найбільш релевантними складовими для характеристики інформаційної ознаки «труднощі з оплатою рахунків» є відповідь «часто» (DPB2); відповідь «інколи» (DPB3). Найбільший вклад в загальну модель вносить ефект DPB3, оскільки сума квадратів відхилень (SS) для даного показника є найбільшою (0,009393).



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

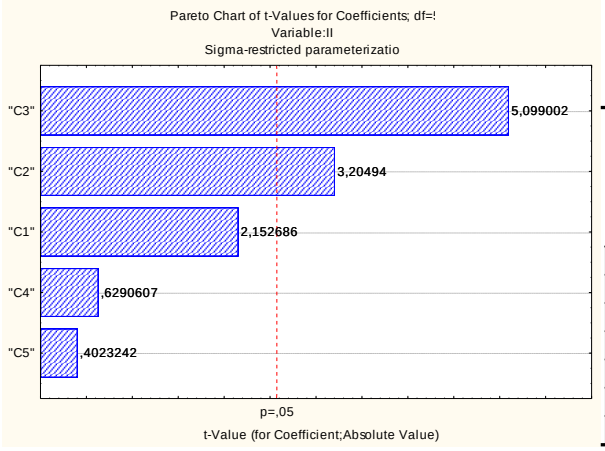
Effect	SS	Degr. of Freedom	MS	F	p
Intercept	0,00001	1	0,00001	0,355(	0,55870(
"DPB1"	0,00000(	1	0,00000(	0,002	0,96267
"DPB2"	0,00594	1	0,00594	141,782(	0,00000(
"DPB3"	0,00939	1	0,00939	223,858(	0,00000(
Error	0,00075	18	0,00004		

Рисунок 3.10 – Скріншот фрагменту діаграми Парето t-значень значущості (лівий фрагмент) та одномірного тесту значущості впливу інформаційної ознаки «труднощі з оплатою рахунків» на результативний показник (правий фрагмент)

Інформаційна ознака «соціальний статус особи».

Соціальний статус споживача фінансових послуг розглянуто у межах 5 градацій. Середньостатистичні європейці, які вважають себе належним до вищого класу (33%) частіше ставали жертвами протиправної діяльності у

віртуальному просторі порівняно з тими особами, які ставлять себе нижче в соціальній шкалі.



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

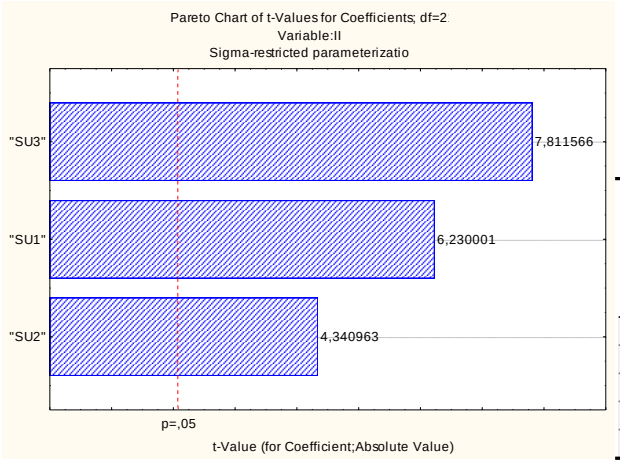
Effect	SS	Degr. of Freedom	MS	F	p
Intercept	0,00011	1	0,00011	2,7627	0,15737
"C1"	0,00018	1	0,00018	4,6340	0,08395
"C2"	0,00041	1	0,00041	10,2716	0,02386
"C3"	0,00105	1	0,00105	25,9998	0,00377
"C4"	0,00001	1	0,00001	0,3957	0,55692
"C5"	0,00000	1	0,00000	0,1618	0,70406
Error	0,00020	5	0,00004		

Рисунок 3.11 – Скріншот фрагменту діаграми Парето t-значень значущості (лівий фрагмент) та одномірного тесту значущості впливу інформаційної ознаки «соціальний статус особи» на результативний показник (правий фрагмент)

Дані рисунку 3.11 вказують, що рівень значущості критерія Фішера менше 0,05 виключно для двох індикаторів: нижчий середній клас (С2); середній клас (С3), що свідчить про їх статистично значущість.

Інформаційна ознака «тип місцевості».

Найбільша кількість правопорушень, пов’язаних із задіянням фінансової та моральної шкоди при фінансових розрахунках, пов’язана з особами, які проживають у великих містах: у Хорватії – 22% громадян, Франції – 18%, Бельгія, Австрія, Великобританія – 15%. Результати побудови графіка Парето та розрахунку одномірного тесту значущості подано на рисунку 3.12.



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

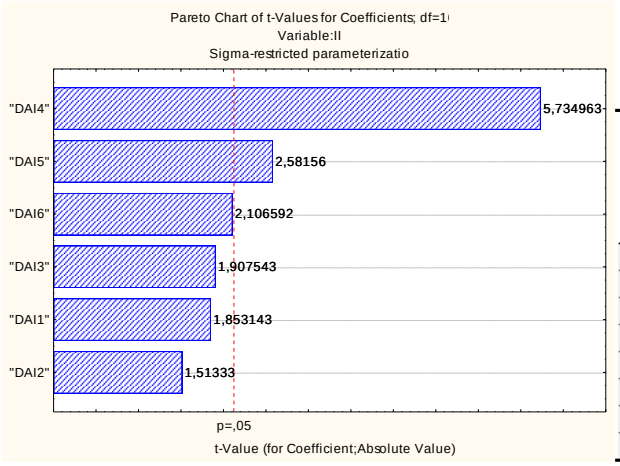
Effect	SS	Degr. of Freedom	MS	F	p
Intercept	0,00000	1	0,00000	0,0001	0,98919
"SU1"	0,00293	1	0,00293	38,8129	0,00000
"SU2"	0,00142	1	0,00142	18,8439	0,00028
"SU3"	0,00461	1	0,00461	61,0205	0,00000
Error	0,00158	21	0,00007		

Рисунок 3.12 – Скріншот фрагменту діаграми Парето t-значень значущості (лівий фрагмент) та одномірного тесту значущості впливу інформаційної ознаки «тип місцевості» на результативний показни (правий фрагмент)

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

Інформаційна ознака «пристрої для доступу до Інтернету»

У середньому 13% жителів європейських країн, які ставали жертвами кібершахрайства, із-за використання ігрової консолі, тоді як у деяких європейських країнах цей показник перевищує у декілька разів: Румунія – 37%, Чехія – 36%, Угорщина – 35%. Крім ігрової консолі, за результатами опитування встановлено, що у середньому 11% європейців піддавалися кібератакам через недосконаліть системи захисту при здійсненні фінансових транзакцій через смарт-телевізори, тоді як у Румунії – 27% громадян, Угорщині – 26%, Латвія – 21%. Результати відбору значимих складових інформаційної ознаки «пристрої для доступу до Інтернету» подано на рисунку 3.13.



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

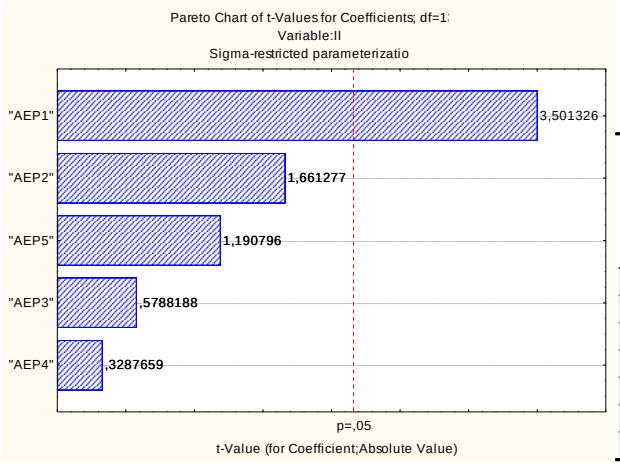
Effect	SS	Degr. of Freedom	MS	F	p
Intercept	0,00019	1	0,00019	4,7055	0,04547
"DAI1"	0,00014	1	0,00014	3,4341	0,08239
"DAI2"	0,00009	1	0,00009	2,2901	0,14969
"DAI3"	0,00015	1	0,00015	3,6387	0,07456
"DAI4"	0,00137	1	0,00137	32,8898	0,00003
"DAI5"	0,00027	1	0,00027	6,6644	0,02007
"DAI6"	0,00018	1	0,00018	4,4377	0,05129
Error	0,00066	16	0,00004		

Рисунок 3.13 – Скріншот фрагменту діаграми Парето t-значень значущості (лівий фрагмент) та одномірного тесту значущості впливу інформаційної ознаки «пристрої для доступу до Інтернету» на результативний показник (правий фрагмент)

Аналізуючи рисунок 3.13, можна зробити висновки, що на рівні 5% відхилення значущим виступає 2 показника: смартфон (DAI4); телевізор (DAI5). Візуальним підтвердженням значущості даних двох ефектів виступає діаграма Парето.

Інформаційна ознака «канали про інформування про кіберзлочинність»

Дані опитування засвідчили, що лише 13% жителів європейських країн проінформовані про способи повідомлення про кібератаку при здійсненні фінансових розрахунків. При цьому варто відзначити, що в деяких країнах Європи цей показник є критично низьким: Латвія – 1%, Іспанія, Португалія, Словаччина – 4%, Швеція – 5%. На рисунку 3.14 представимо результати побудови одномірного тесту значущості та діаграми Парето.



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

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

Рисунок 3.14 – Скріншот фрагменту діаграми Парето t-значень значущості (лівий фрагмент) та одномірного тесту значущоості впливу інформаційної ознаки «канали про інформування про кіберзлочинність» на результативний показник (правий фрагмент)

Дані рисунку 3.14 вказують, що зі складових інформаційної ознаки «канали про інформування про кіберзлочинність» доцільно включати виключно веб-сайт (AEP1).

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

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

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

Побудуємо мережу асоціативних правил причинно-наслідковості зв’язків між індикаторами кібервразливості споживачів фінансових послуг. Для реалізації даного етапу використаємо програмний продукт STATISTICA: команду Data Mining/Sequence, Association and Link Analysis. Отримані результати представимо у вигляді рисунку 3.15.

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

	Body	==>	Head	Support(%)	Confidence(%)
1	0,053493<AEP1<=0,0879(	==>	0,036834<HS1<=0,05361	20,0000(	55,555(
2	0,036834<HS1<=0,05361	==>	0,053493<AEP1<=0,08796	20,0000(	71,428(
3	0,056192<MS2<=0,07181	==>	0,053493<AEP1<=0,08796	20,0000(	83,333
4	0,053493<AEP1<=0,0879(	==>	0,056192<MS2<=0,07181	20,0000(	55,555(
5	0,019518<HC3<=0,0408	==>	0,053493<AEP1<=0,08796	20,0000(	55,555(
6	0,053493<AEP1<=0,0879(	==>	0,019518<HC3<=0,04083	20,0000(	55,555(
7	0,019420<G2<=0,0393	==>	0,053493<AEP1<=0,08796	20,0000(	62,500(
8	0,053493<AEP1<=0,0879(	==>	0,019420<G2<=0,03933	20,0000(	55,555(
9	0,023606<DPB2<=0,0511	==>	0,019420<G2<=0,03933	24,0000(	75,000(
10	0,019420<G2<=0,0393	==>	0,023606<DPB2<=0,05112	24,0000(	75,000(
11	0,023606<DPB2<=0,0511	==>	0,019420<G2<=0,039332, 0,019518<HC3<=0,040	20,0000(	62,500(
12	0,019518<HC3<=0,0408	==>	0,019420<G2<=0,039332, 0,023606<DPB2<=0,051	20,0000(	55,555(
13	0,019518<HC3<=0,040831, 0,023606<DPB2<=0,051	==>	0,019420<G2<=0,03933	20,0000(	83,333
14	0,019420<G2<=0,0393	==>	0,019518<HC3<=0,040831, 0,023606<DPB2<=0,051	20,0000(	62,500(
15	0,019420<G2<=0,039332, 0,023606<DPB2<=0,051	==>	0,019518<HC3<=0,04083	20,0000(	83,333

Рисунок 3.15 – Скріншот фрагменту ідентифікованих асоціативних правил

На основі поглибленого аналізу статистичних даних щодо кібершахрайств у сфері фінансових послуг шляхом побудови асоціативних правил, представлених на рисунку 12 та в таблиці В.3 (додатку В), можна зробити наступні висновки:

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

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

– з ймовірністю в 83,3% прослідковуються причинно-наслідкові зв’язки між наступними параметрами: «жінка, яка періодично відчуває фінансову труднощі та виховує трьох дітей», «жінка, яка має дитину», «жінка у віці 55-64 роки», «заміжня (одружена) особа, яка виховує двох дітей», «особа, яка проживає у невеликому місті та виховує двох (трьох) дітей»

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

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

ВИСНОВКИ

Стрімке впровадження інноваційних інформаційних технологій на різних рівня фінансової системи з одного боку сприяють підвищенню конкурентоспроможності країни на світовій арені, а також її інвестиційної привабливості, а з іншого – викликають зростання масштабів транскордонної економічної злочинності, збільшення та розповсюдження різноманітних схем кіберзлочинності, збільшення кількості обсягів нелегально отриманих доходів, що супроводжується вдосконаленням механізмів відмивання кримінальних коштів. З урахуванням посилення геополітичної конкуренції в кіберпросторі та посилення ландшафту кіберзагроз, особливо в умовах пандемії covid-19, питання захисту інформації від кібератак як на рівні фінансової установи, так і держави є постійно актуальною задачею сьогодення та прийдешнього п’ятиліття.

Масове впровадження цифрових технологій створює як додаткові можливості для розвитку фінансових установ, так і певні загрози (ризик порушення процесів, витік конфіденційних даних, а також банкрутсво окремих фінансових установ із-за посилення конкуренції на ринку фінансових послуг).

У роботі побудовано панельну регресію з випадковими ефектами для формалізації зв’язку між рівнем інтернет банкінгу та показниками цифровізації. Зокрема, збільшення використання фізичними особами Інтернету та здійснення інтернет-покупок на 1% стимулює збільшення рівня інтернет банкінгу на 1,08 % та 0,25% відповідно. Для оцінювання залежності рівня використання фінансових послуг онлайн від розвитку цифрових технологій найбільш адекватною є панельна регресія з випадковими ефектами. В країнах ЄС зростання рівня зайнятості у сфері інформаційно-комунітивних технологій та частки компаній, які займалися падготовкою та перепідготовкою свого персоналу цифровим навичкам на 1% призводило до зростання отримання фінансових послуг онлайн на 3,25% та 0,63 % відповідно.

У роботі розроблено та описано модель для аналізу закономірностей здійснення кібератак в країнах ЄС на основі використання асоціативних правил. Обрана методологія дозволяє обробляти великі бази даних шляхом формування певних економічних алгоритмів, вирішення яких сприяє пошуку розв'язку поставленого завдання з незначними часовими витратами.

За результатами емпіричного дослідження причин стрімкого поширення кібершахрайств у фінансовому секторі економіки шляхом нейронної моделі методом опорних векторів встановлено, що основними драйверами зростання кібершахрайства є частка населення, яка користується онлайн банкінгом, рівень навичок в Інтернеті, інтенсивність онлайн діяльності.

Для оцінювання взаємозалежності FinTech інновацій та фінансовими та кібернетичними злочинами за посередництва фінансових установ шляхом багатомірних адаптивних регресивних MAR-сплайнів встанволено, що на фінансові злочини не мають впливу кількість переданих до держфінмоніторингу повідомлень про підозрілі операції та діяльність банківських установ; на кіберзлочини не має впливу діяльність страхових компаній, натомість з показником фінтех всі інші показники мали мультиплікативний ефект, в тому числі потрійний.

Проаналізовано особливості феномену віктимізації особистості у віртуальному просторі у співставленні з віктимізацією у реальному середовищі. Теоретично визначено сутність віртуальної ідентичності особистості, її зв'язки із віктимізацією у віртуальному просторі. Обґрунтовано, що віртуальна ідентичність має специфічні риси, що впливають на ризики віктимізації індивіда у віртуальному просторі.

