МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Сумський державний університет
Навчально-науковий інститут бізнесу, економіки та менеджменту
Кафедра економічної кібернетики

«До захисту допущено»
Завідувач кафедри
_____ _____
(підпис) (Ім'я та ПРІЗВИЩЕ)
____ _____ 20__ р.

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня ____магістр_____
(бакалавр / магістр)
зі спеціальності _____051 «Економіка»_____ ,
(код та назва)
освітньо-професійної програми «Економічна кібернетика»
(освітньо-професійної / освітньо-наукової) (назва програми)
на тему: «Моделювання ймовірної поведінки дій інсайдерів-кібершахраїв у банках»

Здобувача (ки) групи ЕК.м-21 Рапути Альони Олексіївни
(шифр групи) (прізвище, ім'я, по батькові)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.
_____ Альона РАПУТА
(підпис) (Ім'я та ПРІЗВИЩЕ здобувача)

Керівник
доцентка, д.е.н., доцентка, Ганна ЯРОВЕНКО _____
(посада, науковий ступінь, вчене звання, Ім'я та ПРІЗВИЩЕ) (підпис)

Суми – 2023

Міністерство освіти і науки України

Сумський державний університет

Навчально-науковий інститут бізнесу, економіки та менеджменту

Кафедра економічної кібернетики

ЗАТВЕРДЖУЮ
Завідувач кафедри
к.е.н., доцент
_____ В.В. Койбічук
“__” _____ 2023 р.

ЗАВДАННЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ МАГІСТРА
спеціальність 051 «Економіка (Економічна кібернетика)
студентки 5 курсу, групи ЕК.м-21

_____Рапути Альони Олексіївни_____
(прізвище, ім’я, по батькові студента)

1. Тема роботи «МОДЕЛЮВАННЯ ЙМОВІРНОЇ ПОВЕДІНКИ ДІЙ ІНСАЙДЕРІВ-КІБЕРШАХРАЇВ У БАНКАХ».
затверджена наказом по університету від «22» листопада 2023 року № 1331-VI
2. Термін подання студентом закінченої роботи «17» грудня 2023 року
3. Мета кваліфікаційної роботи – розробка методики моделювання ймовірної поведінки дій інсайдерів-кібершахраїв у банках.
4. Об’єкт дослідження – процес моделювання розвитку кіберзагроз та способів їх усунення у фінансовому секторі.
5. Предмет дослідження – математичні методи та моделі оцінювання ймовірної поведінки дій інсайдерів-кібершахраїв у банках.
6. Кваліфікаційна робота виконується на матеріалах законодавчих та нормативно-правових актів з питань регулювання кібершахрайств у фінансовому секторі, аналітичних звітах та наукових публікаціях вітчизняних та зарубіжних авторів з питань дослідження кібершахрайств у фінансовому секторі; результатах частоти уживаності пошукових запитів на тему кібершахрайств у фінансовому секторі користувачами пошукової системи Google.
7. Орієнтовний план кваліфікаційної роботи, терміни подання розділів керівникові та зміст завдань для виконання поставленої мети
Розділ 1. ТЕОРЕТИЧНІ ТА МЕТОДИЧНІ ЗАСАДИ ПРОБЛЕМИ КІБЕРШАХРАЙСТВ У БАНКАХ – 15 листопада 2023 р.

У розділі 1 проаналізувати сучасні виклики фінансового сектору в контексті розвитку кібершахрайств та їх наслідків; провести систематизацію існуючих теоретичних підходів щодо розгляду кібершахрайств у банках.

Розділ 2. ПОБУДОВА МАТЕМАТИЧНОЇ МОДЕЛІ ЙМОВІРНОЇ ПОВЕДІНКИ ДІЙ ІНСАЙДЕРІВ-КІБЕРШАХРАЇВ У БАНКУ – 25 листопада 2023 р.

У розділі 2 описати вхідні дані для побудови математичної моделі ймовірної поведінки дій інсайдерів-кібершахраїв у банку; сформувати вимоги до методологічного забезпечення моделювання ймовірної поведінки дій інсайдерів-кібершахраїв у банку.

Розділ 3. ПРАКТИЧНА РЕАЛІЗАЦІЯ МОДЕЛІ ЙМОВІРНОЇ ПОВЕДІНКИ ДІЙ ІНСАЙДЕРІВ-КІБЕРШАХРАЇВ У БАНКУ – 7 грудня 2023 р.

У розділі 3 проаналізувати отримані результати та перевірити адекватність побудованої математичної моделі; розробити рекомендації за результатами проведених розрахунків.

8. Консультації з роботи:

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
1	Яровенко Г.М., доцентка кафедри економічної кібернетики, доцентка, д.е.н.	30.10.2023	30.10.2023
2	Яровенко Г.М., доцентка кафедри економічної кібернетики, доцентка, д.е.н.	30.10.2023	30.10.2023
3	Яровенко Г.М., доцентка кафедри економічної кібернетики, доцентка, д.е.н.	30.10.2023	30.10.2023

9. Дата видачі завдання: «30» жовтня 2023 року

Керівник кваліфікаційної роботи _____ Яровенко Г.М.
(підпис) (ініціали, прізвище)

Завдання до виконання одержав _____ Рапута А.О.
(підпис) (ініціали, прізвище)

АНОТАЦІЯ

дипломної роботи на тему:

«МОДЕЛЮВАННЯ ЙМОВІРНОЇ ПОВЕДІНКИ ДІЙ ІНСАЙДЕРІВ-КІБЕРШАХРАЇВ У БАНКАХ»

студентки

Рапути Альони Олексіївни

Актуальність теми дослідження. Актуальність теми визначається активним проникненням кіберзлочинності у банківський сектор, що охоплює широкий спектр шкідливих дій, від складних схем злому до оманливих тактик соціальної інженерії. Крім того, проблема інсайдерського кібершахрайства в банківському секторі є серйозною та складною проблемою для фінансових установ. На відміну від зовнішніх загроз, інсайдерське кібершахрайство може поставити під загрозу цілісність банківських систем і підірвати довіру клієнтів і зацікавлених сторін. Тому важливо розуміти потенційну поведінку інсайдера-кібершахрая в банку для того, щоб вміти вчасно виявити та мінімізувати наслідки від їх шахрайських дій.

Метою даної роботи є розробка методики моделювання ймовірної поведінки дій інсайдерів-кібершахраїв у банках.

Об'єктом дослідження є процес моделювання розвитку кіберзагроз та способів їх усунення у фінансовому секторі.

Предметом дослідження є математичні методи та моделі оцінювання ймовірної поведінки дій інсайдерів-кібершахраїв у банках.

Методи дослідження. Для дослідження поставлених завдань були використані такі *загальнонаукові та специфічні методи дослідження,* як: індукція та дедукція, аналіз та синтез, порівняння та логічне узагальнення, табличний та графічний метод, метод бібліографічного аналізу, метод головних компонент, кластерний аналіз методом *k*-середніх, метод моделювання за допомогою асоціативних правил.

Основний науковий результат роботи. У роботі проведено аналіз сучасних викликів фінансового сектору в контексті розвитку кібершахрайств та їх наслідків; систематизовано існуючі теоретичні підходи щодо розгляду кібершахрайств у

банках; сформовано задачі моделювання ймовірної поведінки дій інсайдерів-кібершахраїв у банках; обрано вхідні дані для побудови математичної моделі ймовірної поведінки дій інсайдерів-кібершахраїв у банках; описано вимоги до методологічного забезпечення моделювання ймовірної поведінки дій інсайдерів-кібершахраїв у банках; проаналізовано отримані результати методу головних компонент, кластеризації і асоціативного аналізу та перевірено адекватність моделі; розроблено рекомендації за результатами проведених розрахунків

Рекомендації щодо використання результатів дослідження. Отримані результати можуть бути використані комерційними банками для виявлення потенційних інсайдерів-кібершахраїв та забезпечення кращого рівня захисту клієнтів від дій інсайдерів-кібершахраїв банку; клієнтами банку для аналізу та уникнення від потенційних загроз зі сторони інсайдерів-кібершахраїв банку; правоохоронними органами для оперативного реагування на потенційні загрозі з боку інсайдерів-кібершахраїв банку.

Інформаційною базою кваліфікаційної роботи є законодавчі та нормативно-правові акти з питань регулювання кібершахрайств у фінансовому секторі, аналітичні звіти та наукові публікації вітчизняних та зарубіжних авторів з питань дослідження кібершахрайств у фінансовому секторі; результати частоти уживаності пошукових запитів на тему кібершахрайств у фінансовому секторі користувачами пошукової системи Google.

Ключові слова: інсайдери-кібершахраї, банк, фінансовий сектор, метод головних компонент, кластерний аналіз, асоціативний аналіз.

Основний зміст кваліфікаційної роботи викладено на 59 сторінках, у тому числі список використаних джерел з 73 найменування, який розміщено на 9 сторінках. Робота містить 10 таблиць, 20 рисунків, а також 2 додатки.

Рік виконання кваліфікаційної роботи – 2023 рік.

Рік захисту роботи – 2023 рік.

SUMMARY

Insider cyber fraud in the banking sector is a serious and complex issue for financial institutions. Unlike external threats, insider cyber fraud entails individuals within the organization exploiting their privileged access to engage in fraudulent activities. Insider threats can jeopardize the integrity of banking systems and undermine trust among clients and stakeholders. This form of cyber fraud is particularly insidious due to the inherent access and knowledge possessed by insiders, necessitating banks to implement comprehensive strategies for detecting, preventing, and responding to these internal threats.

The aim of this study is to develop a methodology for modeling the potential behavior of insider cyber fraudsters in banks.

The research object is the process of modeling the development of cyber threats and ways to mitigate them in the financial sector.

The subject of the research encompasses mathematical methods and models for evaluating the probable behavior of insider cyber fraudsters in banks.

Therefore, the research tasks include:

Analyzing current challenges in the financial sector concerning the evolution of cyber fraud and its consequences.

Systematizing existing theoretical approaches regarding cyber fraud in banks.

Formulating tasks for modeling the probable behavior of insider cyber fraudsters in banks.

Describing the input data for constructing a mathematical model of the probable behavior of insider cyber fraudsters in banks.

Specifying requirements for the methodological support of modeling the probable behavior of insider cyber fraudsters in banks.

Analyzing the obtained results and verifying the adequacy of the constructed mathematical model.

Formulating recommendations based on the results of the conducted calculations.

To achieve the set goal and research tasks, various general scientific and specific research methods were employed, such as induction and deduction, analysis and synthesis,

comparison and logical generalization, tabular and graphical methods, bibliographic analysis method, principal component analysis method, k-means clustering analysis method, and associative rule modeling method.