Проведено емпіричне дослідження віктимності студентської молоді, рівня агресивності особистості у взаємовідносинах з іншими та вимірювання обізнаності щодо кібервіктимізації. Встановлено, що середньозважені групові показники вразливості та агресивності студентської молоді фіксуються на рівні норми. При цьому студентська молодь переважно не має достатнього досвіду для формування власного типу реагування на вразливі ситуації.

Визначено схильність студентської молоді до користування недостатньо надійними ресурсами віртуального простору, а також високий ступінь поширеності досвіду зіткнення з кібершахрайством. Суб'єктивність розуміння ризиків віртуалізації діяльності посилює віктимність студентської молоді у мережі Інтернет та вимагає розроблення активних засобів впливу на формування свідомого користування віртуальними ресурсами.

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

З метою ефективної протидії кіберзагрозам і забезпечення стійкості фінансової системи доцільно прийняти комплекс заходів, направлених на моніторинг складових інформаційної безпеки фінансових установ, об'єднання зусиль національного регулятора та керівників фінансових установ щодо інформування про реальні та потенційні кібератаки, а також створення якісних компетенцій в сфері інформаційної безпеки шляхом підвищення кваліфікації працівників фінансових установ та національного регулятора.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Пігуль Є.І. Моделювання впливу цифровізації на розвиток фінансових технологій: робота на здобуття кваліфікаційного ступеня магістра: спец. 051 - економіка / наук. кер. В. В. Боженко. Суми: Сумський державний університет, 2021. 80 с.

2. Скринька Л.О. Економіко-математичне моделювання ефективності національної системи протидії кібершахрайствам та легалізації кримінальних доходів на основі методів виживання: робота на здобуття кваліфікаційного ступеня магістра: спец. 051 - економіка / наук. кер. О. В. Кузьменко. Суми: Сумський державний університет, 2021. 59 с.

3. Доценко Т. В. Удосконалення системи фінансового моніторингу як інструмент забезпечення економічної безпеки національної економіки: дис... д-ра філософії: 051. Суми, 2021. 305 с.

4. Боженко В. В., Пігуль Є. І. Вплив цифровізації на розвиток фінансових технологій. *Вісник Хмельницького національного університету. Серія: економічні науки.* 2021. №2. С.11-15.

5. Artificial intelligence applications in financial services. 2019. Marsh&McLennan companies. URL:: https://www.oliverwyman.com/content/dam/oliver-wyman/v2/publications/2019/ dec/ai-app-in-fs.pdf (дата звернення 15.04.2021).

6. Removing roadblocks. The new road of fintech. FinTech disruptors 2019. URL: https://www.paymentscardsandmobile.com/research/fintech-disruptors-2019-report/ (дата звернення 15.04.2021).

7. Гулей А.І., Гулей С.А. Цифрова трансформація вітчизняного банківського середовища в умовах розвитку фінтех-екосистеми. *Український журнал прикладної економіки.* 2019. Том 4. № 1. С. 6–15

8. Луцишин О. Як фінтех змінює світовий фінансовий порядок. *Світ фінансів.* 2020. Випуск 2(63). С. 102-114.

9. Руденко З.М. Вплив розвитку фінтех на банківський ринок в Україні. *Соціально-економічні проблеми сучасного періоду України*. 2018. Випуск 2 (130). С. 67-71.

10. Рубанов П. М. Структура ринку FinTech інновацій. *Науковий вісник Полісся.* 2019. № 2 (18). С. 184-189

11. Рубанов П. М. Роль FinTech інновацій у розвитку підприємницького сектору національної економіки. *Методичні підходи до формування стратегічного бачення соціально-економічного розвитку регіонів*: матеріали Міжнар. наук.-практ. конф., 22 лютого 2020 р. Дніпро: НО «Перспектива», 2020. С. 79-81.

12. Рубанов П. М. Використання ФінТех інновацій в діяльності сучасних банків. *Причорноморські економічні студії.* 2019. № 47-2. С. 116-120.

13. Семеног А. Ю. Екосистеми цифрових платформ як фактор трансформації бізнесу в умовах цифрової економіки. *Вісник КНУТД. Серія: Економічні науки.* 2019. Вип.№ 4(137). С. 39-50

14. Шевченко О.М., Рудич Л.В. Розвиток фінансових технологій в умовах цифровізації економіки України. *Ефективна економіка.* 2020. № 7. URL: http://www.economy.nayka.com.ua/pdf/7_2020/63.pdf (дата звернення 15.09.2021).

15. Albeshr S., Nobanee H. Blockchain Applications in Banking Industry: A Mini-Review. *SSRN Electronic Journal*. 2020. URL: http://dx.doi.org/10.2139/ssrn.3539152. (дата звернення 15.09.2021).

16. Risman A., Mulyana B., Silvatika B. A., Sulaeman A. S. The effect of digital finance on financial stability. *Management Science Letters*. 2021. P. 1979–1984. URL: https://doi.org/10.5267/j.msl.2021.3.012

17. Frame W.S., White L.J. Technological change, financial innovation, and diffusion in banking, (available at http://ssrn.com/abstract=2380060) and also in The Oxford Handbook of Banking, Second Edition Edited by Allen N. Berger, Philip Molyneux, and John O.S. Wilson

18. Lyeonov S., Bilan Yu., Rubanov P., Grenčíková A. Countries Financial Development and Digital Readiness as Determinants of Financial Sector Innovativeness. Proceedings of the 34rd International Business Information Management Association Conference, IBIMA 2019: Vision 2025: *Education Excellence and Management of Innovations through Sustainable Economic Competitive Advantage*, 13–14 November 2019. Madrid, 2019. P. 13604–13619

19. Association of Certified Fraud Examiners. Study: AI for fraud detection to triple by 2021. 2019. URL: https://www.acfe.com/ press-release.aspx?id=4295006598 (дата звернення 15.09.2021).

20. Wirdiyanti R. Digital Banking Technology Adoption and Bank Efficiency: The Indonesian Case. Ojk, (December). 2018. P. 1–34.

21. Carbó-Valverde S., Cuadros-Solas P. J., Rodríguez-Fernández F. The Effect of Banks' IT Investments on the Digitalization of their Customers. 2020. Global Policy, 11(S1), 9–17. URL: https://doi.org/10.1111/1758-5899.12749

22. Bazarbash M. FinTech in Financial Inclusion: Machine Learning Applications in Assessing Credit Risk. *IMF Working Papers*. 2019. 19(109). URL: https://doi.org/10.5089/9781498314428.001https://doi.org/10.17010/ijf/2020/v14i5-7/153326 (дата звернення 19.09.2021).

23. Huang Y., Zhang L., Li Z., Qiu H., Sun T., Wang X. Fintech Credit Risk Assessment for SMEs. *IMF Working Papers*. 2020. 20(193). URL: https://doi.org/10.5089/9781513557618.001

24. Frost J., Gambacorta L., Huang Y., Shin H. S., Zbinden P. BigTech and the changing structure of financial intermediation. *Economic Policy*. 2019. 34(100), 761–799. URL: https://doi.org/10.1093/epolic/eiaa003

25. Hari Krishna B. FinTech, BigTech and Banks : Digitalisation and its Impact on Banking Business Models. *Indian Journal of Finance*. 2020. 14(5–7). – URL: https://doi.org/10.17010/ijf/2020/v14i5-7/153326 (дата звернення 15.09.2021).

26. Martínez-Sánchez J.F., Cruz-García S., Venegas-Martínez F. Money laundering control in Mexico: A risk management approach through regression trees (data

mining). *Journal of Money Laundering Control*. 2020. 23(2), P. 427-439, URL: https://www.emerald.com/insight/content/doi/10.1108/JMLC%2D10%2D2019%2D0083/full/html

27. Arner D. W., Barberis J. N., Buckley R. P. The Evolution of FinTech: A New PostCrisis Paradigm?, University of Hong Kong, Faculty of Law Research Paper No. 2015/047

28. The Mobile Economy 2020. GSM Association URL: https://www.gsma.com/mobileeconomy/wp-content/uploads/2020/03/GSMA_MobileEconomy2020_Global.pdf (дата звернення 20.10.2021).

29. Total value of investments into fintech companies worldwide from 2010 to 2020. URL: https://www.statista.com/statistics/719385/investments-into-fintech-companies-globally/ (дата звернення 18.09.2021).

30. Global Social Network Users 2020. URL: https://www.emarketer.com/content/global-social-network-users-2020– (Дата звернення 15.08.2021).

31. PWC 2017 – Risk in review study. URL: https://www.oxfordeconomics.com/my-oxford/projects/364357

32. Europa-2020. A European strategy for smart, sustainable and inclusive growth. URL: http://ec.europa.eu/eu2020/pdf/COMPLET%20EN%20BARROSO %20%20%20007%20-%20Europe%202020%20-%20EN%20version.pdf

33. The Global Covid-19 FinTech Regulatory Rapid Assessment Report. World Bank Group and the University of Cambridge – URL: https://www.jbs.cam.ac.uk/wp-content/uploads/2020/10/2020-ccaf-report-fintech-regulatory-rapid-assessment.pdf

34. Pulse of Fintech H2.2020. KMPG. – URL: https://assets.kpmg/content/dam/kpmg/xx/pdf/2021/02/pulse-of-fintech-h2-2020.pdf

35. Лук'яненко І. Г., Городніченко Ю. О. *Сучасні економетричні методи у фінансах.* Навчальний посібник. – К.: Літера ЛТД, 2002

36. Wooldridge J. M. Econometric Analysis of Cross Section and Panel Data (MIT Press), 2002. 392 p.

37. Сажин Ю.В., Иванова И.А. Эконометрика: учебник; Мордов. гос. ун-т. – Саранск, 2014. – 316 с.

38. Akhta S., Sheorey P. A., Bhattacharya S., Ajith K. V. V. Cyber security solutions for businesses in financial services: Challenges, opportunities, and the way Forward. *International Journal of Business Intelligence Research*. 2021. 12(1). URL: https://doi.org/10.4018/IJBIR.20210101.oa5

39. Al-Tahat S., Moneim O. A. The impact of artificial intelligence on the correct application of cyber governance in Jordanian commercial banks. *International Journal of Scientific and Technology Research*. 2020. 9(3).

40. Noor U., Anwar Z., Amjad T., Choo K. K. R. A machine learning-based FinTech cyber threat attribution framework using high-level indicators of compromise. *Future Generation Computer Systems*. 2019. 96. URL: https://doi.org/10.1016/j.future.2019.02.013

41. Berdyugin A. A., Revenkov P. V. Cyberattack risk assessment in electronic banking technologies (the case of software implementation). *Finance: Theory and Practice*. 2020. 24(6). URL: https://doi.org/10.26794/2587-5671-2020-24-6-51-60

42. Mousa M., Sai A.A., Salhin G. An Exploration for the Motives behind Enhancing Senior Banker's Level of Organizational Resilience: A Holistic Case Study. *Journal of Intercultural Management*. 2017. 9(4). URL: https://doi.org/10.1515/joim-2017-0025

43. Yerdon V. A., Lin J., Wohleber R. W., Matthews G., Reinerman-Jones L., Hancock P. A. Eye-Tracking Active Indicators of Insider Threats: Detecting Illicit Activity During Normal Workflow. *IEEE Transactions on Engineering Management*. 2021. URL: https://doi.org/10.1109/TEM.2021.3059240

44. Alhogail A., Alsabih A. Applying machine learning and natural language processing to detect phishing email. *Computers and Security*. 2021. 110. URL: https://doi.org/10.1016/j.cose.2021.102414

45. Onete C. B., Vargas V. M., Chita S. D. Study on the implications of personal data exposure on the social media platforms. *Transformations in Business and Economics.* 2020. 19(2).

46. Andreou P. C., Anyfantaki S. Financial literacy and its influence on internet banking behavior. *European Management Journal.* 2021. 39(5). URL: https://doi.org/10.1016/j.emj.2020.12.001

47. Carlton M., Levy Y., Ramim M. Mitigating cyber attacks through the measurement of non-IT professionals' cybersecurity skills. *Information and Computer Security*. 2019. 27(1). https://doi.org/10.1108/ICS-11-2016-0088

48. Tweneboah-Koduah S., Atsu F., Prasad R. Reaction of stock volatility to data breach: An event study. *Journal of Cyber Security and Mobility*. 2020. 9(3). https://doi.org/10.13052/JCSM2245-1439.931

49. Arcuri M. C., Gai L., Ielasi F., Ventisette E. Cyber attacks on hospitality sector: stock market reaction. *Journal of Hospitality and Tourism Technology*. 2020. 11(2). URL: https://doi.org/10.1108/JHTT-05-2019-0080

50. Kuzmenko O.V., Dotsenko T.V., Skrynka L.O. Economic and mathematical modelling of the effectiveness of the national system for combatting cyber fraud and legalisation of criminal proceeds based on survival analysis methods. *Scientific Bulletin of Mukachevo State University. Series «Economics»*. 2021. № 8(1). С. 144-153.

51. Кузьменко О.В., Доценко Т.В., Боженко В.В., Світлична А.О. Закономірності здійснення кібератак в країнах ЄС на основі використання асоціативних правил. *Вісник СумДУ. Серія Економіка.* 2021. № 1. С. 95-103

52. Боженко В.В., Кушнерьов О.С., Кільдей А.С. Детермінанти поширення кіберзлочинності у сфері фінансових послуг. *Економічний форум*. 2021.

53. X-Force Threat Intelligence Index 2021. IBM Security. Available at: https://www.ibm.com/downloads/cas/M1X3B7QG

54. Europeans' attitudes towards cyber security. Special Eurobarometer 499. European Commision. 2020. URL: https://europa.eu/eurobarometer/surveys/detail/2249

55. Cyber Threat Landscape for the Finance Sector. F-Secure. 2019. URL: https://www.f-secure.com/content/dam/f-secure/en/business/common/collaterals/f-secure-cyber-threat-landscape-finance-sector.pdf

56. Internet Crime Report. Federal Bureau of Investigation. URL: https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

57. Боженко В.В., Койбічук В.В., Габенко М.М. Вплив кібершахрайств на фінансову систему на прикладі країн Євросоюзу. *Вісник СумДУ. Серія Економіка*. 2021. № 2. С. 47-52.

58. Nish A., Naumann S., Muir J. Enduring Cyber Threats and Emerging Challenges to the Financial Sector. Carnegie Endowment for International Peace. 2020. Available at: https://carnegieendowment.org/2020/11/18/enduring-cyber-threats-and-emerging-challenges-to-financial-sector-pub-83239

59. The Top Threat Actors Targeting Financial Services Organizations. *Insights*. 2018. URL: https://intsights.com/blog/the-top-threat-actors-targeting-financial-services-organizations

60. Savchuk T. O., Pryimak N. V., Slyusarenko N. V., Smolarz A., Smailova S., Amirgaliyev Y. Improved method of searching the associative rules while developing the software. *International Journal of Electronics and Telecommunications*.2020. 66(3), 425-430. doi:10.24425-ijet.2020.131895/715.

61. Horban, H., Kandyba, I., Dvoretskyi, M., & Boiko, A. (2021). Principles of searching for a variety of types of associative rules in OLAP-cubes. *CEUR Workshop Proceedings*, 2845, 181-192.

62. Which countries have the worst (and best) cybersecurity? Comparitech. URL: https://www.comparitech.com/blog/vpn-privacy/cybersecurity-by-country/

63. Digital Economy and Society Index. URL: https://digital-agenda-data.eu/datasets/desi/visualizations

64. Кузьменко О.В., Миненко С.В., Доценко Т.В. Кібершахрайства, фінансові правопорушення та легалізація кримінальних доходів в умовах цифровізації економіки України. *Науковий погляд: економіка та управління*. 2021. №3(72). С. 9-21.

65. Кузьменко О.В., Миненко С.В., Доценко Т.В., Шрамко Е.В. Взаємозалежнысть FinTech інновацій, фінансових, кібернетичних злочинів та легалізації кримінальних доходів за посередництва фінансових установ. *Вісник СумДУ*. 2021. № 1. С. 195-207.

66. Belen Suarez Lopez, David Issó García, Antonio Vargas Alcaide. Blockchain Technology Facing Socioeconomic Challenges. Promise versus Probability. *SocioEconomic Challenges*. 2019. № 3(4). P. 13-24. http://doi.org/10.21272/sec.3(4).13-24.2019.

67. Kuzmenko O.V., Yarovenko H.M., Boyko A.O., Mynenko S.V. Розробка бізнес-моделі процесів фінансового моніторингу економічних агентів. *Ефективна економіка*. 2019. № 12. DOI: https://doi.org/10.32702/2307-2105-2019.12.4

68. Araujo Ricardo. Assessing the efficiency of the anti-money laundering regulation: an incentive-based approach. Journal of Money Laundering Control. 2008. № 11. P. 67-75. 10.1108/13685200810844505.

69. Zarutska E., Pavlova T., Sinyuk A. Structural-functional analysis as innovation in public governance (case of banking supervision). *Marketing and Management of Innovations*. 2018. № 4. P. 349-360. http://doi.org/10.21272/mmi.2018.4-30

70. Державна служба фінансового моніторингу: офіційний веб-сайт. URL: https://fiu.gov.ua/pages/dijalnist/funkcional/statistika-ta-infografika (дата звернення 25.03.2021)

71. Генеральна прокуратура України: офіційний веб-сайт. URL: https://www.gp.gov.ua/ua/1stat (дата звернення 25.03.2021)

72. Теслик Н.М. Гончаренко А.Р., Громико Д.В. Психологічні особливості сприйняття кібершахрбайства студентською молоддю. *Вісник Національного університету оборони України*. 2020. Вип. 4. С. 143-149, DOI: 10.33099/2617-6858–21–60–2–143-149

73. Звіт за результатами соціологічного опитування дорослого населення та фокус-групових дискусій. Сайт Програми розвитку ООН в Україні. 18 березня 2021 р. URL: https://www.ua.undp.org/content/ukraine/uk/home/library/democratic_governance/

electronic-services--experiences--trust--accessibility.html (дата звернення 29.09.2021).

74. Газізова Ю. Кіберзлочинність в Україні. Ера цифрових технологій – ера нових злочинів. Юрист&Закон. 2020. №12. URL: https://uz.ligazakon.ua/ua/magazine_article/EA013606 (дата звернення 07.04.2021).

75. Биктагирова Г.Ф., Валеева Р.А., Дроздикова-Зарипова А.Р., Калацкая Н.Н., Костюнина Н.Ю. Профилактика и коррекция виктимного поведения студенческой молодежи в Глобальной сети Интернет: теория, практика. Россия, Казань: Издательство «Отечество», 2019. 320 с. URL: https://kpfu.ru/portal/docs/F_2098151813/monografiya.obedin.pdf (дата звернення 29.09.2021).

76. Кримінологічна віктимологія. Чернєй В.В. та інші. Мультимедійний навчальний посібник. 2021. URL: https://arm.naiau.kiev.ua/books/kryminoloh_viktym/files/t2.pdf (дата звернення 29.09.2021).

77. Kaakinen, M., Keipi, T., Räsänen, P., Oksanen, A. Cybercrime Victimization and Subjective Well-Being: An Examination of the Buffering Effect Hypothesis Among Adolescents and Young Adults. Cyberpsychology, Behavior, and Social Networking. Vol. 21. Issue 2. Feb. 2018. P. 129-137. http://doi.org/10.1089/cyber.2016.0728.

78. Гарькавець С. О. Форми віктимності особистості у ранньому юнацькому віці. *Теоретичні і прикладні проблеми психології*, 2020, №3 (53). Том 1. С. 62-78. DOI: https://doi.org/10.33216/2219-2654-2020-53-3-1-62-78.

79. Кіберполіція розповідає про типові випадки шахрайства під час коронавірусу. Офіційний сайт Департаменту кіберполіції Національної поліції України. 25 березня 2020 р. URL: https://cyberpolice.gov.ua/article/kiberpolicziya--rozpovidaye-pro-typovi-vypadky-shaxrajstva-pid-chas-koronavirusu-1820/ (дата звернення 09.04.2021).

80. Ніколаєнко С., Ніколаєнко С. Категорія психологічного впливу в психології. Світогляд-Філософія-Релігія, 2011. №1 (1). С. 51-61. URL: http://dspace.nbuv.gov.ua/bitstream/handle/123456789/39499/09-Nikolaienko2.pdf?sequence=1 (дата звернення 07.04.2021).

81. Кравченко О. В. Психологічні особливості шахрайства: автореф. дис… канд. психол. наук: спец. 19.00.06 НУВС, 2005. 23 с. URL: http://irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/VKhnuvs_2004_28_90.pdf (дата звернення 07.04.2021).

82. Про основні засади забезпечення кібербезпеки України. Закон України від 5 жовтня 2017 року. № 45. ст.403. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення 07.04.2021).

83. Палчинська М. В. Віртуальний простір в умовах соціокультурних трансформацій: автореф. дис. … докт. філол. наук: 09.00.03. Одеса, 2016. 43 с. URL: http://dspace.pdpu.edu.ua/bitstream/123456789/715/1/ПальчинськаМар'янаВікторівна.aref.pdf (дата звернення 07.04.2021).

84. Дзюбань О. П. Сучасний віртуальний простір: конгеніальність віртуальності й міфи. Стратегічні пріоритети, 2017. №3. С. 163-170. URL: https://dspace.nlu.edu.ua/bitstream/123456789/14077/3/St_Dzeban.pdf (дата звернення 07.04.2021).

85. Прудка Л.М. Психологічні особливості шахрайства в мережі інтернет. Південноукраїнський правничий часопис, 2018. №2. С. 30-33. URL: http://dspace.oduvs.edu.ua/bitstream/123456789/1382/1/Прудка_2_2018.pdf (дата звернення 07.04.2021).

86. Arató N., Zsidó A.N., Lénárd K. and Lábadi B. (2020) Cybervictimization and Cyberbullying: The Role of Socio-Emotional Skills. Front. Psychiatry 11:248. DOI: 10.3389/fpsyt.2020.00248 (дата звернення 07.04.2021).

87. Мацко Л. А. Основи психології та педагогіки. Психологія: лабораторний практикум / Л. А. Мацко, М. Д. Прищак, Т. В. Первушина. Вінниця: ВНТУ, 2011. 139 с.

88. Про затвердження Положення про здійснення контролю за дотриманням банками вимог законодавства з питань інформаційної безпеки, кіберзахисту та електронних довірчих послуг. Постанова НБУ № 4 від 16 січня 2021 року. URL: https://bank.gov.ua/admin_uploads/law/16012021_4.pdf

89. Guidance on cyber resilience for financial market infrastructures, CPMI-IOSCO, 2016. URL: https://www.bis.org/cpmi/publ/d146.pdf

90. Cyber resilience oversight expectations for financial market infrastructures, ECB, 2018). URL: https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf

91. Cyber-resilience: Range of practicesю December 2018. Basel Committee on Banking Supervision. URL: https://www.bis.org/bcbs/publ/d454.pdf

ДОДАТКИ

Додаток А

Проміжні результати тестування на стаціонарність

Null Hypothesis: Unit root (common unit root process)
Series: INT_H
Sample: 2014 2019
Exogenous variables: Individual effects
Automatic selection of maximum lags
Automatic lag length selection based on SIC: 0
Newey-West automatic bandwidth selection and Bartlett kernel
Total (balanced) observations: 115
Cross-sections included: 23

Method	Statistic	Prob.**
Levin, Lin & Chu t*	-14.0791	0.0000

** Probabilities are computed assuming asympotic normality

Intermediate results on INT_H

Cross section	2nd Stage Coefficient	Variance of Reg	HAC of Dep.	Lag	Max Lag	Band-width	Obs
1	-0.25000	0.7600	0.3200	0	0	4.0	5
2	-0.07143	1.8143	0.5547	0	0	2.0	5
3	-0.09302	0.1302	0.0480	0	0	4.0	5
4	-0.12374	0.7975	0.5680	0	0	1.0	5
5	0.07080	0.5947	0.2240	0	0	4.0	5
6	-0.25000	0.1900	0.0800	0	0	4.0	5
7	0.03716	1.0236	0.1920	0	0	4.0	5
8	-0.06763	2.1643	0.6400	0	0	4.0	5
9	-0.55814	2.2884	0.6240	0	0	4.0	5
10	-0.09302	0.1302	0.0480	0	0	4.0	5
11	-0.19014	1.7493	0.6560	0	0	4.0	5
12	0.16279	2.1488	0.8320	0	0	4.0	5
13	-0.78571	1.9829	1.2480	0	0	4.0	5
14	-0.22078	0.2597	0.3040	0	0	4.0	5
15	-0.77451	4.8027	5.4720	0	0	4.0	5
16	0.08471	0.4211	0.2080	0	0	4.0	5
17	-0.83333	2.4933	0.8640	0	0	4.0	5
18	-0.09827	0.5064	0.1920	0	0	4.0	5
19	-0.23016	0.0251	1.3600	0	0	0.0	5
20	0.11850	3.2457	1.7120	0	0	4.0	5
21	-0.37500	0.3350	0.1920	0	0	4.0	5
22	-1.08333	0.3833	2.4000	0	0	2.0	5
23	-0.27029	0.5100	5.8400	0	0	0.0	5
	Coefficient	t-Stat	SE Reg	mu*	sig*		Obs
Pooled	-0.21405	-13.616	1.313	-0.554	0.919		115

Рисунок А.1 –Результати розрахунку тесту Levin, Lin & Chu Unit Root Test для рівня доступу домогосподарств до мережі Інтернет (INT_H)

Продовження додатку А

Null Hypothesis: Unit root (individual unit root process)
Series: INT_H
Sample: 2014 2019
Exogenous variables: Individual effects
Automatic selection of maximum lags
Automatic lag length selection based on SIC: 0
Total (balanced) observations: 115
Cross-sections included: 23

Method		Statistic	Prob.**
Im, Pesaran and Shin W-stat		-0.28284	0.3887
Im, Pesaran and Shin t-bar		-1.65397	
T-bar critical values ***:	1% level	-2.55000	
	5% level	-2.13800	
	10% level	-1.97600	

** Probabilities are computed assuming asympotic normality
*** Critical values from original paper

Intermediate ADF test results

Cross section	t-Stat	Prob.	E(t)	E(Var)	Lag	Max Lag	Obs
1	-0.8885	0.6970	-1.558	2.648	0	0	5
2	-0.2062	0.8737	-1.558	2.648	0	0	5
3	-0.8281	0.7173	-1.558	2.648	0	0	5
4	-0.9552	0.6737	-1.558	2.648	0	0	5
5	0.4781	0.9585	-1.558	2.648	0	0	5
6	-0.8885	0.6970	-1.558	2.648	0	0	5
7	0.2189	0.9355	-1.558	2.648	0	0	5
8	-0.3240	0.8482	-1.558	2.648	0	0	5
9	-1.1853	0.5864	-1.558	2.648	0	0	5
10	-0.8281	0.7173	-1.558	2.648	0	0	5
11	-0.8393	0.7139	-1.558	2.648	0	0	5
12	0.3568	0.9493	-1.558	2.648	0	0	5
13	-2.2870	0.2038	-1.558	2.648	0	0	5
14	-1.8623	0.3201	-1.558	2.648	0	0	5
15	-2.7648	0.1254	-1.558	2.648	0	0	5
16	0.9949	0.9827	-1.558	2.648	0	0	5
17	-1.4161	0.4886	-1.558	2.648	0	0	5
18	-0.8898	0.6966	-1.558	2.648	0	0	5
19	-12.637	0.0002	-1.558	2.648	0	0	5
20	0.4238	0.9547	-1.558	2.648	0	0	5
21	-1.4195	0.4871	-1.558	2.648	0	0	5
22	-4.6950	0.0207	-1.558	2.648	0	0	5
23	-5.5995	0.0100	-1.558	2.648	0	0	5
Average	-1.6540		-1.558	2.648			

Warning: for some series the expected mean and variance for the given lag and observation are not covered in IPS paper

Рисунок А.2 –Результати розрахунку IM, Pesaran and Shin Test для рівня доступу домогосподарств до мережі Інтернет (INT_H)

Продовження додатку А

Null Hypothesis: Unit root (common unit root process)
Series: X2
Sample: 2014 2019
Exogenous variables: Individual effects
Automatic selection of maximum lags
Automatic lag length selection based on SIC: 0
Newey-West automatic bandwidth selection and Bartlett kernel
Total (balanced) observations: 115
Cross-sections included: 23

Method	Statistic	Prob.**
Levin, Lin & Chu t*	-2.69251	0.0035

** Probabilities are computed assuming asympotic normality

Intermediate results on X2

Cross section	2nd Stage Coefficient	Variance of Reg	HAC of Dep.	Lag	Max Lag	Band-width	Obs
1	-1.36969	0.0045	0.0024	0	0	4.0	5
2	0.08551	0.0005	0.0001	0	0	4.0	5
3	-0.01317	0.0003	8.E-05	0	0	3.0	5
4	-0.15425	0.0004	0.0010	0	0	1.0	5
5	-0.36728	0.0006	0.0039	0	0	1.0	5
6	-0.15251	0.0009	0.0003	0	0	4.0	5
7	-0.07273	0.0070	0.0011	0	0	4.0	5
8	-0.10704	0.0004	0.0004	0	0	1.0	5
9	-0.70070	0.0053	0.0017	0	0	4.0	5
10	-0.54438	0.0002	0.0002	0	0	4.0	5
11	-0.28539	0.0007	0.0008	0	0	2.0	5
12	0.03297	0.0018	0.0004	0	0	4.0	5
13	-0.49120	0.0040	0.0016	0	0	4.0	5
14	0.33811	0.0061	0.0082	0	0	2.0	5
15	-0.62319	0.0258	0.0114	0	0	4.0	5
16	-0.01453	0.0013	0.0002	0	0	4.0	5
17	-0.95637	0.0031	0.0017	0	0	4.0	5
18	-0.12314	0.0060	0.0014	0	0	4.0	5
19	-0.59409	0.0024	0.0067	0	0	2.0	5
20	0.15010	0.0007	0.0012	0	0	0.0	5
21	-0.35356	0.0022	0.0036	0	0	3.0	5
22	0.58185	8.E-05	0.0002	0	0	0.0	5
23	0.02112	0.0010	0.0002	0	0	4.0	5
	Coefficient	t-Stat	SE Reg	mu*	sig*		Obs
Pooled	-0.10530	-3.524	1.299	-0.554	0.919		115

Рисунок А.3 –Результати розрахунку тесту Levin, Lin & Chu Unit Root Test для рівня доступу домогосподарств до мережі Інтернет (IP_I)

Продовження додатку А

Null Hypothesis: Unit root (individual unit root process)
Series: X2
Sample: 2014 2019
Exogenous variables: Individual effects
Automatic selection of maximum lags
Automatic lag length selection based on SIC: 0
Total (balanced) observations: 115
Cross-sections included: 23

Method		Statistic	Prob.**
Im, Pesaran and Shin W-stat		2.14886	0.9842
Im, Pesaran and Shin t-bar		-0.82887	
T-bar critical values ***:	1% level	-2.55000	
	5% level	-2.13800	
	10% level	-1.97600	