The main scientific outcome of this master's thesis lies in the development of a scientific and methodological approach to model the probable behavior of insider cyber fraudsters in banks, based on a complex combination of principal component analysis, k-means clustering, and associative analysis. The obtained results can be utilized by commercial banks for identifying potential insider cyber fraudsters and ensuring a higher level of client protection against the actions of insider cyber fraudsters; by bank clients for analyzing and mitigating potential threats from insider cyber fraudsters; and by law enforcement agencies for prompt responses to potential threats posed by insider cyber fraudsters in banks.

The research is based on legislative and regulatory acts related to the regulation of cyber fraud in the financial sector, analytical reports, and scientific publications by domestic and foreign authors on the investigation of cyber fraud in the financial sector, as well as the frequency of search queries related to cyber fraud in the financial sector by users on the Google search engine.

Within the scope of the presented research topic, the objective was formulated to develop a methodology for modeling the probable behavior of insider cyber fraudsters in banks. To achieve this goal, seven tasks were articulated, each of which was successfully accomplished.

During the analysis of current challenges in the financial sector regarding the evolution of cyber fraud and its implications, key trends and innovations in the banking system were examined. This involved outlining the structure of the most prevalent cyber frauds in the financial sector today and researching the existing international regulatory framework aimed at enhancing cybersecurity in the financial sphere.

The systematization of existing theoretical approaches concerning the examination of cyber fraud in banks revealed a positive trend in the dynamics of the number of published materials in conferences and articles using keywords "cyber" and "frauds" in the Scopus database from 2000 to 2023. Additionally, utilizing the VOSviewer software facilitated the

systematization of keyword combinations used in scholarly publications on the chosen topic, forming clusters to visualize and organize vectors of scientific research.

As part of the formulated tasks for modeling the probable behavior of insider cyber fraudsters in banks, a method of utilizing possible combinations of search queries in the Google search engine was proposed as an array of input variables to assess this behavior. Two lists of variables were generated: the first comprising ten variables directly characterizing cyberattacks, and the second denoting variables indicating a decrease in trust levels in financial institutions.

The proposed methodological approach for modeling the probable behavior of insider cyber fraudsters in banks consisted of three stages. In the first and second stages, using principal component analysis and k-means clustering, a dataset of the most relevant variables for further research was established. Twelve out of twenty initial variables were grouped into three lists. Subsequently, using associative rule modeling in the modeling stage, three models of associative rules were constructed. Based on these models, it was concluded that personal financial information of the client, access to the client's online banking account, and possession of their mobile phone are particularly appealing to potential insider cyber fraudsters in banks. Therefore, preventive measures should be taken by banks to minimize the consequences of insider cyber fraud actions, while clients should be vigilant regarding their personal data.

During the execution of this work, two lists of ten variables each were formed, representing search queries characterizing cyberattacks and the level of decreased trust in financial institutions. Preliminary analysis of the frequency of usage of these search queries by users of the Google search engine confirmed that not all of them are equally popular. However, the positive trend over recent years corroborates the prevalence of the cybercrime issue in society. Associative analysis of three sets of variables, initially selected through the principal method, allowed understanding what is most intriguing for potential insider cybercriminals in banks: the client's personal financial information, access to the client's online banking profile, and seizing their phone.

Hence, to minimize the consequences of insider cybercriminal actions in banks, it is necessary to undertake preventive measures and always remain vigilant. Among the primary preventive measures, the following can be considered:

Engage only with verified bank employees who can appropriately confirm their affiliation with the bank, refraining from sharing personal passwords and other confidential information directly with bank employees.

Employ multi-factor authentication for online banking operations.

Regularly update security software, including antivirus programs.

Monitor the activity of one's own account in real-time to detect unusual or suspicious activities (which may include large transactions, unsuccessful login attempts, or transactions from unfamiliar locations).

Use robust passwords and secure applications for mobile banking.

Protect oneself from potential cybercrimes (such as investing in cyber insurance to reduce financial losses in case of a cyberattack, providing coverage for legal expenses).

By combining these measures, bank clients can strengthen their cybersecurity and minimize the consequences of cybercrime.

The work involved an analysis of contemporary challenges within the financial sector concerning the development of cyber frauds and their repercussions. It systematically organized existing theoretical approaches regarding the examination of cyber frauds within banking institutions. It formulated tasks for modeling the probable behavior of insider cyber fraudsters within banks. Furthermore, it analyzed the obtained results and proposed recommendations to commercial banks, bank clients, and law enforcement agencies responsible for regulating cyber fraud issues.

Keywords: insider cyber fraudsters, bank, financial sector, principal component analysis, cluster analysis, associative analysis.

The diploma thesis was carried out within the framework of the state-funded research work 0121U109559 "National Security through the Convergence of Financial Monitoring Systems and Cybersecurity: Intelligent Modeling of Financial Market Regulation Mechanisms.".

ЗМІСТ

ВСТУП

Інсайдерське кібершахрайство в банківському секторі є серйозною та складною проблемою для фінансових установ. На відміну від зовнішніх загроз, інсайдерське кібершахрайство передбачає, що особи в організації використовують свій привілейований доступ для здійснення шахрайських дій. Інсайдерські загрози можуть поставити під загрозу цілісність банківських систем і підірвати довіру клієнтів і зацікавлених сторін. Ця форма кібершахрайства є особливо підступною через невід'ємний доступ і знання, якими володіють інсайдери, що робить обов'язковим для банків впровадження комплексних стратегій для виявлення, запобігання та реагування на ці внутрішні загрози.

Метою даної роботи є розробка методики моделювання ймовірної поведінки дій інсайдерів-кібершахраїв у банках.

Об'єктом дослідження є процес моделювання розвитку кіберзагроз та способів їх усунення у фінансовому секторі.

Предметом дослідження є математичні методи та моделі оцінювання ймовірної поведінки дій інсайдерів-кібершахраїв у банках.

У зв'язку із цим, *завданнями дослідження* є:

– проаналізувати сучасні виклики фінансового сектору в контексті розвитку кібершахрайств та їх наслідків;

– систематизувати існуючі теоретичні підходи щодо розгляду кібершахрайств у банках;

– сформовати задачі моделювання ймовірної поведінки дій інсайдерів-кібершахраїв у банках;

– описати вхідні дані для побудови математичної моделі ймовірної поведінки дій інсайдерів-кібершахраїв у банках;

– сформулювати вимоги до методологічного забезпечення моделювання ймовірної поведінки дій інсайдерів-кібершахраїв у банках;

– проаналізувати отримані результати та перевірити адекватність побудованої математичної моделі;

– розробити рекомендації за результатами проведених розрахунків.

Для досягнення поставленої мети та завдань дослідження були використані такі *загальнонаукові та специфічні методи дослідження*, як: індукція та дедукція, аналіз та синтез, порівняння та логічне узагальнення, табличний та графічний метод, метод бібліографічного аналізу, метод головних компонент, кластерний аналіз методом *k*-середніх, метод моделювання за допомогою асоціативних правил.

Основний науковий результат кваліфікаційної магістерської роботи полягає в розробці науково-методичного підходу до моделі ймовірної поведінки дій інсайдерів-кібершахраїв у банках на основі визначення комплексного поєднання методу головних компонент, кластеризації методом k-середніх та асоціативного аналізу, , що дозволило змоделювати потенційні портрети інсайдерів-кібершахраїв у банках. Одержані результати можуть бути використані комерційними банками для виявлення потенційних інсайдерів-кібершахраїв та забезпечення кращого рівня захисту клієнтів від дій інсайдерів-кібершахраїв банку; клієнтами банку для аналізу та уникнення від потенційних загроз зі сторони інсайдерів-кібершахраїв банку; правоохоронними органами для оперативного реагування на потенційні загрозі з боку інсайдерів-кібершахраїв банку.

Інформаційною базою дослідження є законодавчі та нормативно-правові акти з питань регулювання кібершахрайств у фінансовому секторі, аналітичні звіти та наукові публікації вітчизняних та зарубіжних авторів з питань дослідження кібершахрайств у фінансовому секторі; результати частоти уживаності пошукових запитів на тему кібершахрайств у фінансовому секторі користувачами пошукової системи Google.

Дипломна робота виконана в рамках держбюджетної науково-дослідної роботи 0121U109559 «Національна безпека через конвергенцію систем фінансового моніторингу та кібербезпеки: інтелектуальне моделювання механізмів регулювання фінансового ринку».

1. ТЕОРЕТИЧНІ ТА МЕТОДИЧНІ ЗАСАДИ ПРОБЛЕМИ КІБЕРШАХРАЙСТВ У БАНКАХ

1.1 Сучасні виклики фінансового сектору в контексті розвитку кібершахрайств та їх наслідків

Банківська система є одним із сегментів економіки, що продукує та акумулює в собі великі масиви даних. Крім того, саме банківська система є однією із найпопулярніших сфер, де почали активно запроваджувати концепцію «великих даних». Протягом останніх років банківська індустрія продовжує трансформуватись під впливом ряду інновацій, що виникають під впливом технологічного прогресу, поведінкових аспектів споживачів ринку банківських послуг та нормативного забезпечення. Серед важливих інновацій у банківській системі варто виділити наступні [54; 55; 1]:

1. Цифровий банкінг:

– інтернет-банкінг (дозволяє отримувати банківські послуги онлайн, виконувати різні транзакції, перевіряти баланси та керувати рахунками з особистих пристроїв);

– мобільний банкінг (використання спеціальних мобільних застосунків у банківській сфері дозволяє спрощувати ряд функцій пов’язаних із мобільними депозитами, переказами коштів, моніторингу рахунку в режимі реального часу тощо);

2. Fintech: охоплює широкий спектр інновацій, додатків і бізнес-моделей, які спрямовані на вдосконалення та оптимізацію різних аспектів фінансової індустрії.

3. Платіжні інновації: фінтех-компанії представили різні платіжні рішення, включаючи однорангові (P2P) платежі, мобільні гаманці та безконтактні платежі.

4. Робо-консультанти: автоматизовані інвестиційні платформи, які використовують алгоритми для надання фінансових консультацій і управління інвестиційними портфелями на основі індивідуальних уподобань і вілкритості до ризику.

5. Блокчейн і криптовалюти:

– криптовалюти (популяризація криптовалют, таких як біткойн та ефіріум, кинуло виклик традиційним банківським системам, забезпечивши децентралізовані та цифрові альтернативи традиційним валютам);

– технологія блокчейн (банки використовують блокчейн для безпечних і прозорих транзакцій, зменшення шахрайства та підвищення ефективності процесів, зокрема, транскордонних платежів).

6. Штучний інтелект (Artificial Intelligence, AI) і машинне навчання:

– чат-боти та віртуальні помічники (чат-боти та керований штучний інтелект використовуються для обслуговування клієнтів, відповідей на запити та надання інформації, що покращує взаємодію з клієнтами та оптимізує різноманітні банківські процеси);

– кредитний скоринг (алгоритми штучного інтелекту, який використовуються для більш точної оцінки кредитного ризику, що дозволяє банкам приймати кращі рішення щодо організації процесу кредитування).