** Probabilities are computed assuming asympotic normality
*** Critical values from original paper

Intermediate ADF test results

Cross section	t-Stat	Prob.	E(t)	E(Var)	Lag	Max Lag	Obs
1	-2.3777	0.1852	-1.558	2.648	0	0	5
2	0.3283	0.9466	-1.558	2.648	0	0	5
3	-0.0494	0.9002	-1.558	2.648	0	0	5
4	-2.4599	0.1694	-1.558	2.648	0	0	5
5	-3.2518	0.0763	-1.558	2.648	0	0	5
6	-0.6196	0.7756	-1.558	2.648	0	0	5
7	-0.2624	0.8621	-1.558	2.648	0	0	5
8	-1.4880	0.4590	-1.558	2.648	0	0	5
9	-0.9852	0.6629	-1.558	2.648	0	0	5
10	-1.8171	0.3354	-1.558	2.648	0	0	5
11	-1.5314	0.4417	-1.558	2.648	0	0	5
12	0.1017	0.9227	-1.558	2.648	0	0	5
13	-1.4017	0.4945	-1.558	2.648	0	0	5
14	0.6016	0.9672	-1.558	2.648	0	0	5
15	-0.6538	0.7662	-1.558	2.648	0	0	5
16	-0.1440	0.8846	-1.558	2.648	0	0	5
17	-1.7142	0.3714	-1.558	2.648	0	0	5
18	-0.3607	0.8400	-1.558	2.648	0	0	5
19	-3.2669	0.0752	-1.558	2.648	0	0	5
20	1.4436	0.9921	-1.558	2.648	0	0	5
21	-1.9163	0.3023	-1.558	2.648	0	0	5
22	2.4594	0.9981	-1.558	2.648	0	0	5
23	0.3016	0.9440	-1.558	2.648	0	0	5
Average	-0.8289		-1.558	2.648			

Warning: for some series the expected mean and variance for the given lag and observation are not covered in IPS paper

Рисунок А.4 –Результати розрахунку IM, Pesaran and Shin Test для рівня доступу домогосподарств до мережі Інтернет (IP_I)

Продовження додатку А

Null Hypothesis: Unit root (common unit root process)
Series: X3
Sample: 2014 2019
Exogenous variables: Individual effects
Automatic selection of maximum lags
Automatic lag length selection based on SIC: 0
Newey-West automatic bandwidth selection and Bartlett kernel
Total (balanced) observations: 115
Cross-sections included: 23

Method	Statistic	Prob.**
Levin, Lin & Chu t*	-14.9320	0.0000

** Probabilities are computed assuming asympotic normality

Intermediate results on X3

Cross section	2nd Stage Coefficient	Variance of Reg	HAC of Dep.	Lag	Max Lag	Band-width	Obs
1	0.06214	0.0005	0.0002	0	0	4.0	5
2	0.30422	0.0005	0.0006	0	0	0.0	5
3	0.41607	0.0021	0.0019	0	0	1.0	5
4	-3.29754	0.0028	0.0043	0	0	4.0	5
5	-0.92147	0.0020	0.0048	0	0	4.0	5
6	-0.06105	0.0006	0.0001	0	0	4.0	5
7	-0.05613	0.0016	0.0003	0	0	4.0	5
8	0.11758	0.0009	0.0003	0	0	4.0	5
9	-0.48513	0.0004	0.0012	0	0	0.0	5
10	-0.68536	0.0066	0.0026	0	0	4.0	5
11	-0.05491	0.0002	4.E-05	0	0	4.0	5
12	-0.52539	0.0015	0.0008	0	0	2.0	5
13	-1.07439	0.0002	0.0258	0	0	2.0	5
14	0.18548	0.0027	0.0011	0	0	4.0	5
15	-1.61323	0.0012	0.0022	0	0	4.0	5
16	0.06912	0.0003	0.0002	0	0	2.0	5
17	-0.40139	0.0070	0.0086	0	0	2.0	5
18	-0.81313	0.0073	0.0051	0	0	1.0	5
19	-0.75230	0.0017	0.0034	0	0	1.0	5
20	-0.72659	0.0056	0.0046	0	0	4.0	5
21	-0.77922	0.0061	0.0088	0	0	0.0	5
22	-0.62159	0.0010	0.0004	0	0	1.0	5
23	-0.10277	0.0061	0.0013	0	0	4.0	5
	Coefficient	t-Stat	SE Reg	mu*	sig*		Obs
Pooled	-0.76999	-14.875	2.024	-0.554	0.919		115

Рисунок А.5 –Результати розрахунку тесту Levin, Lin & Chu Unit Root Test для рівня електронного урядування (EG_I)

Продовження додатку А

Null Hypothesis: Unit root (individual unit root process)
Series: X3
Sample: 2014 2019
Exogenous variables: Individual effects
Automatic selection of maximum lags
Automatic lag length selection based on SIC: 0
Total (balanced) observations: 115
Cross-sections included: 23

Method		Statistic	Prob.**
Im, Pesaran and Shin W-stat		-1.51229	0.0652
Im, Pesaran and Shin t-bar		-2.07113	
T-bar critical values ***:	1% level	-2.55000	
	5% level	-2.13800	
	10% level	-1.97600	

** Probabilities are computed assuming asympotic normality
*** Critical values from original paper

Intermediate ADF test results

Cross section	t-Stat	Prob.	E(t)	E(Var)	Lag	Max Lag	Obs
1	0.0966	0.9220	-1.558	2.648	0	0	5
2	1.0568	0.9846	-1.558	2.648	0	0	5
3	0.6528	0.9692	-1.558	2.648	0	0	5
4	-2.8562	0.1141	-1.558	2.648	0	0	5
5	-3.9451	0.0398	-1.558	2.648	0	0	5
6	-0.1494	0.8836	-1.558	2.648	0	0	5
7	-0.3332	0.8463	-1.558	2.648	0	0	5
8	0.4606	0.9574	-1.558	2.648	0	0	5
9	-2.6627	0.1386	-1.558	2.648	0	0	5
10	-1.4763	0.4639	-1.558	2.648	0	0	5
11	-0.5165	0.8019	-1.558	2.648	0	0	5
12	-0.5936	0.7823	-1.558	2.648	0	0	5
13	-26.336	0.0000	-1.558	2.648	0	0	5
14	0.2172	0.9354	-1.558	2.648	0	0	5
15	-4.4064	0.0265	-1.558	2.648	0	0	5
16	0.4936	0.9596	-1.558	2.648	0	0	5
17	-0.5801	0.7859	-1.558	2.648	0	0	5
18	-1.2388	0.5638	-1.558	2.648	0	0	5
19	-1.3449	0.5190	-1.558	2.648	0	0	5
20	-1.3083	0.5350	-1.558	2.648	0	0	5
21	-1.1603	0.5970	-1.558	2.648	0	0	5
22	-1.2209	0.5711	-1.558	2.648	0	0	5
23	-0.4852	0.8097	-1.558	2.648	0	0	5
Average	-2.0711		-1.558	2.648			

Warning: for some series the expected mean and variance for the given lag and observation are not covered in IPS paper

Рисунок А.6 –Результати розрахунку IM, Pesaran and Shin Test для для рівня електронного урядування (EG_I)

Продовження додатку А

Null Hypothesis: Unit root (common unit root process)
Series: X5
Sample: 2014 2019
Exogenous variables: Individual effects
Automatic selection of maximum lags
Automatic lag length selection based on SIC: 0
Newey-West automatic bandwidth selection and Bartlett kernel
Total number of observations: 109
Cross-sections included: 22 (1 dropped)

Method	Statistic	Prob.**
Levin, Lin & Chu t*	-13.6501	0.0000

** Probabilities are computed assuming asympotic normality

Intermediate results on X5

Cross section	2nd Stage Coefficient	Variance of Reg	HAC of Dep.	Lag	Max Lag	Band-width	Obs
1	-1.21191	0.0013	0.0018	0	0	4.0	5
2	-0.75006	0.0019	0.0030	0	0	2.0	5
3	-0.69988	0.0018	0.0024	0	0	0.0	5
4	-0.03097	0.0083	0.0019	0	0	4.0	5
5	-1.42259	0.0395	0.0256	0	0	4.0	5
6	-0.06951	0.0050	0.0011	0	0	3.0	4
7	-0.74221	0.0010	0.0021	0	0	4.0	5
8	-1.07838	0.0011	0.0005	0	0	4.0	5
9	-2.69809	0.0017	0.0233	0	0	0.0	5
10	-0.90246	0.0014	0.0011	0	0	4.0	5
11	0.97129	0.0191	0.0296	0	0	0.0	5
12	-0.21508	0.0009	0.0002	0	0	4.0	5
13	-1.70664	0.0101	0.0140	0	0	0.0	5
14	-0.95504	0.0002	0.0040	0	0	2.0	5
15	-1.53493	0.0013	0.0009	0	0	4.0	5
16	-1.72973	0.0021	0.0100	0	0	1.0	5
17	-0.71117	0.0016	0.0085	0	0	1.0	5
18		Dropped from Test					
19	-1.57868	0.0128	0.0262	0	0	3.0	5
20	-1.03109	0.0007	0.0120	0	0	3.0	5
21	-1.21531	0.0029	0.0025	0	0	4.0	5
22	-1.17802	0.0012	0.0007	0	0	4.0	5
23	-0.42890	0.0024	0.0084	0	0	0.0	5

	Coefficient	t-Stat	SE Reg	mu*	sig*	Obs
Pooled	-0.88231	-14.836	1.406	-0.554	0.919	109

Рисунок А.7–Результати розрахунку тесту Levin, Lin & Chu Unit Root Test для частки підприємств, які проводили навчання для розвитку / підвищення кваліфікації інформаційно-комунікативних технологій (TR_E)

Продовження додатку А

Null Hypothesis: Unit root (individual unit root process)
Series: X5
Sample: 2014 2019
Exogenous variables: Individual effects
Automatic selection of maximum lags
Automatic lag length selection based on SIC: 0
Total number of observations: 114
Cross-sections included: 23

Method		Statistic	Prob.**
Im, Pesaran and Shin W-stat		-3.46928	0.0003
Im, Pesaran and Shin t-bar		-2.71648	
T-bar critical values ***:	1% level	2.57024	
	5% level	2.94038	
	10% level	3.12114	

** Probabilities are computed assuming asympotic normality
*** Critical values from original paper

Intermediate ADF test results

Cross section	t-Stat	Prob.	E(t)	E(Var)	Lag	Max Lag	Obs
1	-3.1550	0.0837	-1.558	2.648	0	0	5
2	-1.3417	0.5204	-1.558	2.648	0	0	5
3	-0.9770	0.6659	-1.558	2.648	0	0	5
4	-0.1017	0.8915	-1.558	2.648	0	0	5
5	-0.8408	0.7134	-1.558	2.648	0	0	5
6	-0.1744	0.8580	-1.246	2.118	0	0	4
7	-3.4573	0.0627	-1.558	2.648	0	0	5
8	-1.8736	0.3163	-1.558	2.648	0	0	5
9	-6.1955	0.0065	-1.558	2.648	0	0	5
10	-2.4489	0.1713	-1.558	2.648	0	0	5
11	1.2793	0.9895	-1.558	2.648	0	0	5
12	-0.5265	0.7995	-1.558	2.648	0	0	5
13	-1.0655	0.6326	-1.558	2.648	0	0	5
14	-9.4994	0.0009	-1.558	2.648	0	0	5
15	-3.1466	0.0844	-1.558	2.648	0	0	5
16	-5.9030	0.0081	-1.558	2.648	0	0	5
17	-2.9993	0.0983	-1.558	2.648	0	0	5
18	-1.4639	0.4688	-1.558	2.648	0	0	5
19	-2.4959	0.1634	-1.558	2.648	0	0	5
20	-9.0016	0.0012	-1.558	2.648	0	0	5
21	-2.5018	0.1624	-1.558	2.648	0	0	5
22	-1.8359	0.3290	-1.558	2.648	0	0	5
23	-2.7532	0.1269	-1.558	2.648	0	0	5
Average	-2.7165		-1.544	2.625			

Warning: for some series the expected mean and variance for the given lag and observation are not covered in IPS paper

Рисунок А.8 –Результати розрахунку IM, Pesaran and Shin Test для частки підприємств, які проводили навчання для розвитку / підвищення кваліфікації інформаційно-комунікативних технологій (TR_E)

Продовження додатку А

Null Hypothesis: Unit root (common unit root process)
Series: X4
Sample: 2014 2019
Exogenous variables: Individual effects
Automatic selection of maximum lags
Automatic lag length selection based on SIC: 0
Newey-West automatic bandwidth selection and Bartlett kernel
Total (balanced) observations: 115
Cross-sections included: 23

Method	Statistic	Prob.**
Levin, Lin & Chu t*	-3.83240	0.0001

** Probabilities are computed assuming asympotic normality

Intermediate results on X4

Cross section	2nd Stage Coefficient	Variance of Reg	HAC of Dep.	Lag	Max Lag	Band-width	Obs
1	-0.23594	6.E-05	4.E-05	0	0	4.0	5
2	-0.03255	0.0002	5.E-05	0	0	4.0	5
3	0.04897	0.0001	3.E-05	0	0	4.0	5
4	-0.27537	0.0007	0.0002	0	0	4.0	5
5	-1.57525	0.0024	0.0019	0	0	4.0	5
6	0.10484	0.0004	0.0001	0	0	4.0	5
7	0.15347	0.0004	0.0005	0	0	0.0	5
8	-0.02510	0.0004	7.E-05	0	0	4.0	5
9	-0.12022	4.E-05	8.E-05	0	0	0.0	5
10	-0.28396	0.0004	0.0001	0	0	4.0	5
11	-0.55825	0.0004	0.0024	0	0	0.0	5
12	-0.28440	0.0039	0.0011	0	0	4.0	5
13	-0.32138	0.0013	0.0040	0	0	2.0	5
14	-1.04828	0.0008	0.0003	0	0	4.0	5
15	-0.56003	0.0054	0.0092	0	0	0.0	5
16	-0.33207	0.0021	0.0040	0	0	3.0	5
17	0.09640	0.0023	0.0024	0	0	0.0	5
18	-2.01716	0.0004	0.0011	0	0	2.0	5
19	-0.71898	0.0054	0.0052	0	0	2.0	5
20	-0.38823	0.0014	0.0004	0	0	4.0	5
21	0.65460	0.0040	0.0058	0	0	1.0	5
22	-1.36488	0.0010	0.0006	0	0	3.0	5
23	-0.77002	0.0010	0.0005	0	0	4.0	5
	Coefficient	t-Stat	SE Reg	mu*	sig*		Obs
Pooled	-0.19482	-5.035	1.250	-0.554	0.919		115

Рисунок А.9 –Результати розрахунку тесту Levin, Lin & Chu Unit Root Test для рівня зайнятого населення у сфері інформаційно-комунікативних технологій (EMP)

Продовження додатку А

Null Hypothesis: Unit root (individual unit root process)
Series: X4
Sample: 2014 2019
Exogenous variables: Individual effects
Automatic selection of maximum lags
Automatic lag length selection based on SIC: 0
Total (balanced) observations: 115
Cross-sections included: 23

Method		Statistic	Prob.**
Im, Pesaran and Shin W-stat		1.30455	0.9040
Im, Pesaran and Shin t-bar		-1.11535	
T-bar critical values ***:	1% level	-2.55000	
	5% level	-2.13800	
	10% level	-1.97600	

** Probabilities are computed assuming asympotic normality
*** Critical values from original paper

Intermediate ADF test results

Cross section	t-Stat	Prob.	E(t)	E(Var)	Lag	Max Lag	Obs
1	-1.3164	0.5314	-1.558	2.648	0	0	5
2	-0.2615	0.8623	-1.558	2.648	0	0	5
3	0.2201	0.9357	-1.558	2.648	0	0	5
4	-0.7898	0.7289	-1.558	2.648	0	0	5
5	-2.6535	0.1398	-1.558	2.648	0	0	5
6	0.3120	0.9450	-1.558	2.648	0	0	5
7	0.7034	0.9717	-1.558	2.648	0	0	5
8	-0.1073	0.8906	-1.558	2.648	0	0	5
9	-1.9676	0.2872	-1.558	2.648	0	0	5
10	-0.6019	0.7802	-1.558	2.648	0	0	5
11	-3.7700	0.0466	-1.558	2.648	0	0	5
12	-0.7290	0.7462	-1.558	2.648	0	0	5
13	-2.2691	0.2077	-1.558	2.648	0	0	5
14	-1.7755	0.3507	-1.558	2.648	0	0	5
15	-1.4524	0.4733	-1.558	2.648	0	0	5
16	-2.2364	0.2156	-1.558	2.648	0	0	5
17	0.2063	0.9342	-1.558	2.648	0	0	5
18	-2.8989	0.1092	-1.558	2.648	0	0	5
19	-0.4503	0.8183	-1.558	2.648	0	0	5
20	-0.9172	0.6868	-1.558	2.648	0	0	5
21	0.9248	0.9805	-1.558	2.648	0	0	5
22	-2.3255	0.1957	-1.558	2.648	0	0	5
23	-1.4974	0.4553	-1.558	2.648	0	0	5
Average	-1.1154		-1.558	2.648			