7. Open Banking:

– інтерфейси прикладного програмування (Application Programming Interface, API) (дані інтерфейси відкритого банківського обслуговування передбачають безпечний обмін фінансовими даними, що дозволяє розробникам створювати інноваційні фінансові продукти та послуги);

– агрегація даних (клієнти мають змогу консолідувати свою фінансову інформацію з кількох установ в одному місці, надаючи повний огляд свого фінансового стану)

8. Регуляторні зміни:

– Директива про платіжні послуги 2 (Payment Services Directive2, PSD2) (дана Директива використовується у країнах Європейського союзу і сприяє розвитку відкритого банківського обслуговування, вимагаючи від банків безпечного обміну даними клієнтів із третіми сторонами, сприяючи розвитку конкурентних переваг фінансової установи та безпечному інноваційному розвитку);

– загальний регламент захисту даних (General Data Protection Regulation, GDPR) (дана технологія дозволяє підсилити захист даних і конфіденційність для окремих осіб, впливаючи на те, як фінансові установи, зокрема банки, обробляють дані клієнтів і формують політику конфіденційності).

9. Інновації в кібербезпеці:

– біометрична автентифікація (використання розпізнавання відбитків пальців, розпізнавання обличчя та інших біометричних методів підвищує безпеку здійснення банківських операцій);

– розширене шифрування (банки застосовують більш надійні методи шифрування для захисту даних клієнтів і фінансових операцій від кіберзагроз).

10. Сталий банкінг: все частіше банки та інші фінансові установи у своїх процесах прийняття рішень щодо формування пропозиції фінансових продуктів та послуг враховують екологічні, соціальні та управлінські чинники (ESG).

Ці інновації спільно формують ландшафт банківської галузі, що розвивається, надаючи нові можливості для ефективності, безпеки та обслуговування клієнтів.

Питанню безпеки в умовах цифровізації фінансової діяльності суб'єктів, які ведуть свою діяльність на фінансовому ринку, приділяється все більше уваги. Оскільки із розвитком інноваційних підходів трансформації фінансового сектору все більше актуалізується проблема кібершахрайства. Структура найбільш популярних кібершахрайств у фінансовій сфері на сьогоднішній день має наступний вигляд (табл. 1).

У період з жовтня 2021 року по вересень 2022 року шкідливе програмне забезпечення було найпоширенішим типом кібератак у фінансових і страхових організаціях у світі (рис. 1.1). З огляду на результати даного перерозподілу найбільше фінансових і страхових організацій у світі постраждали саме від шкідливого програмного забезпечення (40%). На другій та третій позиціях за рівнем уражених організацій фінансового сектору знаходяться кібершахрайства здійснені через веб-сайти та мобільні застосунки (23%) і внутрішньосистемні шахрайства (20%). По 8% світових фінансових та страхових організацій постраждали через захоплення облікових записів та соціального інжинірингу.

Таблиця 1.1 – Перелік найбільш популярних кібершахрайств у фінансовій сфері

№	Назва кібершахрайства	Характеристика
1.	Фішинг (phishing) та вішинг (vishing) атаки	Фішингова атака представляє масову розсилку електронних листів шахраїв, які видають себе за банк, змушуючи клієнтів або співробітників банку розкрити конфіденційну інформацію (імена користувачів, паролі, дані облікового запису). Вішинг (голосовий фішинг) використовується злочинцями під час телефонних дзвінків, щоб видавати себе за представників банку, переконуючи людей надати конфіденційну інформацію.
2.	Скімінг банкоматів	Злочинці встановлюють скімінгові пристрої на банкоматах, щоб отримати інформацію про картку та PIN-коди користувачів, після чого викрадені дані використовуються для здійснення несанкціонованих транзакцій або створення клонованих карток.
3.	Захоплення облікового запису	Хакери отримують несанкціонований доступ до онлайн-банківського рахунку клієнта, що дозволяє їм здійснювати несанкціоновані транзакції або змінювати дані рахунку.
4.	Атаки програм-вимагачів	Шкідливе програмне забезпечення використовується для шифрування критично важливих даних банку, а за ключ дешифрування вимагається викуп, що впливає на хід банківських операцій та безпеку конфіденційної інформації клієнтів.
5.	Шахрайська експлуатація мережі SWIFT	Ініціювання шахрайських транзакцій або маніпуляція фінансовими повідомленнями для переказу коштів на неавторизовані рахунки в мережі SWIFT.
6.	Внутрішні загрози	Незадоволені співробітники або інсайдери, які мають доступ до конфіденційної інформації та можуть вчинити шахрайські дії, що призводять до розкрадання або витоку даних клієнтів.
7.	Компроміс ділової переписки через електронну пошту	Шахраї компрометують або видають себе за високопоставлених керівників у банку, щоб обманом змусити працівників ініціювати банківські перекази або надати конфіденційну фінансову інформацію.
8.	Крадіжка кредитної картки	Викрадені дані кредитної картки використовуються для здійснення неавторизованих транзакцій, які передбачають великі покупки або зняття грошей із банкоматів.
9.	Несанкційний доступ до персональних даних	Кіберзлочинці отримують несанкціонований доступ до великих баз даних банків із інформацією про клієнтів, яку використовують для подальших шахрайств.
10.	Порушення аутентифікації	Низький рівень аутентифікації або погано реалізовані протоколи безпеки можуть бути використані зловмисниками для отримання несанкціонованого доступу до банківських систем або облікових записів клієнтів.
11.	Шахрайство через мобільний банкінг	Шахраї використовують уразливості мобільних банківських застосунків або здійснюють фішингові атаки, націлені на користувачів мобільних пристроїв, щоб отримати доступ до конфіденційної фінансової інформації.
12.	Фальшиві банківські програми та веб-сайти	Зловмисники створюють фальшиві мобільні застосунки або веб-сайти, які імітують реальні банки, щоб обманом змусити користувачів ввести свої облікові дані, що призводить до вразливості облікового запису.

Джерело: складено авторкою на основі [25; 18; 24]

Порушення політики безпеки виявилося найменшою проблемою для сучасних фінансових та страхових орагнізацій.

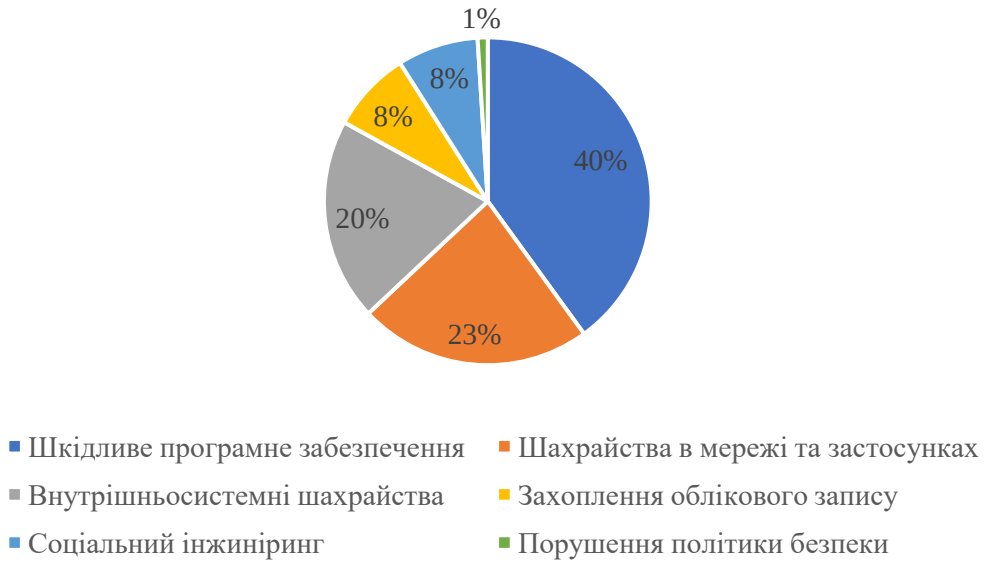


Рисунок 1.1 – Розподіл за типами найпоширеніших кібершахрайств на фінансові та страхові організації по всьому світу з жовтня 2021 року по вересень 2022 року

Джерело: складено авторкою на основі [40]

З метою мінімізації ризику втрат, пов’язаних із перерахованими кібершахрайствами, банки вкладають значні кошти в заходи кібербезпеки, включаючи шифрування, удосконалення багатофакторної аутентифікації, навчання співробітників і постійний моніторинг підозрілих дій. Клієнтів також закликають залишатися пильними, використовувати безпечні паролі, вмикати багатофакторну автентифікацію та негайно повідомляти про будь-які підозрілі дії із особистими акаунтами своїм банкам [11].

У 2022 році в усьому світі було зареєстровано 1829 інцидентів кібершахрайств у фінансовій галузі, порівняно з 2527 у попередньому році (рис. 1.2).

Рисунок 1.2 – Загальна кількість випадків кібершахрайств у фінансовій сфері, в тому числі випадки кібершахрайств, які супроводжувались витоком даних у світі протягом 2013-2022 років

Джерело: складено авторкою на основі [40]

З огляду на представлений графік, протягом 2013-2022 років загальна кількість випадків кібершахрайств у фінансовій сфері зросла на 46,8% (з 856 випадків у 2013 році до 1829 випадків у 2022 році). Найнижчий рівень кількості кібершахрайств у фінансовій сфері спостерігався у 2017 році (598 випадків). Відповідно, випадки кібершахрайств, які супроводжувались витоком даних протягом представленого періоду змінювалася пропорційно до попереднього показника. Проте, варто зазначити, що у відсотковому співвідношенні найбільша кількість випадків кібершахрайств, які супроводжувалися витоком даних у фінансовій сфері, відбулася у 2020 році (64,8%). Протягом 2021-2022 років кількість подібних кібершахрайств не перевищує 28%, що свідчить про покращення рівня кіберзахисту у фінансовому секторі.