Warning: for some series the expected mean and variance for the given lag and observation are not covered in IPS paper

Рисунок А.10 –Результати розрахунку IM, Pesaran and Shin Test для рівня зайнятого населення у сфері інформаційно-комунікативних технологій (EMP)

Продовження додатку А

Null Hypothesis: Unit root (common unit root process)
Series: Y1
Sample: 2014 2019
Exogenous variables: Individual effects
Automatic selection of maximum lags
Automatic lag length selection based on SIC: 0
Newey-West automatic bandwidth selection and Bartlett kernel
Total (balanced) observations: 115
Cross-sections included: 23

Method	Statistic	Prob.**
Levin, Lin & Chu t*	2.30322	0.9894

** Probabilities are computed assuming asympotic normality

Intermediate results on Y1

Cross section	2nd Stage Coefficient	Variance of Reg	HAC of Dep.	Lag	Max Lag	Band-width	Obs
1	0.56983	4.E-05	0.0001	0	0	0.0	5
2	0.24185	0.0003	0.0002	0	0	2.0	5
3	-0.00726	7.E-05	2.E-05	0	0	4.0	5
4	0.01506	0.0004	8.E-05	0	0	4.0	5
5	-0.51493	0.0029	0.0009	0	0	4.0	5
6	-0.20672	0.0003	0.0003	0	0	0.0	5
7	-0.17013	0.0087	0.0019	0	0	3.0	5
8	0.11004	0.0004	0.0002	0	0	4.0	5
9	-0.64848	0.0005	0.0002	0	0	4.0	5
10	0.03334	0.0008	0.0008	0	0	0.0	5
11	-0.00593	0.0006	0.0001	0	0	1.0	5
12	0.04241	8.E-05	3.E-05	0	0	4.0	5
13	-1.33705	9.E-05	0.0001	0	0	4.0	5
14	0.09313	0.0029	0.0010	0	0	1.0	5
15	-0.72860	0.0110	0.0208	0	0	4.0	5
16	0.09212	0.0035	0.0035	0	0	0.0	5
17	-0.95633	0.0027	0.0010	0	0	4.0	5
18	0.18161	0.0009	0.0012	0	0	0.0	5
19	0.00546	0.0046	0.0011	0	0	4.0	5
20	0.18858	0.0006	0.0010	0	0	0.0	5
21	-0.24320	0.0105	0.0024	0	0	4.0	5
22	0.18063	9.E-06	2.E-05	0	0	1.0	5
23	0.14698	0.0023	0.0035	0	0	2.0	5
	Coefficient	t-Stat	SE Reg	mu*	sig*		Obs
Pooled	0.03396	0.980	1.285	-0.554	0.919		115

Рисунок А.11 –Результати розрахунку тесту Levin, Lin & Chu Unit Root Test для рівня інтернет банкінгу (INR)

Продовження додатку А

Null Hypothesis: Unit root (individual unit root process)
Series: Y1
Sample: 2014 2019
Exogenous variables: Individual effects
Automatic selection of maximum lags
Automatic lag length selection based on SIC: 0
Total (balanced) observations: 115
Cross-sections included: 23

Method		Statistic	Prob.**
Im, Pesaran and Shin W-stat		4.27265	1.0000
Im, Pesaran and Shin t-bar		-0.10825	
T-bar critical values ***:	1% level	-2.55000	
	5% level	-2.13800	
	10% level	-1.97600	

** Probabilities are computed assuming asympotic normality
*** Critical values from original paper

Intermediate ADF test results

Cross section	t-Stat	Prob.	E(t)	E(Var)	Lag	Max Lag	Obs
1	1.9989	0.9966	-1.558	2.648	0	0	5
2	0.8459	0.9778	-1.558	2.648	0	0	5
3	-0.0994	0.8919	-1.558	2.648	0	0	5
4	0.1260	0.9257	-1.558	2.648	0	0	5
5	-0.8251	0.7186	-1.558	2.648	0	0	5
6	-0.6136	0.7772	-1.558	2.648	0	0	5
7	-0.4087	0.8285	-1.558	2.648	0	0	5
8	0.9564	0.9815	-1.558	2.648	0	0	5
9	-1.2255	0.5693	-1.558	2.648	0	0	5
10	0.2033	0.9339	-1.558	2.648	0	0	5
11	-0.0304	0.9030	-1.558	2.648	0	0	5
12	0.3694	0.9504	-1.558	2.648	0	0	5
13	-4.0376	0.0367	-1.558	2.648	0	0	5
14	0.2249	0.9362	-1.558	2.648	0	0	5
15	-3.2418	0.0770	-1.558	2.648	0	0	5
16	0.1740	0.9314	-1.558	2.648	0	0	5
17	-1.7315	0.3653	-1.558	2.648	0	0	5
18	1.0123	0.9834	-1.558	2.648	0	0	5
19	0.0206	0.9109	-1.558	2.648	0	0	5
20	1.2818	0.9895	-1.558	2.648	0	0	5
21	-0.4974	0.8065	-1.558	2.648	0	0	5
22	1.6154	0.9940	-1.558	2.648	0	0	5
23	1.3919	0.9913	-1.558	2.648	0	0	5
Average	-0.1083		-1.558	2.648			

Warning: for some series the expected mean and variance for the given lag and observation are not covered in IPS paper

Рисунок А.12 –Результати розрахунку IM, Pesaran and Shin Test для рівня інтернет банкінгу (INR)

Продовження додатку А

Null Hypothesis: Unit root (common unit root process)
Series: Y2
Sample: 2014 2019
Exogenous variables: Individual effects
Automatic selection of maximum lags
Automatic lag length selection based on SIC: 0
Newey-West automatic bandwidth selection and Bartlett kernel
Total (balanced) observations: 115
Cross-sections included: 23

Method	Statistic	Prob.**
Levin, Lin & Chu t*	-28.9839	0.0000

** Probabilities are computed assuming asympotic normality

Intermediate results on Y2

Cross section	2nd Stage Coefficient	Variance of Reg	HAC of Dep.	Lag	Max Lag	Band-width	Obs
1	-0.40531	0.0030	0.0292	0	0	0.0	5
2	-0.77660	0.0748	0.3442	0	0	0.0	5
3	-0.09096	0.0037	0.0006	0	0	4.0	5
4	-0.65083	0.0101	0.2420	0	0	0.0	5
5	-0.60387	0.0138	0.1604	0	0	0.0	5
6	-0.42227	0.0138	0.0096	0	0	4.0	5
7	-0.53025	0.0393	0.2077	0	0	1.0	5
8	-0.63404	0.0373	0.1354	0	0	0.0	5
9	-0.51763	0.0007	0.0990	0	0	0.0	5
10	0.05507	0.0203	0.0045	0	0	4.0	5
11	-0.64797	0.0035	0.0807	0	0	0.0	5
12	-0.60228	0.0213	0.0846	0	0	0.0	5
13	-0.38619	0.0293	0.0687	0	0	0.0	5
14	-0.18577	0.1334	0.0481	0	0	1.0	5
15	-0.89679	0.0817	0.2923	0	0	0.0	5
16	-0.18329	0.1695	0.0417	0	0	4.0	5
17	-0.78551	0.0290	0.1009	0	0	0.0	5
18	-0.83703	0.0820	0.3240	0	0	2.0	5
19	-0.48490	0.0412	0.0360	0	0	3.0	5
20	-0.18577	0.1334	0.0481	0	0	1.0	5
21	-0.19011	0.0621	0.0683	0	0	0.0	5
22	-0.33088	0.0177	0.0532	0	0	0.0	5
23	-0.20403	0.0581	0.0105	0	0	3.0	5
	Coefficient	t-Stat	SE Reg	mu*	sig*		Obs
Pooled	-0.51963	-28.452	1.200	-0.554	0.919		115

Рисунок А.13 –Результати розрахунку тесту Levin, Lin & Chu Unit Root Test для рівня використання фінансових послуг онлайн (FIN)

Продовження додатку А

Null Hypothesis: Unit root (individual unit root process)
Series: Y2
Sample: 2014 2019
Exogenous variables: Individual effects
Automatic selection of maximum lags
Automatic lag length selection based on SIC: 0
Total (balanced) observations: 115
Cross-sections included: 23

Method		Statistic	Prob.**
Im, Pesaran and Shin W-stat		-5.78314	0.0000
Im, Pesaran and Shin t-bar		-3.52027	
T-bar critical values ***:	1% level	-2.55000	
	5% level	-2.13800	
	10% level	-1.97600	

** Probabilities are computed assuming asympotic normality
*** Critical values from original paper

Intermediate ADF test results

Cross section	t-Stat	Prob.	E(t)	E(Var)	Lag	Max Lag	Obs
1	-5.1081	0.0148	-1.558	2.648	0	0	5
2	-3.2873	0.0738	-1.558	2.648	0	0	5
3	-0.4168	0.8265	-1.558	2.648	0	0	5
4	-8.2923	0.0018	-1.558	2.648	0	0	5
5	-5.6501	0.0097	-1.558	2.648	0	0	5
6	-1.8408	0.3271	-1.558	2.648	0	0	5
7	-3.0419	0.0939	-1.558	2.648	0	0	5
8	-2.8111	0.1196	-1.558	2.648	0	0	5
9	-21.280	0.0000	-1.558	2.648	0	0	5
10	0.1912	0.9326	-1.558	2.648	0	0	5
11	-8.0985	0.0020	-1.558	2.648	0	0	5
12	-2.9891	0.0993	-1.558	2.648	0	0	5
13	-2.0045	0.2761	-1.558	2.648	0	0	5
14	-0.7497	0.7405	-1.558	2.648	0	0	5
15	-2.7811	0.1234	-1.558	2.648	0	0	5
16	-0.3794	0.8356	-1.558	2.648	0	0	5
17	-2.7271	0.1301	-1.558	2.648	0	0	5
18	-3.8293	0.0441	-1.558	2.648	0	0	5
19	-1.5189	0.4465	-1.558	2.648	0	0	5
20	-0.7497	0.7405	-1.558	2.648	0	0	5
21	-0.5490	0.7938	-1.558	2.648	0	0	5
22	-2.4561	0.1701	-1.558	2.648	0	0	5
23	-0.5969	0.7815	-1.558	2.648	0	0	5
Average	-3.5203		-1.558	2.648			

Warning: for some series the expected mean and variance for the given lag and observation are not covered in IPS paper

Рисунок А.14 –Результати розрахунку IM, Pesaran and Shin Test для рівня використання фінансових послуг онлайн (FIN)

Продовження додатку А

Null Hypothesis: Unit root (common unit root process)
Series: Y3
Sample: 2014 2019
Exogenous variables: Individual effects
Automatic selection of maximum lags
Automatic lag length selection based on SIC: 0
Newey-West automatic bandwidth selection and Bartlett kernel
Total (balanced) observations: 115
Cross-sections included: 23

Method	Statistic	Prob.**
Levin, Lin & Chu t*	1.49475	0.9325

** Probabilities are computed assuming asympotic normality

Intermediate results on Y3

Cross section	2nd Stage Coefficient	Variance of Reg	HAC of Dep.	Lag	Max Lag	Band-width	Obs
1	-0.00167	0.0059	0.0015	0	0	3.0	5
2	0.08465	8.E-05	4.E-05	0	0	4.0	5
3	-0.02420	0.0022	0.0005	0	0	4.0	5
4	0.14637	0.0004	0.0006	0	0	1.0	5
5	0.84138	0.0103	0.0174	0	0	2.0	5
6	0.22449	0.0014	0.0009	0	0	4.0	5
7	-0.47878	0.0004	0.0003	0	0	1.0	5
8	0.16698	0.0004	0.0003	0	0	4.0	5
9	-0.43095	0.0026	0.0053	0	0	1.0	5
10	-0.33769	0.0020	0.0034	0	0	0.0	5
11	-0.34661	0.0002	0.0011	0	0	0.0	5
12	0.18021	4.E-05	0.0002	0	0	0.0	5
13	-0.18285	0.0004	0.0003	0	0	4.0	5
14	-0.48881	0.0004	0.0002	0	0	4.0	5
15	0.41602	0.0003	0.0006	0	0	0.0	5
16	0.03396	0.0037	0.0010	0	0	4.0	5
17	0.17809	0.0004	0.0004	0	0	1.0	5
18	-5.12299	0.0203	0.0405	0	0	1.0	5
19	-1.38699	0.0023	0.0102	0	0	4.0	5
20	-0.05096	0.0003	6.E-05	0	0	4.0	5
21	0.22801	0.0005	0.0007	0	0	2.0	5
22	-0.17542	0.0028	0.0014	0	0	4.0	5
23	0.00852	0.0001	2.E-05	0	0	4.0	5
	Coefficient	t-Stat	SE Reg	mu*	sig*		Obs
Pooled	0.01174	0.315	1.554	-0.554	0.919		115

Рисунок А.15 –Результати розрахунку тесту Levin, Lin & Chu Unit Root Test для кількості відділень банків (СВВ)

Продовження додатку А

Null Hypothesis: Unit root (individual unit root process)
Series: Y3
Sample: 2014 2019
Exogenous variables: Individual effects
Automatic selection of maximum lags
Automatic lag length selection based on SIC: 0
Total (balanced) observations: 115
Cross-sections included: 23

Method		Statistic	Prob.**
Im, Pesaran and Shin W-stat		3.53027	0.9998
Im, Pesaran and Shin t-bar		-0.36015	
T-bar critical values ***:	1% level	-2.55000	
	5% level	-2.13800	
	10% level	-1.97600	

** Probabilities are computed assuming asympotic normality
*** Critical values from original paper

Intermediate ADF test results

Cross section	t-Stat	Prob.	E(t)	E(Var)	Lag	Max Lag	Obs
1	-0.0088	0.9063	-1.558	2.648	0	0	5
2	0.5132	0.9610	-1.558	2.648	0	0	5
3	-0.0833	0.8944	-1.558	2.648	0	0	5
4	1.0548	0.9845	-1.558	2.648	0	0	5
5	1.5366	0.9931	-1.558	2.648	0	0	5
6	1.1340	0.9865	-1.558	2.648	0	0	5
7	-1.6648	0.3905	-1.558	2.648	0	0	5
8	1.1922	0.9877	-1.558	2.648	0	0	5
9	-1.8173	0.3354	-1.558	2.648	0	0	5
10	-1.4400	0.4785	-1.558	2.648	0	0	5
11	-3.3344	0.0704	-1.558	2.648	0	0	5
12	3.7219	0.9996	-1.558	2.648	0	0	5
13	-1.3066	0.5357	-1.558	2.648	0	0	5
14	-1.1417	0.6048	-1.558	2.648	0	0	5
15	1.7335	0.9950	-1.558	2.648	0	0	5
16	0.1099	0.9239	-1.558	2.648	0	0	5
17	0.8020	0.9760	-1.558	2.648	0	0	5
18	-1.8642	0.3195	-1.558	2.648	0	0	5
19	-6.8196	0.0044	-1.558	2.648	0	0	5
20	-0.2444	0.8662	-1.558	2.648	0	0	5
21	0.6523	0.9692	-1.558	2.648	0	0	5
22	-1.0799	0.6274	-1.558	2.648	0	0	5
23	0.0711	0.9186	-1.558	2.648	0	0	5
Average	-0.3601		-1.558	2.648			

Warning: for some series the expected mean and variance for the given lag and observation are not covered in IPS paper

Рисунок А.16 –Результати розрахунку IM, Pesaran and Shin Test для кількості відділень банків (СВВ)

Додаток Б

Таблиця Б.1 – Вхідна інформаційна база для побудови панельної регресії

ID	Country name	Year	INT_H	IP_I	EG_I	EMP	TR_E	INR	FIN
1	Finland	2014	90,0	53,0	80,0	6,3	40,0	86,0	5,0
1	Finland	2015	90,0	49,0	79,0	6,4	37,0	86,0	8,0
1	Finland	2016	92,0	48,0	82,0	6,6	34,0	86,0	12,0
1	Finland	2017	94,0	58,0	83,0	6,7	38,0	87,0	13,0
1	Finland	2018	94,0	51,0	83,0	6,7	36,0	89,0	15,0
1	Finland	2019	94,0	55,0	87,0	6,8	37,0	91,0	16,0
2	France	2014	83,0	49,0	64,0	3,2	21,0	58,0	0,5
2	France	2015	83,0	49,0	63,0	3,4	21,0	58,0	1,3
2	France	2016	86,0	52,0	66,0	3,6	20,0	59,0	3,0
2	France	2017	86,0	54,0	68,0	3,8	19,0	62,0	2,0
2	France	2018	89,0	55,0	71,0	3,9	19,0	63,0	3,0
2	France	2019	90,0	58,0	75,0	4,2	21,0	66,0	2,0
3	Germany	2014	89,0	61,0	53,0	3,6	31,0	49,0	4,4
3	Germany	2015	90,0	64,0	55,0	3,7	30,0	51,0	5,0
3	Germany	2016	92,0	64,0	53,0	3,7	29,0	53,0	6,0
3	Germany	2017	93,0	66,0	57,0	3,8	28,0	56,0	6,0
3	Germany	2018	94,0	68,0	59,0	3,9	30,0	59,0	7,0
3	Germany	2019	95,0	71,0	66,0	4,0	32,0	61,0	8,0
4	Italy	2014	73,0	15,0	24,0	3,2	10,0	26,0	0,3
4	Italy	2015	75,0	18,0	24,0	3,2	12,0	28,0	1,0
4	Italy	2016	79,0	20,0	25,0	3,3	12,0	29,0	2,0
4	Italy	2017	81,0	23,0	24,0	3,4	13,0	31,0	2,0
4	Italy	2018	84,0	26,0	23,0	3,6	17,0	34,0	2,0
4	Italy	2019	85,0	28,0	29,0	3,5	19,0	36,0	2,0
5	Latvia	2014	73,0	24,0	52,0	2,5	11,0	57,0	0,2
5	Latvia	2015	76,0	27,0	69,0	2,8	12,0	64,0	0,5
5	Latvia	2016	77,0	31,0	69,0	2,8	12,0	62,0	1,0
5	Latvia	2017	79,0	33,0	66,0	2,8	10,0	61,0	0,0
5	Latvia	2018	82,0	33,0	70,0	2,6	11,0	66,0	1,0
5	Latvia	2019	85,0	34,0	76,0	3,1	18,0	72,0	1,0
6	Netherlands	2014	96,0	59,0	75,0	4,8	18,0	83,0	4,0
6	Netherlands	2015	96,0	59,0	76,0	5,0	18,0	85,0	6,0
6	Netherlands	2016	97,0	63,0	79,0	5,1	22,0	85,0	7,0
6	Netherlands	2017	98,0	68,0	82,0	5,1	24,0	89,0	7,0
6	Netherlands	2018	98,0	70,0	81,0	5,3	26,0	89,0	10,0
6	Netherlands	2019	98,0	70,0	86,0	5,6	:	91,0	10,0
7	Poland	2014	75,0	24,0	27,0	2,6	10,0	33,0	0,2
7	Poland	2015	76,0	24,0	30,0	2,6	12,0	31,0	0,4
7	Poland	2016	80,0	31,0	31,0	2,7	12,0	39,0	1,0
7	Poland	2017	82,0	33,0	35,0	2,8	12,0	40,0	1,0

Продовження таблиці Б.1

ID	Country name	Year	INT_H	IP_I	EG_I	EMP	TR_E	INR	FIN
7	Poland	2018	84,0	37,0	40,0	3,0	13,0	44,0	1,0
7	Poland	2019	87,0	41,0	42,0	3,1	13,0	47,0	1,0
8	Spain	2014	74,0	28,0	49,0	3,1	22,0	37,0	0,7
8	Spain	2015	79,0	32,0	50,0	3,1	22,0	39,0	1,3
8	Spain	2016	82,0	35,0	52,0	3,3	23,0	43,0	2,0
8	Spain	2017	83,0	40,0	57,0	3,4	23,0	46,0	2,0
8	Spain	2018	86,0	43,0	58,0	3,5	21,0	49,0	3,0
8	Spain	2019	91,0	47,0	63,0	3,6	22,0	55,0	2,0
9	Sweden	2014	90,0	62,0	73,0	5,8	27,0	82,0	5,0
9	Sweden	2015	91,0	56,0	78,0	6,1	26,0	80,0	12,0
9	Sweden	2016	94,0	63,0	84,0	6,3	25,0	83,0	19,0
9	Sweden	2017	95,0	67,0	83,0	6,6	28,0	86,0	24,0
9	Sweden	2018	93,0	64,0	86,0	6,8	24,0	84,0	26,0
9	Sweden	2019	96,0	70,0	86,0	7,0	32,0	84,0	26,0
10	UK	2014	90,0	72,0	49,0	5,0	24,0	57,0	4,0
10	UK	2015	91,0	75,0	53,0	5,2	27,0	58,0	4,0
10	UK	2016	93,0	78,0	49,0	5,3	28,0	64,0	6,0
10	UK	2017	94,0	78,0	59,0	5,2	26,0	68,0	7,0
10	UK	2018	95,0	77,0	63,0	5,4	28,0	74,0	8,0
10	UK	2019	96,0	80,0	57,0	5,6	29,0	78,0	11,0
11	Austria	2014	81,0	43,0	57,0	3,6	34,0	48,0	1,0
11	Austria	2015	82,0	46,0	60,0	4,0	33,0	51,0	2,0
11	Austria	2016	85,0	48,0	62,0	4,2	37,0	53,0	3,0
11	Austria	2017	89,0	53,0	66,0	4,4	31,0	57,0	3,0
11	Austria	2018	89,0	53,0	70,0	4,5	27,0	58,0	3,0
11	Austria	2019	90,0	54,0	72,0	4,3	18,0	63,0	3,0
12	Belgium	2014	83,0	41,0	55,0	4,2	33,0	61,0	1,2
12	Belgium	2015	82,0	42,0	52,0	4,2	32,0	62,0	2,0
12	Belgium	2016	85,0	46,0	55,0	4,2	34,0	64,0	3,0
12	Belgium	2017	86,0	49,0	55,0	4,9	35,0	67,0	4,0
12	Belgium	2018	87,0	49,0	56,0	5,2	36,0	69,0	3,0
12	Belgium	2019	90,0	55,0	59,0	5,0	36,0	71,0	3,0
13	Estonia	2014	83,0	37,0	51,0	3,9	14,0	77,0	1,0
13	Estonia	2015	88,0	46,0	81,0	4,4	14,0	81,0	1,5
13	Estonia	2016	86,0	45,0	77,0	5,3	13,0	79,0	3,0
13	Estonia	2017	88,0	46,0	78,0	5,6	13,0	79,0	3,0
13	Estonia	2018	90,0	51,0	79,0	5,7	13,0	80,0	4,0
13	Estonia	2019	90,0	56,0	80,0	6,0	17,0	81,0	4,0
14	Ireland	2014	82,0	43,0	51,0	4,8	25,0	48,0	0,2
14	Ireland	2015	85,0	44,0	50,0	4,6	30,0	51,0	0,3
14	Ireland	2016	87,0	41,0	52,0	4,9	30,0	52,0	1,0

Продовження таблиці Б.1

ID	Country name	Year	INT_H	IP_I	EG_I	EMP	TR_E	INR	FIN
14	Ireland	2017	88,0	44,0	55,0	5,0	30,0	58,0	1,0
14	Ireland	2018	89,0	52,0	54,0	4,8	30,0	58,0	2,0
14	Ireland	2019	91,0	59,0	61,0	4,9	31,0	67,0	3,0
15	Croatia	2014	68,0	22,0	32,0	2,7	23,0	19,0	0,4
15	Croatia	2015	77,0	26,0	35,0	2,7	25,0	33,0	0,9
15	Croatia	2016	77,0	25,0	36,0	3,3	22,0	38,0	1,0
15	Croatia	2017	76,0	21,0	32,0	3,3	23,0	33,0	2,0
15	Croatia	2018	82,0	27,0	36,0	3,5	24,0	41,0	1,0
15	Croatia	2019	81,0	35,0	33,0	3,2	23,0	46,0	1,0
16	Lithuania	2014	66,0	19,0	41,0	1,7	9,0	54,0	0,3
16	Lithuania	2015	68,0	22,0	44,0	2,1	11,0	50,0	0,5
16	Lithuania	2016	72,0	24,0	45,0	2,5	10,0	54,0	1,0
16	Lithuania	2017	75,0	29,0	48,0	2,7	11,0	56,0	1,0
16	Lithuania	2018	78,0	34,0	51,0	2,7	9,0	61,0	1,0
16	Lithuania	2019	82,0	38,0	55,0	3,1	11,0	65,0	3,0
17	Luxembourg	2014	96,0	62,0	67,0	5,1	22,0	67,0	3,0
17	Luxembourg	2015	97,0	63,0	70,0	5,0	25,0	65,0	5,0
17	Luxembourg	2016	97,0	69,0	76,0	5,1	29,0	71,0	8,0
17	Luxembourg	2017	97,0	69,0	75,0	5,2	28,0	76,0	7,0
17	Luxembourg	2018	93,0	60,0	63,0	5,9	27,0	68,0	6,0
17	Luxembourg	2019	95,0	63,0	60,0	6,1	27,0	71,0	5,0
18	Hungary	2014	73,0	20,0	49,0	3,5	16,0	31,0	0,2
18	Hungary	2015	76,0	23,0	42,0	3,6	16,0	34,0	0,8
18	Hungary	2016	79,0	27,0	48,0	3,6	16,0	35,0	1,0
18	Hungary	2017	82,0	26,0	47,0	3,6	17,0	38,0	1,0
18	Hungary	2018	83,0	29,0	53,0	3,7	17,0	41,0	2,0
18	Hungary	2019	86,0	35,0	53,0	3,4	16,0	47,0	1,0
19	Portugal	2014	65,0	17,0	41,0	3,1	26,0	25,0	0,9
19	Portugal	2015	70,0	23,0	43,0	3,0	22,0	28,0	1,0
19	Portugal	2016	74,0	23,0	45,0	3,1	23,0	29,0	2,0
19	Portugal	2017	77,0	25,0	46,0	2,9	21,0	31,0	2,0
19	Portugal	2018	79,0	27,0	42,0	3,1	19,0	39,0	2,0
19	Portugal	2019	81,0	28,0	41,0	3,6	28,0	42,0	2,0
20	Slovenia	2014	77,0	26,0	53,0	3,5	20,0	32,0	0,2
20	Slovenia	2015	78,0	28,0	45,0	3,6	28,0	34,0	0,3
20	Slovenia	2016	78,0	30,0	45,0	3,5	27,0	35,0	1,0
20	Slovenia	2017	82,0	35,0	50,0	3,8	27,0	39,0	1,0
20	Slovenia	2018	87,0	39,0	54,0	4,0	29,0	42,0	2,0
20	Slovenia	2019	89,0	45,0	53,0	3,9	28,0	47,0	3,0
21	Slovakia	2014	78,0	31,0	57,0	2,8	17,0	41,0	0,6
21	Slovakia	2015	79,0	35,0	51,0	2,8	19,0	37,0	0,7

Продовження таблиці Б.1

ID	Country name	Year	INT_H	IP_I	EG_I	EMP	TR_E	INR	FIN
21	Slovakia	2016	81,0	41,0	48,0	2,9	20,0	45,0	1,0
21	Slovakia	2017	81,0	46,0	47,0	2,8	17,0	51,0	1,0
21	Slovakia	2018	81,0	44,0	51,0	3,2	18,0	50,0	2,0
21	Slovakia	2019	82,0	47,0	59,0	3,7	18,0	55,0	2,0
22	Norway	2014	93,0	60,0	82,0	4,5	41,0	89,0	3,0
22	Norway	2015	97,0	61,0	81,0	4,5	44,0	90,0	5,0
22	Norway	2016	97,0	61,0	85,0	4,2	42,0	91,0	10,0
22	Norway	2017	97,0	62,0	84,0	4,6	40,0	92,0	11,0
22	Norway	2018	96,0	64,0	90,0	4,5	42,0	93,0	14,0
22	Norway	2019	98,0	67,0	87,0	4,6	44,0	95,0	16,0
23	Turkey	2014	60,0	9,0	27,0	1,1	9,0	14,0	0,6
23	Turkey	2015	70,0	11,0	28,0	1,2	11,0	15,0	0,7
23	Turkey	2016	76,0	13,0	37,0	1,2	12,0	18,0	1,0
23	Turkey	2017	81,0	15,0	42,0	1,2	14,0	23,0	1,0
23	Turkey	2018	84,0	19,0	46,0	1,2	15,0	28,0	2,0
23	Turkey	2019	88,0	23,0	51,0	1,3	14,0	35,0	2,0

Додаток В

Таблиця В.1 – Статистична база характеристики детермінант поширення кіберзагроз станом на 2020 рік

		I1	I2	I3	I4	I5	I6	I7	I8	I9	I10	I11	I12	I13	I14	I15
Австрія	AUS	1,82	0,02	0	0,2	0,06	2,87	5,51	1,39	0,05	0,15	0,16	0,38	0,62	10,17	22321
Бельгія	BEL	2,85	0,02	0,01	0,2	0,05	4,39	5,85	1,98	0,08	0,2	0,13	0,25	0,28	16,4	49342
Болгарія	BGR	3,5	0,03	0,01	0,5	0,16	4,83	15,43	0,66	0,24	0,56	0,17	0,5	0,38	11,35	301
Хорватія	HRV	2,54	0,02	0,01	0,3	0,08	3,89	7,39	1,04	0,1	0,36	0,13	1,3	0,37	9,15	8418
Данія	DNK	1,33	0	0	0,1	0,02	1,33	2,83	1,42	0,02	0,11	0,07	0,07	0,06	3,26	9208
Фінляндія	FIN	1,06	0,02	0,01	0,3	0,06	2,73	5,77	0,39	0,02	0,36	0,09	0,23	0,01	7,14	1994
Франція	FRA	2,56	0,01	0	0,2	0,08	6,71	6,45	2,53	0,46	0,16	4,03	5,97	1,12	17,9	30485
Німеччина	DEU	1,63	0,02	0,01	0,3	0,06	3,54	4,94	1,8	0,66	0,12	4,67	10,97	7,28	9,68	314459
Греція	GRC	2,75	0,01	0	0,5	0,14	5,39	13,27	1,4	2,52	0,49	0,19	0,21	1,75	16	10677
Угорщина	HUN	3,34	0	0	0,2	0,12	4,33	12,7	1,83	0,3	0,42	0,35	0,83	0,34	15,1	2546
Ірландія	IRL	2,12	0	0,01	0,1	0,04	1,35	3,49	1,63	0,04	0,19	0,33	0,25	0,06	3,42	22331
Італія	ITA	3,26	0,31	0,02	0,5	0,12	4,38	10,74	2,32	1,56	0,22	1,35	1,02	5,45	15,45	578779
Латвія	LVA	3,36	0,02	0	0,3	0,16	7,31	13,95	0,61	0,1	0,73	0,06	0,91	0,3	12,86	78
Нідердланди	NLD	1,66	0,02	0,01	0,2	0,05	1,66	4,24	1,1	0,28	0,19	1,86	4	0,26	4,84	15537
Польща	POL	2,79	0,09	0,01	0,3	0,09	3,69	7,54	1,48	0,61	0,37	0,48	2,05	0,65	12,7	5976
Португалія	PRT	3,38	0,01	0,01	0,9	0,12	5,34	11,5	2,2	0,1	0,44	0,17	0,35	1,88	19,73	2299
Румунія	ROU	5,04	0,02	0,02	0,4	0,04	5,3	14,4	1,32	0,58	0,14	0,29	0,49	0,98	5,76	2812
Словаччина	SVK	3,5	0,03	0,01	0,3	0,11	3,43	8,24	1,24	0,09	0,5	0,04	0,19	0,09	12,94	450
Іспанія	ESP	4,31	0,22	0,01	0,3	0,09	5,92	11,63	2,27	0,7	0,36	0,72	2,66	8,48	13,49	1825476
Швеція	SWE	1,78	0,01	0,01	0,2	0,03	1,435	3,34	1,54	0,28	0,18	0,38	0,19	0,05	3,35	3337
Великобританія	GBR	2,26	0,03	0,01	0,2	0,05	2,71	4,77	1,65	0,89	0,2	1,69	1,04	1,07	9,75	11228