Підвищенню рівня кібербезпеки у фінансовій сфері сприяє впровадження ряду нормативно-регулятивних заходів у світі [16]:

– Стандарти безпеки даних в індустрії платіжних карток (*Payment Card Industry Data Security Standards, PCI DSS*) – це набір стандартів безпеки, розроблений для індустрії платіжних карток, мета яких сприяти зменшенню шахрайства з кредитними картками та захисту конфіденційної інформації власників кредитних карток. Фінансові організації, що видають кредитні картки, зобов'язані дотримуватися даних стандартів, щоб захистити безпеку транзакцій із кредитними картками;

– Директива про платіжні послуги 2 (*Payment Services Directive, PSD 2*) – це Директива Європейського Союзу, яка сприяє підтримці конкуренції в банківському секторі та є стандартом безпеки фінансових даних, розроблений у межах попереднього стандарту . PSD 2 містить стандарти для захисту онлайн-платежів, посилення безпеки даних клієнтів і надійної аутентифікації клієнтів;

– Національний інститут стандартів і технологій (NIST) – це американська версія Міжнародного інституту стандартизації (ISO), яка надає широкий спектр вимог до інформаційної безпеки, включаючи відповідність кібербезпеці у фінансовій сфері;

– ISO/IEC 27001 є загальновизнаним у всьому світі стандартом для зниження ризиків безпеки та захисту інформаційних систем, визнаний набір політик і процесів безпеки, які визначають, як покращити рівень безпеки компанії в будь-якій галузі, у тому числі у фінансовій сфері;

– Закон Сарбейнса-Окслі (SOX) був прийнятий Конгресом Сполучених Штатів (США) у 2002 році. Даний закон передбачає забезпечення захисту інвесторів від фінансового шахрайства. Завдяки набору внутрішніх перевірок структура SOX забезпечує рекомендовані процедури безпеки для уникнення шахрайської фінансової діяльності;

– Закон Гремма–Ліча–Блайлі (GLBA), США, передбачає наступне: фінансові установи зобов'язані захищати дані споживачів і повністю розкривати клієнтам усі методи обміну даними, а також створити засоби контролю безпеки, щоб захистити інформацію клієнтів від будь-яких подій, які загрожують цілісності та безпеці даних відповідно до цього закону США;

– Загальний регламент Європейського Союзу про захист даних (*European Union's General Data Protection Regulation, EU-GDPR*) – це документ, який призначений для запобігання поширення особистих даних громадян. Найвищий пріоритет захисту відповідно до даного регламенту мають наступні види даних: аплікаційні форми на веб-сайтах, дані файлів cookie, які збираються від відвідувачів веб-сайту, розсилка рекламних листів, відстеження IP-адрес, розміщення зображень або особистої інформації про людину на веб-сайті.

З розвитком та впровадженням цифрових інновацій у фінансовому секторі проблема поширення кібершахрайств постійно актуалізується і потребує все нових рішень, тому важливо постійно вести моніторинг потенційних кіберзагроз для уникнення негативних наслідків їхнього впливу.

1.2 Систематизація існуючих теоретичних підходів щодо розгляду кібершайхраств у банках

Під час дослідження поточного стану опрацювання питань пов’язаних із кібершахрайством в банках необхідно провести комплексний аналіз існуючих наукових робіт у даній сфері, які дозволяють отримати уявлення про історію походження кібершахрайств, типи кіберзагроз, найпопулярніші технологічні вразливості, нормативний ландшафт, вплив кіберзагроз на зацікавлених суб’єктів, заходи із кібербезпеки тощо. Розуміння цих аспектів дозволить отримати загальну картину розвитку кібершахрайства насьогодні і дозволить фінансовим установам та іншим дослідникам спільно відшукати дієві способи захисту цілісності інформації в банківському секторі.

Станом на листопад 2023 року в авторитетній міжнародній науковій базі даних Scopus за запитом із ключових слів «cyber» та «frauds» (з англ. «кібершахрайства») отримано 1262 документи, в тому числі 547 матеріалів конференцій, 451 статтю, 119 розділів книг, 58 анотацій виступів на конференції та інших наукових робіт. Результати запитів за ключовими словами «cyber frauds» та «banks» (від англ. «банки»

отримано всього 24 результати опублікованих наукових робіт, а у результаті поєднання ключових запитів «cyber scammer» (від англ. «кібершахрай») та «banks» - 25 наукових робіт відповідно. Тому було прийнято рішення більш детальніше зупинитись на результатах отриманих за допомогою ключових слів «cyber» та «frauds».

За допомогою спеціальних аналітичних інструментів бази даних Scopus можна проаналізувати динаміку зміни кількості опублікованих наукових робіт (обмеживши пошуковий запит при цьому лише до матеріалів конференцій та статей, 997 документів) (рис. 1.3).

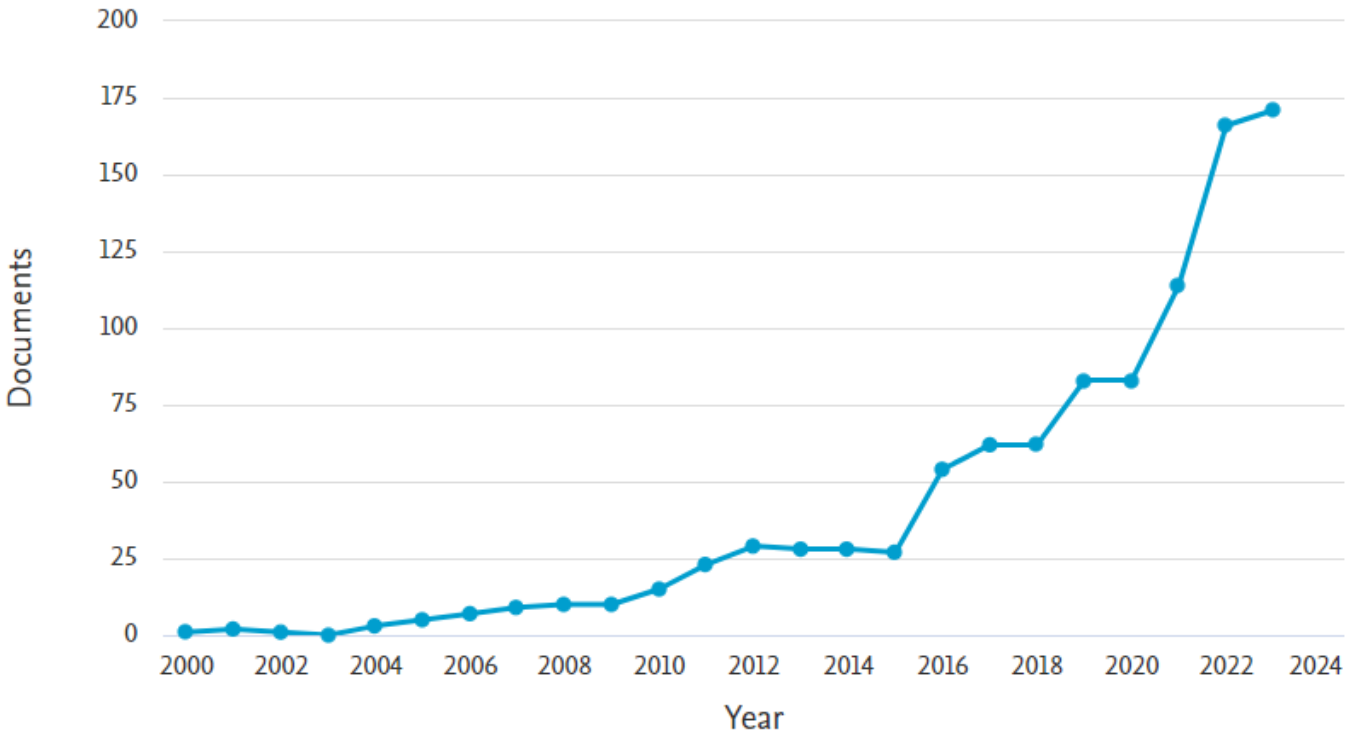


Рисунок 1.3 – Динаміка кількості опублікованих матеріалів конференцій та статей за ключовими словами «cyber» та «frauds» в міжнародній базі Scopus протягом 2000-2023 років

Джерело: складено авторкою на основі [61]

Як видно із графіка на рисунку 1.3 протягом 2000-2023 років зацікавленість міжнародної наукової спільноти до теми пов’язаної із кібершахрайствами зростала, особливо відчутний стрибок публікаційної активності спостерігається, починаючи із

2010 року. Протягом 2010-2023 років кількість опублікованих наукових праць із тематики кібершахрайств збільшилась більше ніж на 100%. У 2021 році кількість робіт перевищила позначку 100 в рік і в кожному наступному році ця кількість продовжує збільшувати, що свідчить про підвищений інтерес наукової спільноти до питань пов'язаних із кібершахрайствами.

Особливу зацікавленість викликає географічна структура представлених наукових публікацій у досліджуваній сфері (рис. 1.4).

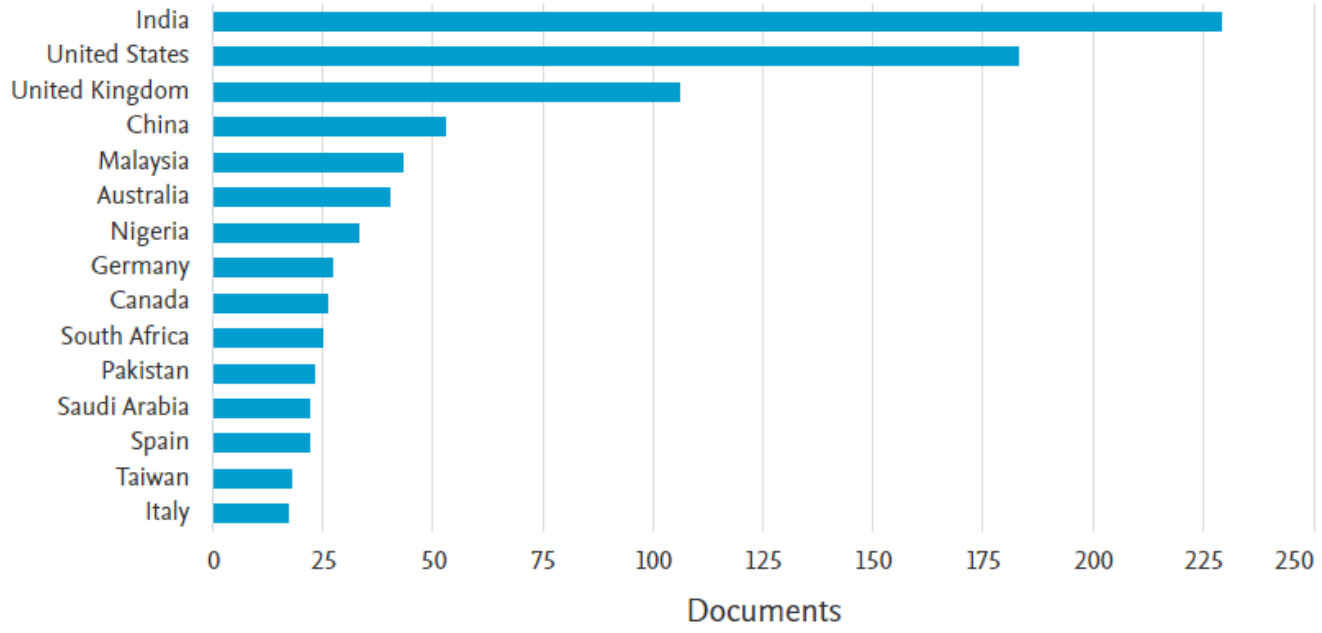


Рисунок 1.4 – Географічна структура опублікованих матеріалів конференцій та статей за ключовими словами «cyber» та «frauds» в міжнародній базі Scopus протягом 2000-2023 років

Джерело: складено автором на основі [61]

Найбільша кількість опублікованих матеріалів конференцій та статей із теми «кібершахрайство» належить науковцям із Індії (229 робіт), США (183 роботи) та Великої Британії (106 робіт). За цими країнами-лідерами йде група країн, кількість публікацій яких знаходиться в проміжку від 25 до 75 (Китай, Малайзія, Австралія, Нігерія, Німеччина, Канада та Південно-Африканська республіка). З огляду на представлений топ-15 країн, не можна окремо виділити регіони світу, де проблема

кібершахрайства є більш популярною, що свідчить про глобальний інтерес світової наукової спільноти до даної тематики. Це також підтверджується спектром галузей, в межах яких проводяться дослідження за напрямком вивчення природи кібершахрайств (рис. 1.5).

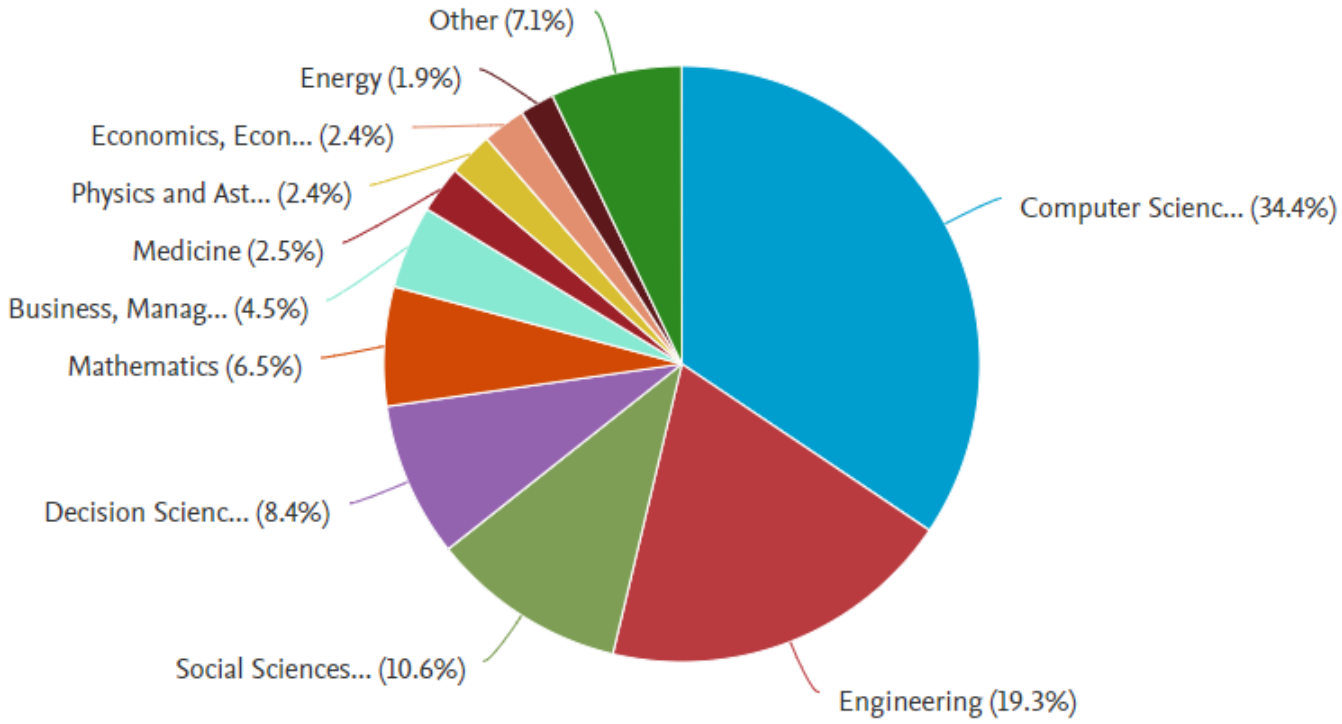


Рисунок 1.5 – Галузева структура опублікованих матеріалів конференцій та статей за ключовими словами «cyber» та «frauds» в міжнародній базі Scopus протягом 2000-2023 років

Джерело: складено автором на основі [61]

Представлена на рисунку 1.5 сегментна діаграма демонструє, що найбільше робіт із теми «кібершахрайства» опубліковано за наступними предметними галузями:

– комп’ютерні науки (34,4%);
– інженерія (19,3%);
– соціальні науки (10,6%);
– наука про рішення (8,4%);
– математика (6,5%).

При цьому у сферах бізнесу та менеджменту опубліковано 4,5% наукових робіт на тему «кібершахрайства», а у сфері економіки – 2,4%. Більш детальний аналіз актуальних наукових робіт, які мають відношення до теми «кібершахрайства» та формують узагальнену картину теоретичного підґрунтя, дозволяє провести спеціалізований програмний продукт VOSviewer. Даний продукт є потужним інструментом для аналізу комбінацій ключових слів, які використовуються в наукових публікаціях за обраною темою, та дозволяє сформувати із них кластери, що дає можливість візуалізувати та систематизувати вектори наукових досліджень.

Після додаткових налаштувань в програмному середовищі VOSviewer на основі вивантаженого із бази даних Scopus масиву опублікованих матеріалів конференцій та статей за ключовими словами «cyber» та «frauds» отримано наступну карту понять, які найчастіше зустрічаються в поєднанні із даними ключовими словами (рис. 1.6).

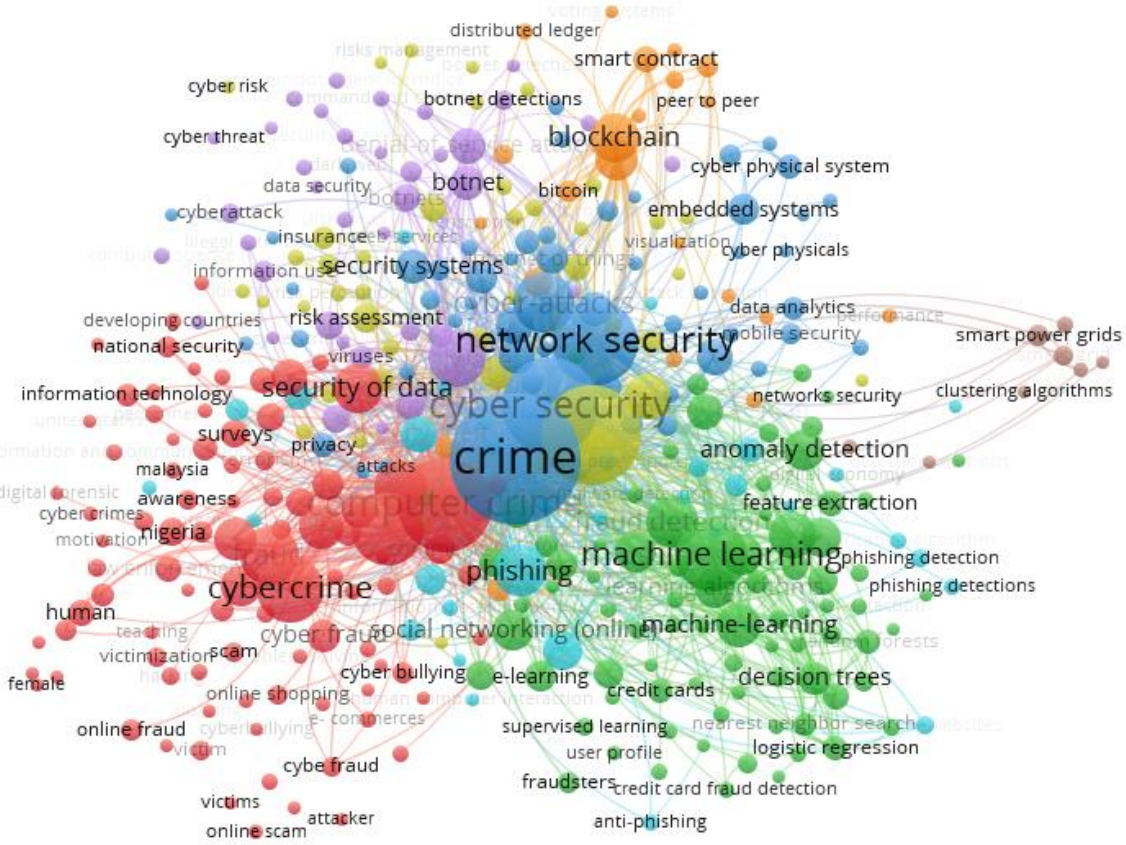


Рисунок 1.6 – Розподіл наукових публікацій за тематикою «кібершахрайства» за кластерами в міжнародній базі Scopus

Джерело: складено автором на основі [61]

Провівши аналіз представленої карти понять, можна виділити вісім кластерів. Елементи кластерів у формі куль позначають конкретне поняття. Від того на скільки часто в наукових роботах згадується те чи інше поняття залежить діаметр кулі. У перший кластер (червоний) увійшли поняття більшою мірою пов'язані із кримінальною складовою кібершахрайств, оскільки найчастіше зустрічаються поняття «комп'ютеризований кримінал», «кіберкримінал», «закон та легалізація», «кримінальна діяльність», «цифрова криміналістика» тощо. Зв'язок із кібершахрайствами у фінансовій сфері в даному кластері представлені за рахунок представлених понять «електронна комерція», «онлайн шопінг», «фінансовий кримінал», «відмивання грошей», «онлайн банкінг».

Другий за величиною кластер (зелений) містить в центрі такі поняття, як «машинне навчання», «алгоритми навчання», «нейромережі», «системи навчання», «виявлення шахрайств», «соціальний нетворкінг», «поведінкові аспекти». Це свідчить про те, що під час дослідження теми кібершахрайств активно використовуються технології машинного навчання та необхідно враховувати поведінкові аспекти суб'єктів, що можуть здійснювати кібершахрайства. Зі сфери фінансового сектору в даному кластері з'являються такі поняття: «кредитні картки», «фішинг», «фінансові транзакції».

Третій кластер (синій) містить в центрі поняття, які найбільше пов'язані із забезпеченням кібербезпеки: «кібербезпека», «системи контролю», «мережева безпека», «системи безпеки», «хмарні обчислення», «безпекові загрози». Зі сфери фінансового сектору в синьому кластері з'являються такі поняття: «фінансова інформація», «електронні гроші».

Решта виділених п'ять кластерів є значно меншими за попередні три розглянуті. Проте, варто зазначити, що у четвертому (жовтому) кластері найчастіше зустрічаються поняття із фінансової сфери, які безпосередньо пов'язані із банківською діяльністю – «банківська система», «крадіжка кредитної картки», «електронний банкінг», «мобільний банкінг», «фінтех», «фінансова інклюзія». Це підтверджує тісний зв'язок кібершахрайством та банківською діяльністю.

Наступні чотири кластери (фіолетовий, блакитний, помаранчевий, коричневий) присвячені прикладам конкретних кібершахрайств.

Для того, щоб зрозуміти поточний стан розвитку кібершахрайства в банках, важливо дослідити її історичні корені. Ранні випадки банківського шахрайства передусім включали фізичні порушення та традиційні методи, поступово переходячи до більш складних кібертехнік [57, 8, 45, 37, 22]. Розуміння цієї еволюції створює контекст для сучасних викликів і інформує про стратегії подолання кіберзагроз [35, 69, 53].