Таблиця В.2 – Індикатори, що характеризують рівень кібервразливості споживачів фінансових послуг

	R1	R2	R3	R4	R5	R6	R7	R8	R9	R10	R11	R12	R13	R14	R15	R16	R17
BE	46%	46%	27%	9%	27%	14%	43%	28%	50%	49%	7%	29%	17%	27%	1%	54%	29%
BG	32%	52%	15%	11%	25%	9%	32%	17%	36%	32%	2%	22%	7%	12%	7%	66%	19%
CZ	36%	37%	27%	7%	26%	6%	31%	23%	43%	34%	5%	24%	7%	19%	2%	54%	24%
DK	27%	39%	25%	2%	41%	19%	34%	41%	59%	58%	9%	27%	25%	31%	6%	19%	14%
D-W	42%	57%	35%	3%	50%	17%	25%	43%	51%	59%	18%	36%	17%	31%	2%	41%	22%
DE	41%	57%	36%	4%	48%	17%	26%	42%	50%	57%	17%	34%	16%	30%	4%	42%	20%
D-E	39%	55%	41%	6%	39%	14%	32%	36%	45%	49%	15%	24%	9%	26%	10%	50%	15%
EE	25%	33%	34%	3%	33%	16%	41%	32%	64%	50%	12%	27%	18%	23%	6%	42%	24%
IE	52%	53%	36%	11%	28%	18%	35%	30%	38%	35%	9%	25%	14%	26%	2%	39%	28%
EL	44%	57%	23%	22%	40%	9%	46%	15%	47%	56%	4%	16%	4%	17%	4%	57%	40%
ES	49%	53%	20%	8%	19%	7%	26%	21%	33%	29%	5%	17%	8%	22%	9%	55%	14%
FR	43%	49%	31%	7%	24%	14%	42%	29%	50%	45%	8%	35%	13%	29%	4%	46%	17%
HR	40%	49%	13%	9%	24%	8%	22%	15%	27%	30%	14%	14%	5%	15%	1%	60%	30%
IT	41%	40%	23%	8%	18%	8%	27%	18%	31%	29%	4%	15%	8%	12%	2%	67%	22%
CY	43%	60%	22%	16%	39%	6%	44%	22%	47%	33%	6%	17%	5%	17%	7%	50%	24%
LV	29%	38%	49%	2%	23%	8%	35%	27%	43%	34%	8%	18%	12%	15%	10%	50%	24%
LT	36%	44%	39%	12%	42%	5%	37%	17%	45%	57%	6%	20%	10%	16%	4%	42%	17%
LU	42%	44%	34%	9%	26%	17%	35%	31%	55%	51%	9%	37%	22%	28%	3%	37%	30%
HU	35%	31%	18%	12%	20%	9%	20%	13%	25%	33%	9%	17%	8%	13%	1%	59%	23%
MT	31%	45%	26%	4%	19%	11%	44%	34%	45%	45%	3%	29%	10%	22%	4%	32%	44%
NL	44%	48%	39%	5%	59%	22%	45%	56%	64%	60%	7%	42%	31%	46%	3%	27%	31%
AT	27%	34%	41%	12%	32%	20%	25%	28%	42%	54%	14%	30%	20%	23%	6%	46%	34%
PL	24%	32%	31%	6%	25%	8%	27%	19%	35%	33%	6%	17%	10%	17%	1%	43%	20%
PT	32%	54%	15%	11%	33%	10%	34%	20%	43%	35%	2%	15%	4%	15%	13%	57%	18%
RO	40%	34%	10%	13%	13%	6%	13%	14%	23%	28%	5%	18%	7%	13%	4%	67%	14%
SI	43%	47%	22%	9%	28%	11%	33%	23%	46%	42%	5%	20%	5%	20%	7%	56%	25%
SK	37%	31%	24%	3%	16%	6%	29%	15%	35%	45%	3%	17%	5%	18%	2%	54%	23%
FI	39%	43%	28%	2%	42%	28%	36%	46%	59%	53%	10%	37%	22%	22%	5%	31%	34%
SE	42%	43%	26%	6%	55%	30%	37%	51%	60%	52%	30%	40%	34%	37%	2%	28%	18%
UK	46%	44%	42%	10%	29%	19%	35%	34%	40%	36%	6%	27%	16%	21%	3%	29%	32%

Таблиця В.3 - Асоціативні правила причинно-наслідковості зв’язків між індикаторами кібервразливості споживачів фінансових послуг

Body	==>	Head	Support, %	Confidence, %
0,053493<AEP1<=0,087964	==>	0,036834<HS1<=0,053611	20,00000	55,5556
0,036834<HS1<=0,053611	==>	0,053493<AEP1<=0,087964	20,00000	71,4286
0,056192<MS2<=0,071812	==>	0,053493<AEP1<=0,087964	20,00000	83,3333
0,053493<AEP1<=0,087964	==>	0,056192<MS2<=0,071812	20,00000	55,5556
0,019518<HC3<=0,040831	==>	0,053493<AEP1<=0,087964	20,00000	55,5556
0,053493<AEP1<=0,087964	==>	0,019518<HC3<=0,040831	20,00000	55,5556
0,019420<G2<=0,039332	==>	0,053493<AEP1<=0,087964	20,00000	62,5000
0,053493<AEP1<=0,087964	==>	0,019420<G2<=0,039332	20,00000	55,5556
0,023606<DPB2<=0,051124	==>	0,019420<G2<=0,039332	24,00000	75,0000
0,019420<G2<=0,039332	==>	0,023606<DPB2<=0,051124	24,00000	75,0000
0,023606<DPB2<=0,051124	==>	0,019420<G2<=0,039332, 0,019518<HC3<=0,040831	20,00000	62,5000
0,019518<HC3<=0,040831	==>	0,019420<G2<=0,039332, 0,023606<DPB2<=0,051124	20,00000	55,5556
0,019518<HC3<=0,040831, 0,023606<DPB2<=0,051124	==>	0,019420<G2<=0,039332	20,00000	83,3333
0,019420<G2<=0,039332	==>	0,019518<HC3<=0,040831, 0,023606<DPB2<=0,051124	20,00000	62,5000
0,019420<G2<=0,039332, 0,023606<DPB2<=0,051124	==>	0,019518<HC3<=0,040831	20,00000	83,3333
0,019420<G2<=0,039332, 0,019518<HC3<=0,040831	==>	0,023606<DPB2<=0,051124	20,00000	71,4286
0,023606<DPB2<=0,051124	==>	0,019420<G2<=0,039332, 0,023642<HS4<=0,045705	20,00000	62,5000
0,023642<HS4<=0,045705	==>	0,019420<G2<=0,039332, 0,023606<DPB2<=0,051124	20,00000	83,3333
0,023642<HS4<=0,045705, 0,023606<DPB2<=0,051124	==>	0,019420<G2<=0,039332	20,00000	83,3333
0,019420<G2<=0,039332	==>	0,023642<HS4<=0,045705, 0,023606<DPB2<=0,051124	20,00000	62,5000
0,019420<G2<=0,039332, 0,023606<DPB2<=0,051124	==>	0,023642<HS4<=0,045705	20,00000	83,3333
0,019420<G2<=0,039332, 0,023642<HS4<=0,045705	==>	0,023606<DPB2<=0,051124	20,00000	100,0000
0,023606<DPB2<=0,051124	==>	0,019420<G2<=0,039332, 0,023642<HS4<=0,045705, 0,019518<HC3<=0,040831	20,00000	62,5000
0,019518<HC3<=0,040831	==>	0,019420<G2<=0,039332, 0,023642<HS4<=0,045705, 0,023606<DPB2<=0,051124	20,00000	55,5556
0,019518<HC3<=0,040831, 0,023606<DPB2<=0,051124	==>	0,019420<G2<=0,039332, 0,023642<HS4<=0,045705	20,00000	83,3333

0,023642<HS4<=0,045705	==>	0,019420<G2<=0,039332, 0,019518<HC3<=0,040831, 0,023606<DPB2<=0,051124	20,00000	83,3333
0,023642<HS4<=0,045705, 0,023606<DPB2<=0,051124	==>	0,019420<G2<=0,039332, 0,019518<HC3<=0,040831	20,00000	83,3333
0,023642<HS4<=0,045705, 0,019518<HC3<=0,040831	==>	0,019420<G2<=0,039332, 0,023606<DPB2<=0,051124	20,00000	83,3333
0,023642<HS4<=0,045705, 0,019518<HC3<=0,040831, 0,023606<DPB2<=0,051124	==>	0,019420<G2<=0,039332	20,00000	83,3333
0,019420<G2<=0,039332	==>	0,023642<HS4<=0,045705, 0,019518<HC3<=0,040831, 0,023606<DPB2<=0,051124	20,00000	62,5000
0,019420<G2<=0,039332, 0,023606<DPB2<=0,051124	==>	0,023642<HS4<=0,045705, 0,019518<HC3<=0,040831	20,00000	83,3333
0,019420<G2<=0,039332, 0,019518<HC3<=0,040831	==>	0,023642<HS4<=0,045705, 0,023606<DPB2<=0,051124	20,00000	71,4286
0,019420<G2<=0,039332, 0,019518<HC3<=0,040831, 0,023606<DPB2<=0,051124	==>	0,023642<HS4<=0,045705	20,00000	100,0000
0,019420<G2<=0,039332, 0,023642<HS4<=0,045705	==>	0,019518<HC3<=0,040831, 0,023606<DPB2<=0,051124	20,00000	100,0000
0,019420<G2<=0,039332, 0,023642<HS4<=0,045705, 0,023606<DPB2<=0,051124	==>	0,019518<HC3<=0,040831	20,00000	100,0000
0,019420<G2<=0,039332, 0,023642<HS4<=0,045705, 0,019518<HC3<=0,040831	==>	0,023606<DPB2<=0,051124	20,00000	100,0000
0,019518<HC3<=0,040831	==>	0,019420<G2<=0,039332	28,00000	77,7778
0,019420<G2<=0,039332	==>	0,019518<HC3<=0,040831	28,00000	87,5000
0,019518<HC3<=0,040831	==>	0,019420<G2<=0,039332, 0,012580<HC2<=0,033788	20,00000	55,5556
0,012580<HC2<=0,033788	==>	0,019420<G2<=0,039332, 0,019518<HC3<=0,040831	20,00000	71,4286
0,012580<HC2<=0,033788, 0,019518<HC3<=0,040831	==>	0,019420<G2<=0,039332	20,00000	83,3333
0,019420<G2<=0,039332	==>	0,012580<HC2<=0,033788, 0,019518<HC3<=0,040831	20,00000	62,5000
0,019420<G2<=0,039332, 0,019518<HC3<=0,040831	==>	0,012580<HC2<=0,033788	20,00000	71,4286
0,019420<G2<=0,039332, 0,012580<HC2<=0,033788	==>	0,019518<HC3<=0,040831	20,00000	100,0000
0,019518<HC3<=0,040831	==>	0,019420<G2<=0,039332, 0,023642<HS4<=0,045705	20,00000	55,5556
0,023642<HS4<=0,045705	==>	0,019420<G2<=0,039332, 0,019518<HC3<=0,040831	20,00000	83,3333
0,023642<HS4<=0,045705, 0,019518<HC3<=0,040831	==>	0,019420<G2<=0,039332	20,00000	83,3333

0,019420<G2<=0,039332	==>	0,023642<HS4<=0,045705, 0,019518<HC3<=0,040831	20,00000	62,5000
0,019420<G2<=0,039332, 0,019518<HC3<=0,040831	==>	0,023642<HS4<=0,045705	20,00000	71,4286
0,019420<G2<=0,039332, 0,023642<HS4<=0,045705	==>	0,019518<HC3<=0,040831	20,00000	100,0000
0,019518<HC3<=0,040831	==>	0,019420<G2<=0,039332, 0,021421<MS1<=0,042453	20,00000	55,5556
0,021421<MS1<=0,042453	==>	0,019420<G2<=0,039332, 0,019518<HC3<=0,040831	20,00000	83,3333
0,021421<MS1<=0,042453, 0,019518<HC3<=0,040831	==>	0,019420<G2<=0,039332	20,00000	83,3333
0,019420<G2<=0,039332	==>	0,021421<MS1<=0,042453, 0,019518<HC3<=0,040831	20,00000	62,5000
0,019420<G2<=0,039332, 0,019518<HC3<=0,040831	==>	0,021421<MS1<=0,042453	20,00000	71,4286
0,019420<G2<=0,039332, 0,021421<MS1<=0,042453	==>	0,019518<HC3<=0,040831	20,00000	100,0000
0,019518<HC3<=0,040831	==>	0,019420<G2<=0,039332, 0,011420<A5<=0,034840	20,00000	55,5556
0,011420<A5<=0,034840	==>	0,019420<G2<=0,039332, 0,019518<HC3<=0,040831	20,00000	83,3333
0,011420<A5<=0,034840, 0,019518<HC3<=0,040831	==>	0,019420<G2<=0,039332	20,00000	100,0000
0,019420<G2<=0,039332	==>	0,011420<A5<=0,034840, 0,019518<HC3<=0,040831	20,00000	62,5000
0,019420<G2<=0,039332, 0,019518<HC3<=0,040831	==>	0,011420<A5<=0,034840	20,00000	71,4286
0,019420<G2<=0,039332, 0,011420<A5<=0,034840	==>	0,019518<HC3<=0,040831	20,00000	100,0000
0,012580<HC2<=0,033788	==>	0,019420<G2<=0,039332	20,00000	71,4286
0,019420<G2<=0,039332	==>	0,012580<HC2<=0,033788	20,00000	62,5000
0,023642<HS4<=0,045705	==>	0,019420<G2<=0,039332	20,00000	83,3333
0,019420<G2<=0,039332	==>	0,023642<HS4<=0,045705	20,00000	62,5000
0,021421<MS1<=0,042453	==>	0,019420<G2<=0,039332	20,00000	83,3333
0,019420<G2<=0,039332	==>	0,021421<MS1<=0,042453	20,00000	62,5000
0,017056<SPC5<=0,039673	==>	0,019420<G2<=0,039332	20,00000	62,5000
0,019420<G2<=0,039332	==>	0,017056<SPC5<=0,039673	20,00000	62,5000
0,011420<A5<=0,034840	==>	0,019420<G2<=0,039332	20,00000	83,3333
0,019420<G2<=0,039332	==>	0,011420<A5<=0,034840	20,00000	62,5000
0,019518<HC3<=0,040831	==>	0,011420<A5<=0,034840	20,00000	55,5556
0,011420<A5<=0,034840	==>	0,019518<HC3<=0,040831	20,00000	83,3333
0,019529<DAI4<=0,038758	==>	0,017056<SPC5<=0,039673	20,00000	71,4286
0,017056<SPC5<=0,039673	==>	0,019529<DAI4<=0,038758	20,00000	62,5000
0,023606<DPB2<=0,051124	==>	0,017056<SPC5<=0,039673	24,00000	75,0000
0,017056<SPC5<=0,039673	==>	0,023606<DPB2<=0,051124	24,00000	75,0000