Література розкриває різноманітні методи кібершахрайства, націлених на банки, включаючи фішинг [59, 47, 33, 29], атаки зловмисного програмного забезпечення [31, 49], крадіжки особистих даних та кредитних карток [19, 10, 3] і програми-вимагачі [42]. Кожен метод використовує різні вразливості в банківській системі, що вимагає багатогранного підходу для протидії цим загрозам. Повне розуміння цих методів має вирішальне значення для розробки ефективних профілактичних заходів [41].

Оскільки банки впроваджують все більш складні технології, вони стають більш ефективними та вразливими до кібератак. У літературі висвітлюються вразливості, пов’язані з платформами онлайн-банкінгу, мобільними додатками, використання блокчейн технологій [13, 56, 58] та хмарними службами [14]. Вивчення цих технологічних слабких місць є обов’язковим для розробки надійних стратегій кібербезпеки. Крім того, важливу роль у кібервразливості фінансових систем відіграють поведінкові аспекти суб’єктів фінансового ринку [2].

Нормативно-правове регулювання відіграє важливу роль у формуванні практик кібербезпеки банків [60]. У роботах [30, 20] досліджуються існуючі нормативні рамки, спрямовані на захист фінансових установ від кіберзагроз. Аналіз ефективності цих нормативних актів дає змогу зрозуміти потенційні сфери для покращення боротьби з кібершахрайством.

У літературі постійно наголошується на далекосяжних наслідках кібершахрайства для різних зацікавлених сторін, включаючи банки, клієнтів та економіку в цілому [52, 46, 39, 6]. Фінансові втрати, репутаційні збитки та підрив

довіри є звичайними результатами впливу кібершахрайств. Розуміння впливу на зацікавлених сторін має важливе значення для розробки профілактичних заходів для запобігання та подолання кібершахрайства [50, 12, 48].

Дослідники ретельно досліджували заходи кібербезпеки, які використовують банки для захисту від кібершахрайства. У своїх роботах [4, 23, 9, 36, 38, 34] вчені аналізують ефективність шифрування, багатофакторної аутентифікації, штучного інтелекту, біометричних засобів та інших технологічних рішень [5]. Оцінка сильних сторін і обмежень цих заходів сприяє розробці надійних структур кібербезпеки.

Ландшафт кібершахрайства динамічний, у ньому постійно з’являються нові загрози та принципи їх виявлення. Огляд літературних джерел підтверджує актуальність використання наступних технологій: нейромереж [44, 17, 7] для систематизованої обробки великих даних у сфері банківського бізнесу останні тенденції, такі як зростання дипфейків, атаки на основі штучного інтелекту та роль темної мережі [43] для передбачення майбутніх викликів дозволяє банкам випереджати кіберзлочинців і завчасно усунути потенційні вразливості.

Варто відзначити ряд вітчизняних вчених, які також приділяють увагу питанням виявленню кіберзагроз в банках та можливостям усунення негативних наслідків: Яровенко Г. [71, 73, 72], Годнюк І. [26], Дубина М. [62], Чучко С. [70], Кришевич [68], Коваль [67], Коваленко [65, 64, 63], Гриценко К. [28]

Проведена систематизація існуючих теоретичних підходів щодо розгляду теми кібершахрайств у фінансовій сфері в цілому та в банках зокрема дозволяє актуалізувати дану роботу та створює підґрунтя для проведення подальших досліджень і вирішення нових наукових задач.

1.3 Постановка завдання моделювання

Теоретичні засади дослідження та систематизація існуючих підходів до розгляду кібершайхраств у банках, можна сформувати основні завдання в контексті цієї роботи.

Метою представленої роботи є розробка підходу щодо моделювання імовірної поведінки дій інсайдерів-кібершахраїв у банках. Об’єктом дослідження є процес оцінки поведінки інсайдерів-кібершахраїв у банках на основі ключових інтернет-запитів. Предметом дослідження є математичні методи та моделі оцінки поведінки інсайдерів-кібершахраїв у банках.

Для проведення даного дослідження було обрано наступні методи: метод головних компонент для відбору найбільш релевантних запитів; кластерний аналіз методом методом k-середніх для формування потенційних «портретів» інсайдерів-кібершахраїв у банках; асоціативний аналіз для побудови асоціативних правил, які дозволяють зрозуміти потенційну поведінку інсайдерів-кібершахраїв.

Завдання моделювання у межах досліджуваної предметної галузі представлено в таблиці 1.2.

Таблиця 1.2 – Формулювання проблеми моделювання імовірної поведінки дій інсайдерів-кібершахраїв у банках

Елементи	Описання
Проблема	Моделювання імовірної поведінки дій інсайдерів-кібершахраїв у банках
Впливає на	Діяльність банку та відповідних регулятивних органів у питаннях виявлення кібершахрайств у банках, які здійснюються інсайдерами
Результатом чого є	Розробка науково-методичного підходу щодо моделювання імовірної поведінки дій інсайдерів-кібершахраїв у банках
Переваги моделі	Аргументований список вхідних показників; відкритий та зрозумілий алгоритм відбору релевантних змінних; високий ступінь наочності та візуалізації представлених результатів; можливість прогнозування поведінки інсайдера-кібершахрая в банку у майбутньому

Джерело: складено авторкою

2. ПОБУДОВА МАТЕМАТИЧНОЇ МОДЕЛІ ЙМОВІРНОЇ ПОВЕДІНКИ ДІЙ ІНСАЙДЕРІВ-КІБЕРШАХРАЇВ У БАНКУ

2.1 Опис вхідних даних для побудови моделі

Інсайдери-кібершахраї в банках використовують різні тактики та демонструють певну поведінку для здійснення своєї незаконної діяльності. Розуміння цих ключових аспектів може допомогти окремим особам і організаціям краще захистити себе від кіберзагроз.

Основна небезпека кібершахраїв, які діють як інсайдери в банку, полягає в їхньому потенціалі використовувати свій привілейований доступ і знання внутрішніх систем і процесів банку. Інсайдерські загрози можуть становити значні ризики для безпеки та цілісності фінансових установ. Серед ключових загроз можуть бути наступні: порушення даних і крадіжка; неавторизований доступ до внутрішньої системи та конфіденційних даних клієнтів, фінансових записів та іншої конфіденційної інформації; крадіжка даних; фінансове шахрайство; інсайдерська торгівля; саботаж і порушення; пошкодження даних; відмивання грошей; зловживання обліковими даними; соціальна інженерія та схеми шахрайства та ін. для того, щоб пом’якшити вплив негативних наслідків, пов’язаних з інсайдерськими загрозами, банкам необхідно запровадити надійні заходи кібербезпеки, включаючи контроль доступу, системи моніторингу та програми навчання співробітників. Регулярні аудити, репутація та культура обізнаності про безпеку також важливі для ефективного виявлення та запобігання внутрішнім загрозам.

В контексті поставленої мети даної роботи необхідно змоделювати імовірну поведінку інасайдерів-кібершахраїв у банку. Оскільки все, що має відношення до оцінки поведінкових аспектів людської діяльності носить більшою мірою суб’єктивний характер, основною складністю у проведенні подібних досліджень є підбір вхідних параметрів для цього. Передбачити стовідсотково як себе поведе людина в тій чи іншій ситуації, зокрема, інсайдер-кібершахрай банку не можливо так, як її поведінка обумовлюється рядом ендогенних та екзогенних кількісних та якісних

факторів, вплив яких дуже складно проаналізувати. Враховуючи характер потенційних шахрайських дій інсайдера-кібершахрая банку, в якості масиву вхідних змінних, які дозволять оцінити його можливу поведінку, запропоновано використовувати можливі комбінації пошукових запитів в пошуковій системі Google. Всього в якості основи формування вхідного масиву даних для представленого дослідження сформовано два списки пошукових запитів: список запитів характеристики кібератак (табл. 2.1) та список запитів, що характеризують рівень зменшення довіри до фінансових установ (табл. 2.2).

Таблиця 2.1 – Вхідний масив даних, який включає список запитів характеристики кібератак

Ум. позн.	Пошуковий запит (укр.)	Пошуковий запит (англ.)
var1	Номер кіберполіції	Cyber police number
var2	Номер поліції	Police number
var3	Що робити, коли тебе зламали	What to do when you are hacked
var4	Перші дії при кібератаці	How to respond to a cyber attack
var5	Як посилити захист комп'ютера	How to protect your computer
var6	Як не допустити злому персональних даних (сайту, соціальних мереж)	How to prevent hacking
var7	Найпоширеніші кібератаки	The most common cyber attacks
var8	Як виявити кібератаку	Detection of a cyber attack
var9	Як захистити себе від кібератак	How to protect yourself from cyber attacks
var10	Як зрозуміти, що комп'ютер (телефон) зламали	How to find that phone is hacked

Джерело: складено авторкою

Засобами внутрішньої надбудови пошукової системи Google, Google Trends [27], отримано результати частоти звернень користувачів мережі Інтернет за представленими щотижневими пошуковими запитами протягом останніх п'яти років з 2018 р. до 2023 р. Всі пошукові запити досліджувались для всього світу, тому було прийнято рішення задавати їх в Google Trends англійською мовою. Проаналізуємо частоту отриманих результатів за сформованими пошуковими запитами за допомогою графічного представлення.

Таблиця 2.2 – Вхідний масив даних, який включає список запитів, що характеризують рівень зменшення довіри до фінансових установ

Ум. позн.	Пошуковий запит (укр.)	Пошуковий запит (англ.)
var11	Як заблокувати транзакцію	How to block a transaction
var12	Як заблокувати банківську карту	How to block a bank card
var13	Як змінити пароль на банківській картці	How to change password of bank card
var14	Як зменшити ліміт по банківській картці	How to reduce the credit limit
var15	Як зменшити ліміт розрахунків в інтернеті	Management of online payments
var16	Який банк найбільш захищений (в Інтернеті)	Which bank is the most secure online
var17	Рейтинг надійних банків (або рейтинг найбільш кіберстійких банків)	The most reliable banks
var18	Номер підтримки банку (або номер кол-центру банку)	Bank call center number
var19	Як змінити обслуговуючий банк (як перевести виплату зарплати з одного банку на інший)	How to change the bank
var20	Чорний список користувачів	Black list of customers

Джерело: складено авторкою

На рисунку 2.1 представлено динаміку запитів «Cyber police number», «Police number» та «What to do when you are hacked».

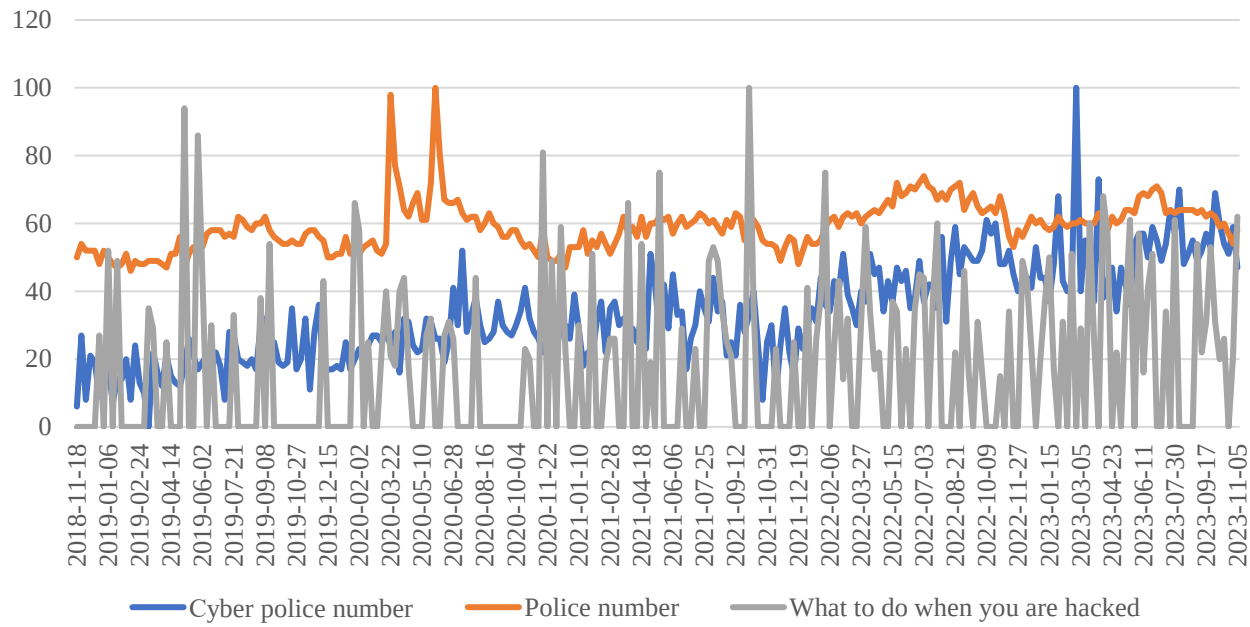


Рисунок 2.1 – Динаміка запитів «Cyber police number», «Police number» та «What to do when you are hacked» протягом 2018-2023 рр.

Джерело: складено авторкою на основі [27]

З огляду на представлений графік запити «Cyber police number» та «Police number» не втрачали популярності протягом всього досліджуваного періоду. Варто зазначити, що запит «Cyber police number» продовжує набирати популярності (на рис. 2.1 це підтверджується висхідним характером графіку), оскільки, починаючи із кінця 2022 року, він вперше за п’ять років перевищив за популярністю запит «Police number» і досягнув максимального значення (100 запитів на тиждень) в кінці лютого 2023 року. Це підтверджує актуалізацію проблему поширення кібершахрайств та потребу в усуненні їх наслідків. Щодо результатів для третього пошукового запиту, «What to do when you are hacked», то характер його динаміки носить стрибкоподібний характер і проте варто зазначити, що частота подібного запиту у світі є високою (близько 100 запитів на тиждень), що також підтверджує потребу населення в усуненні негативних наслідків кібератак власними зусиллями.

На наступному графіку (рис. 2.2) представлено динаміку зміни наступних трьох запитів зі списку запитів характеристики кібератак.

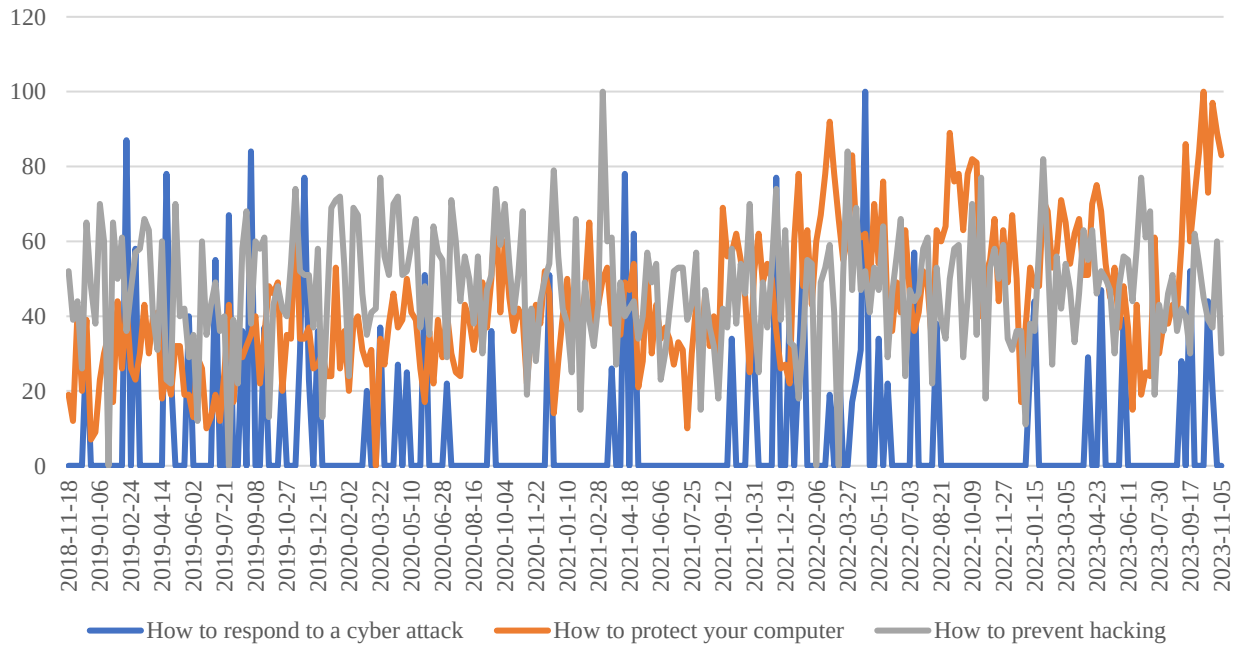


Рисунок 2.2 – Динаміка запитів «How to respond to a cyber attack», «How to protect your computer» та «How to prevent hacking» протягом 2018-2023 рр.

Джерело: складено авторкою на основі [27]

Активність пошукових запитів «How to prevent hacking» та «How to protect your computer» протягом досліджуваного періоду демонструють постійно високу популярність серед користувачів пошукової системи Google у світі. Крім того, людей більше цікавить питання як посилити захист комп'ютера в цілому і інтерес до даного питання почав активно зростати із кінця 2022 року. Щодо результатів частоти пошукового запиту «How to respond to a cyber attack», то тут досить схожа ситуація із пошуковим запитом «What to do when you are hacked», оскільки він також носить стрибкоподібний характер проте при цьому досягає пікових значень (близько 100 запитів на тиждень).

Аналіз результатів наступної пари пошукових запитів зі списку запитів характеристики кібератак зображено на наступному графіку (рис. 2.3).

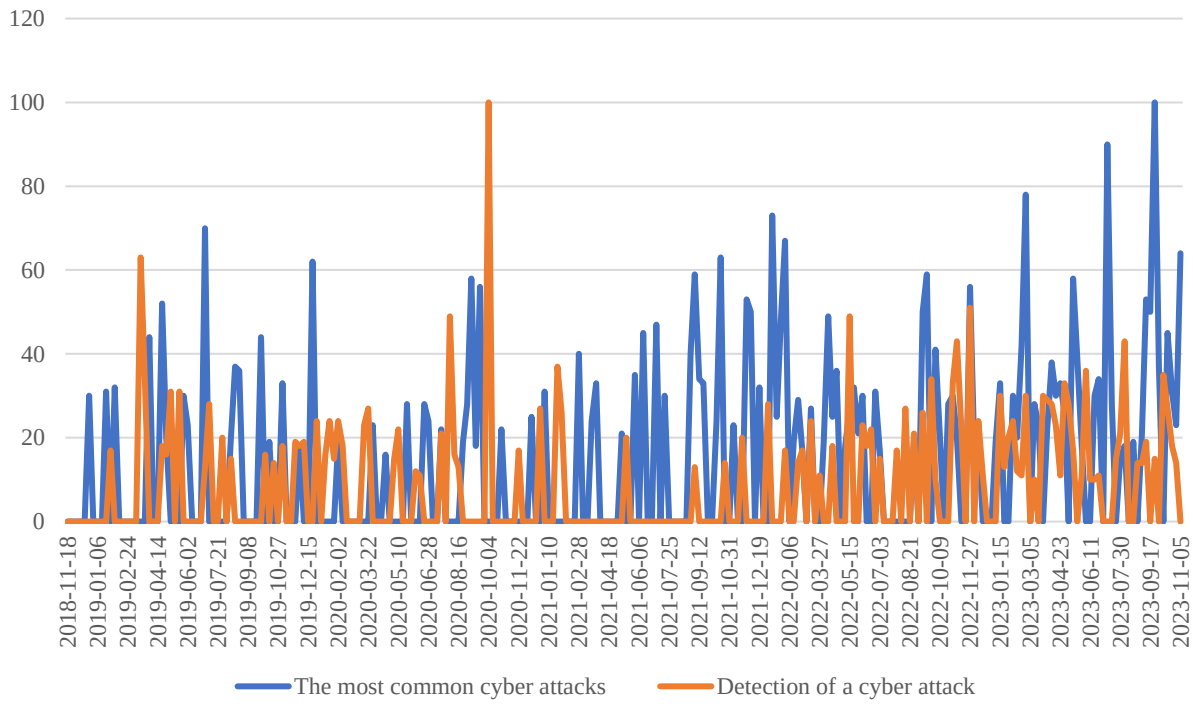


Рисунок 2.3 – Динаміка запитів «The most common cyber attacks» та «Detection of a cyber attack» протягом 2018-2023 рр.

Джерело: складено авторкою на основі [27]

Як бачимо, протягом 2018-2023 рр. тема найпоширеніших кібератак та способів їх виявлення є досить популярною і коливається в середньому від 10 до 60 запитів на

тиждень. При цьому варто відзначити, що активність пошукового запиту серед користувачів Google за пошуковим запитом «The most common cyber attacks» є вищою ніж за запитом «Detection of a cyber attack». Це все пояснюється тим, що питанням найпоширеніших кібератак займаються представники різних напрямків діяльності – від науковців до журналістів. Крім того, з початку 2022 року кількість розглянутих пошукових запитів почала популяризуватись. Максимальне значення, 100, за пошуковим запитом «Detection of a cyber attack» було отримане у квітні 2020 року, а «The most common cyber attacks» – у середині вересня 2023 року.

Остання пара пошукових запитів зі списку запитів характеристики кібератак, присвячених особистому захисту від кібератак і розумінню, що комп'ютер або телефон було зламано, зображено на наступному графіку (рис. 2.4).