0,019518<HC3<=0,040831	==>	0,017056<SPC5<=0,039673	24,00000	66,6667
0,017056<SPC5<=0,039673	==>	0,019518<HC3<=0,040831	24,00000	75,0000
0,023606<DPB2<=0,051124	==>	0,021421<MS1<=0,042453	20,00000	62,5000
0,021421<MS1<=0,042453	==>	0,023606<DPB2<=0,051124	20,00000	83,3333
0,023606<DPB2<=0,051124	==>	0,021421<MS1<=0,042453, 0,019518<HC3<=0,040831	20,00000	62,5000
0,019518<HC3<=0,040831	==>	0,021421<MS1<=0,042453, 0,023606<DPB2<=0,051124	20,00000	55,5556
0,019518<HC3<=0,040831, 0,023606<DPB2<=0,051124	==>	0,021421<MS1<=0,042453	20,00000	83,3333
0,021421<MS1<=0,042453	==>	0,019518<HC3<=0,040831, 0,023606<DPB2<=0,051124	20,00000	83,3333
0,021421<MS1<=0,042453, 0,023606<DPB2<=0,051124	==>	0,019518<HC3<=0,040831	20,00000	100,0000
0,021421<MS1<=0,042453, 0,019518<HC3<=0,040831	==>	0,023606<DPB2<=0,051124	20,00000	83,3333
0,023606<DPB2<=0,051124	==>	0,021421<MS1<=0,042453, 0,023642<HS4<=0,045705	20,00000	62,5000
0,023642<HS4<=0,045705	==>	0,021421<MS1<=0,042453, 0,023606<DPB2<=0,051124	20,00000	83,3333
0,023642<HS4<=0,045705, 0,023606<DPB2<=0,051124	==>	0,021421<MS1<=0,042453	20,00000	83,3333
0,021421<MS1<=0,042453	==>	0,023642<HS4<=0,045705, 0,023606<DPB2<=0,051124	20,00000	83,3333
0,021421<MS1<=0,042453, 0,023606<DPB2<=0,051124	==>	0,023642<HS4<=0,045705	20,00000	100,0000
0,021421<MS1<=0,042453, 0,023642<HS4<=0,045705	==>	0,023606<DPB2<=0,051124	20,00000	100,0000
0,023606<DPB2<=0,051124	==>	0,021421<MS1<=0,042453, 0,023642<HS4<=0,045705, 0,019518<HC3<=0,040831	20,00000	62,5000
0,019518<HC3<=0,040831	==>	0,021421<MS1<=0,042453, 0,023642<HS4<=0,045705, 0,023606<DPB2<=0,051124	20,00000	55,5556
0,019518<HC3<=0,040831, 0,023606<DPB2<=0,051124	==>	0,021421<MS1<=0,042453, 0,023642<HS4<=0,045705	20,00000	83,3333
0,023642<HS4<=0,045705	==>	0,021421<MS1<=0,042453, 0,019518<HC3<=0,040831, 0,023606<DPB2<=0,051124	20,00000	83,3333
0,023642<HS4<=0,045705, 0,023606<DPB2<=0,051124	==>	0,021421<MS1<=0,042453, 0,019518<HC3<=0,040831	20,00000	83,3333
0,023642<HS4<=0,045705, 0,019518<HC3<=0,040831	==>	0,021421<MS1<=0,042453, 0,023606<DPB2<=0,051124	20,00000	83,3333
0,023642<HS4<=0,045705, 0,019518<HC3<=0,040831, 0,023606<DPB2<=0,051124	==>	0,021421<MS1<=0,042453	20,00000	83,3333
0,021421<MS1<=0,042453	==>	0,023642<HS4<=0,045705, 0,019518<HC3<=0,040831, 0,023606<DPB2<=0,051124	20,00000	83,3333

0,021421<MS1<=0,042453, 0,023606<DPB2<=0,051124	==>	0,023642<HS4<=0,045705, 0,019518<HC3<=0,040831	20,00000	100,0000
0,021421<MS1<=0,042453, 0,019518<HC3<=0,040831	==>	0,023642<HS4<=0,045705, 0,023606<DPB2<=0,051124	20,00000	83,3333
0,021421<MS1<=0,042453, 0,019518<HC3<=0,040831, 0,023606<DPB2<=0,051124	==>	0,023642<HS4<=0,045705	20,00000	100,0000
0,021421<MS1<=0,042453, 0,023642<HS4<=0,045705	==>	0,019518<HC3<=0,040831, 0,023606<DPB2<=0,051124	20,00000	100,0000
0,021421<MS1<=0,042453, 0,023642<HS4<=0,045705, 0,023606<DPB2<=0,051124	==>	0,019518<HC3<=0,040831	20,00000	100,0000
0,021421<MS1<=0,042453, 0,023642<HS4<=0,045705, 0,019518<HC3<=0,040831	==>	0,023606<DPB2<=0,051124	20,00000	100,0000
0,019518<HC3<=0,040831	==>	0,021421<MS1<=0,042453	24,00000	66,6667
0,021421<MS1<=0,042453	==>	0,019518<HC3<=0,040831	24,00000	100,0000
0,019518<HC3<=0,040831	==>	0,021421<MS1<=0,042453, 0,012580<HC2<=0,033788	20,00000	55,5556
0,012580<HC2<=0,033788	==>	0,021421<MS1<=0,042453, 0,019518<HC3<=0,040831	20,00000	71,4286
0,012580<HC2<=0,033788, 0,019518<HC3<=0,040831	==>	0,021421<MS1<=0,042453	20,00000	83,3333
0,021421<MS1<=0,042453	==>	0,012580<HC2<=0,033788, 0,019518<HC3<=0,040831	20,00000	83,3333
0,021421<MS1<=0,042453, 0,019518<HC3<=0,040831	==>	0,012580<HC2<=0,033788	20,00000	83,3333
0,021421<MS1<=0,042453, 0,012580<HC2<=0,033788	==>	0,019518<HC3<=0,040831	20,00000	100,0000
0,019518<HC3<=0,040831	==>	0,021421<MS1<=0,042453, 0,023642<HS4<=0,045705	20,00000	55,5556
0,023642<HS4<=0,045705	==>	0,021421<MS1<=0,042453, 0,019518<HC3<=0,040831	20,00000	83,3333
0,023642<HS4<=0,045705, 0,019518<HC3<=0,040831	==>	0,021421<MS1<=0,042453	20,00000	83,3333
0,021421<MS1<=0,042453	==>	0,023642<HS4<=0,045705, 0,019518<HC3<=0,040831	20,00000	83,3333
0,021421<MS1<=0,042453, 0,019518<HC3<=0,040831	==>	0,023642<HS4<=0,045705	20,00000	83,3333
0,021421<MS1<=0,042453, 0,023642<HS4<=0,045705	==>	0,019518<HC3<=0,040831	20,00000	100,0000
0,012580<HC2<=0,033788	==>	0,021421<MS1<=0,042453	20,00000	71,4286
0,021421<MS1<=0,042453	==>	0,012580<HC2<=0,033788	20,00000	83,3333
0,023642<HS4<=0,045705	==>	0,021421<MS1<=0,042453	20,00000	83,3333
0,021421<MS1<=0,042453	==>	0,023642<HS4<=0,045705	20,00000	83,3333
0,019518<HC3<=0,040831	==>	0,001923<HS3<=0,020802	20,00000	55,5556
0,001923<HS3<=0,020802	==>	0,019518<HC3<=0,040831	20,00000	100,0000
0,023606<DPB2<=0,051124	==>	0,023642<HS4<=0,045705	24,00000	75,0000

0,023642<HS4<=0,045705	==>	0,023606<DPB2<=0,051124	24,00000	100,0000
0,023606<DPB2<=0,051124	==>	0,023642<HS4<=0,045705, 0,019518<HC3<=0,040831	24,00000	75,0000
0,019518<HC3<=0,040831	==>	0,023642<HS4<=0,045705, 0,023606<DPB2<=0,051124	24,00000	66,6667
0,019518<HC3<=0,040831, 0,023606<DPB2<=0,051124	==>	0,023642<HS4<=0,045705	24,00000	100,0000
0,023642<HS4<=0,045705	==>	0,019518<HC3<=0,040831, 0,023606<DPB2<=0,051124	24,00000	100,0000
0,023642<HS4<=0,045705, 0,023606<DPB2<=0,051124	==>	0,019518<HC3<=0,040831	24,00000	100,0000
0,023642<HS4<=0,045705, 0,019518<HC3<=0,040831	==>	0,023606<DPB2<=0,051124	24,00000	100,0000
0,023606<DPB2<=0,051124	==>	0,023642<HS4<=0,045705, 0,012580<HC2<=0,033788	20,00000	62,5000
0,012580<HC2<=0,033788	==>	0,023642<HS4<=0,045705, 0,023606<DPB2<=0,051124	20,00000	71,4286
0,012580<HC2<=0,033788, 0,023606<DPB2<=0,051124	==>	0,023642<HS4<=0,045705	20,00000	100,0000
0,023642<HS4<=0,045705	==>	0,012580<HC2<=0,033788, 0,023606<DPB2<=0,051124	20,00000	83,3333
0,023642<HS4<=0,045705, 0,023606<DPB2<=0,051124	==>	0,012580<HC2<=0,033788	20,00000	83,3333
0,023642<HS4<=0,045705, 0,012580<HC2<=0,033788	==>	0,023606<DPB2<=0,051124	20,00000	100,0000
0,023606<DPB2<=0,051124	==>	0,023642<HS4<=0,045705, 0,012580<HC2<=0,033788, 0,019518<HC3<=0,040831	20,00000	62,5000
0,019518<HC3<=0,040831	==>	0,023642<HS4<=0,045705, 0,012580<HC2<=0,033788, 0,023606<DPB2<=0,051124	20,00000	55,5556
0,019518<HC3<=0,040831, 0,023606<DPB2<=0,051124	==>	0,023642<HS4<=0,045705, 0,012580<HC2<=0,033788	20,00000	83,3333
0,012580<HC2<=0,033788	==>	0,023642<HS4<=0,045705, 0,019518<HC3<=0,040831, 0,023606<DPB2<=0,051124	20,00000	71,4286
0,012580<HC2<=0,033788, 0,023606<DPB2<=0,051124	==>	0,023642<HS4<=0,045705, 0,019518<HC3<=0,040831	20,00000	100,0000
0,012580<HC2<=0,033788, 0,019518<HC3<=0,040831	==>	0,023642<HS4<=0,045705, 0,023606<DPB2<=0,051124	20,00000	83,3333
0,012580<HC2<=0,033788, 0,019518<HC3<=0,040831, 0,023606<DPB2<=0,051124	==>	0,023642<HS4<=0,045705	20,00000	100,0000
0,023642<HS4<=0,045705	==>	0,012580<HC2<=0,033788, 0,019518<HC3<=0,040831, 0,023606<DPB2<=0,051124	20,00000	83,3333
0,023642<HS4<=0,045705, 0,023606<DPB2<=0,051124	==>	0,012580<HC2<=0,033788, 0,019518<HC3<=0,040831	20,00000	83,3333

0,023642<HS4<=0,045705, 0,019518<HC3<=0,040831	==>	0,012580<HC2<=0,033788, 0,023606<DPB2<=0,051124	20,00000	83,3333
0,023642<HS4<=0,045705, 0,019518<HC3<=0,040831, 0,023606<DPB2<=0,051124	==>	0,012580<HC2<=0,033788	20,00000	83,3333
0,023642<HS4<=0,045705, 0,012580<HC2<=0,033788	==>	0,019518<HC3<=0,040831, 0,023606<DPB2<=0,051124	20,00000	100,0000
0,023642<HS4<=0,045705, 0,012580<HC2<=0,033788, 0,023606<DPB2<=0,051124	==>	0,019518<HC3<=0,040831	20,00000	100,0000
0,023642<HS4<=0,045705, 0,012580<HC2<=0,033788, 0,019518<HC3<=0,040831	==>	0,023606<DPB2<=0,051124	20,00000	100,0000
0,019518<HC3<=0,040831	==>	0,023642<HS4<=0,045705	24,00000	66,6667
0,023642<HS4<=0,045705	==>	0,019518<HC3<=0,040831	24,00000	100,0000
0,019518<HC3<=0,040831	==>	0,023642<HS4<=0,045705, 0,012580<HC2<=0,033788	20,00000	55,5556
0,012580<HC2<=0,033788	==>	0,023642<HS4<=0,045705, 0,019518<HC3<=0,040831	20,00000	71,4286
0,012580<HC2<=0,033788, 0,019518<HC3<=0,040831	==>	0,023642<HS4<=0,045705	20,00000	83,3333
0,023642<HS4<=0,045705	==>	0,012580<HC2<=0,033788, 0,019518<HC3<=0,040831	20,00000	83,3333
0,023642<HS4<=0,045705, 0,019518<HC3<=0,040831	==>	0,012580<HC2<=0,033788	20,00000	83,3333
0,023642<HS4<=0,045705, 0,012580<HC2<=0,033788	==>	0,019518<HC3<=0,040831	20,00000	100,0000
0,012580<HC2<=0,033788	==>	0,023642<HS4<=0,045705	20,00000	71,4286
0,023642<HS4<=0,045705	==>	0,012580<HC2<=0,033788	20,00000	83,3333
0,012587<SU2<=0,031392	==>	0,012580<HC2<=0,033788	20,00000	83,3333
0,012580<HC2<=0,033788	==>	0,012587<SU2<=0,031392	20,00000	71,4286
0,023606<DPB2<=0,051124	==>	0,012580<HC2<=0,033788	20,00000	62,5000
0,012580<HC2<=0,033788	==>	0,023606<DPB2<=0,051124	20,00000	71,4286
0,023606<DPB2<=0,051124	==>	0,012580<HC2<=0,033788, 0,019518<HC3<=0,040831	20,00000	62,5000
0,019518<HC3<=0,040831	==>	0,012580<HC2<=0,033788, 0,023606<DPB2<=0,051124	20,00000	55,5556
0,019518<HC3<=0,040831, 0,023606<DPB2<=0,051124	==>	0,012580<HC2<=0,033788	20,00000	83,3333
0,012580<HC2<=0,033788	==>	0,019518<HC3<=0,040831, 0,023606<DPB2<=0,051124	20,00000	71,4286
0,012580<HC2<=0,033788, 0,023606<DPB2<=0,051124	==>	0,019518<HC3<=0,040831	20,00000	100,0000
0,012580<HC2<=0,033788, 0,019518<HC3<=0,040831	==>	0,023606<DPB2<=0,051124	20,00000	83,3333
0,019518<HC3<=0,040831	==>	0,012580<HC2<=0,033788	24,00000	66,6667
0,012580<HC2<=0,033788	==>	0,019518<HC3<=0,040831	24,00000	85,7143
0,012587<SU2<=0,031392	==>	0,019518<HC3<=0,040831	20,00000	83,3333

0,019518<HC3<=0,040831	==>	0,012587<SU2<=0,031392	20,00000	55,5556
0,037186<SU1<=0,059862	==>	0,019518<HC3<=0,040831	20,00000	100,0000
0,019518<HC3<=0,040831	==>	0,037186<SU1<=0,059862	20,00000	55,5556
0,016892<A6<=0,035008	==>	0,019518<HC3<=0,040831	20,00000	100,0000
0,019518<HC3<=0,040831	==>	0,016892<A6<=0,035008	20,00000	55,5556
0,019529<DAI4<=0,038758	==>	0,019518<HC3<=0,040831	20,00000	71,4286
0,019518<HC3<=0,040831	==>	0,019529<DAI4<=0,038758	20,00000	55,5556
0,023606<DPB2<=0,051124	==>	0,019518<HC3<=0,040831	24,00000	75,0000
0,019518<HC3<=0,040831	==>	0,023606<DPB2<=0,051124	24,00000	66,6667
0,019529<DAI4<=0,038758	==>	0,023606<DPB2<=0,051124	20,00000	71,4286
0,023606<DPB2<=0,051124	==>	0,019529<DAI4<=0,038758	20,00000	62,5000
0,045453<C3<=0,066084	==>	0,036882<C2<=0,061094	20,00000	100,0000
0,036882<C2<=0,061094	==>	0,045453<C3<=0,066084	20,00000	83,3333