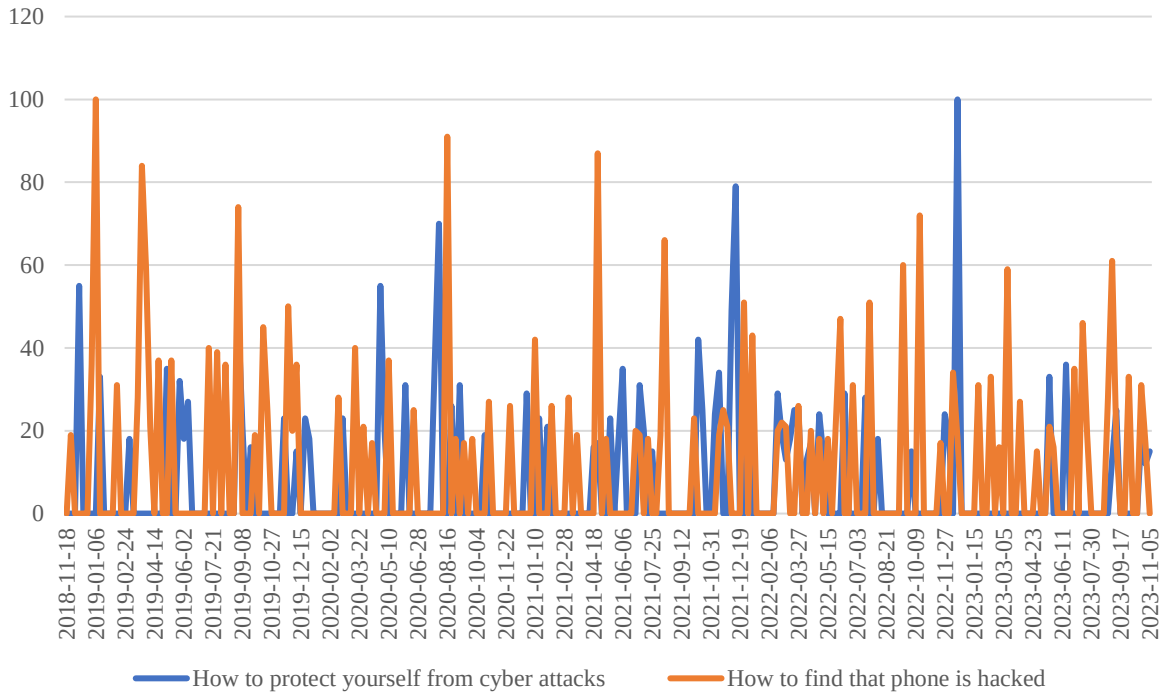


Рисунок 2.4 – Динаміка запитів «How to protect yourself from cyber attacks» та «How to find that phone is hacked» протягом 2018-2023 рр.

Джерело: складено авторкою на основі [27]

З огляду на представлений графік частота досліджуваних запитів протягом 2018-2023 рр. приблизно однакова і носит стрибкоподібний характер. Цікавим

спостереженням є те, що людей у світі більше цікавить питання як виявити факт ураження ком'пютера або телефона тією чи іншою кібератакою. Протягом останніх п'яти років спостерігалося мінімум чотири тижні, коли кількість запитів «How to find that phone is hacked» перевищувала 60.

Таким чином, серед пошукових запитів зі списку запитів характеристики кібератак стабільну популярність протягом 2018-2023 рр. мають наступні пошукові запити: «Cyber police number», «Police number», «How to protect your computer» та «How to prevent hacking».

Проаналізуємо детальніше динаміку пошукових запитів із другого списку, який бере участь у дослідженні. На графіку 2.5 представлена динаміка перших трьох запитів із даного списку (рис. 2.5).

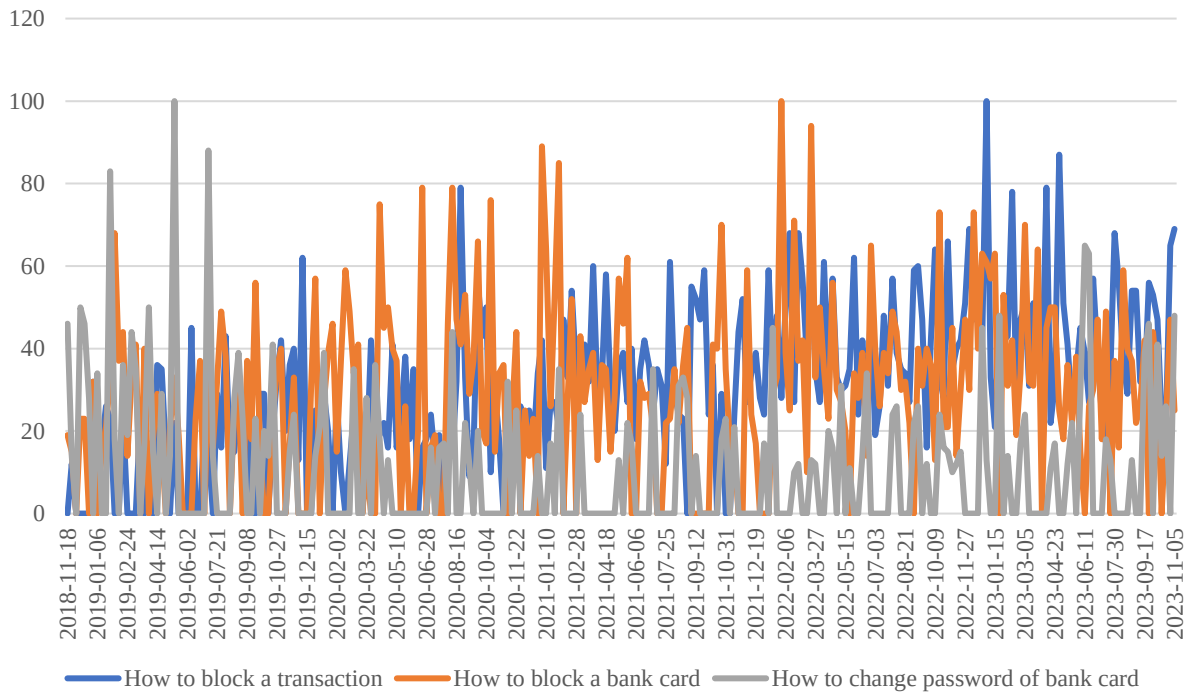


Рисунок 2.5 – Динаміка запитів «How to block a trasaction», «How to block a bank card» та «How to change password of bank card» протягом 2018-2023 рр.

Джерело: складено авторкою на основі [27]

Частота пошукового запиту, який стосується зміни пароля від банківської картки дещо знизилась у 2022-2023 роках у порівнянні до 2018-2019 років. Однак, незважаючи на це, запити «How to block a trasaction» та «How to block a bank card»

демонструють позитивну динаміку, що означає підвищений інтерес суспільства до проблеми збереження особистих банківських даних, пошкоджених імовірніше за все за рахунок кібершахрайства з огляду на результати попереднього блоку поушквих запитів.

Результати за наступними трьома пошуковими запитами представлені на графіку (рис. 2.6).

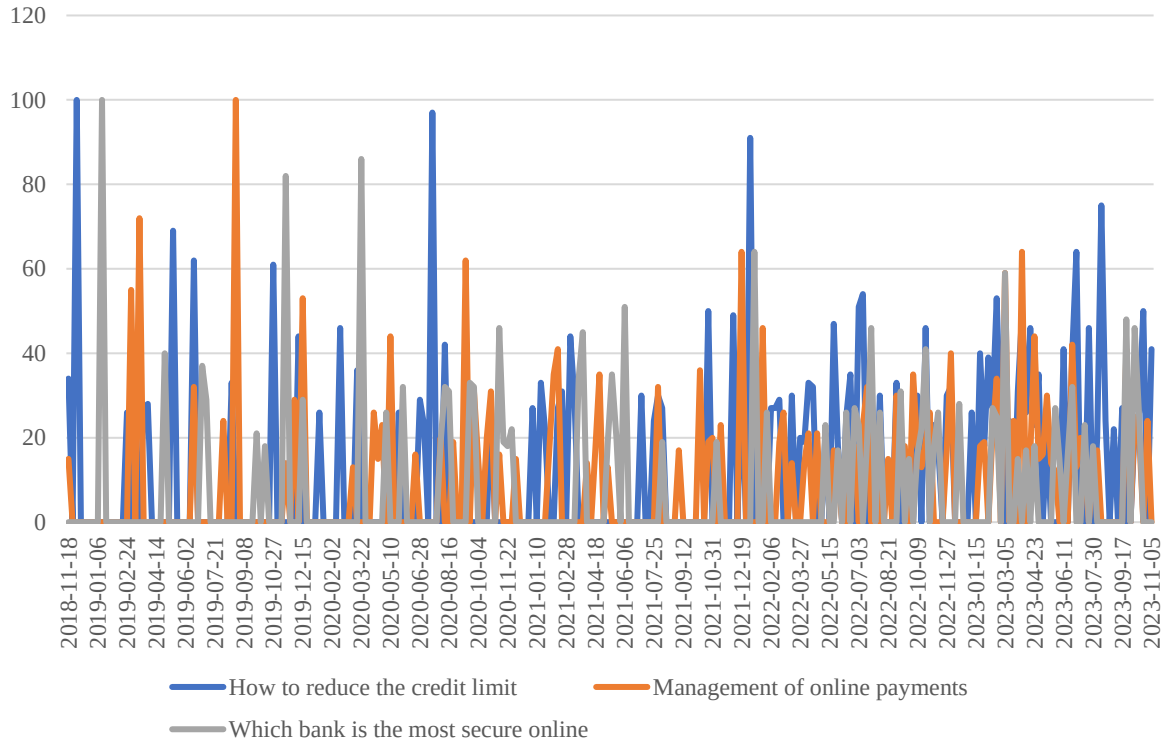


Рисунок 2.6 – Динаміка запитів «How to reduce the credit limit», «Management of online payments» та «Which bank is the most secure online» протягом 2018-2023 рр.

Джерело: складено авторкою на основі [27]

Серед представленої трійки пошукових записів найвищу популярність має пошуковий запит «How to reduce the credit limit». Протягом досліджуваного періоду даний пошуковий запит досить часто з'являвся серед користувачів Google більше 60 разів на тиждень, особливо у період з 2018 до 2020 року. Два інші пошукові запити, які аналізуються на рисунку 2.6, мають приблизно однакову частоту у період 2021-2023 рр. До цього, починаючи із початку 2019 року і до весни 2020 року людей у світі особливо цікавило питання щодо найбільш захищеного банку в Інтернеті. Питання

управління онлайн-платежами особливо актуалізувалось з осені 2021 року, що свідчить про зростання популярності безготівкових розрахунків у світі.

Наступний аналіз пошукових запитів, що характеризують рівень зменшення довіри до фінансових установ, «The most reliable banks» та «Bank call center number», представлені на рисунку 2.7.

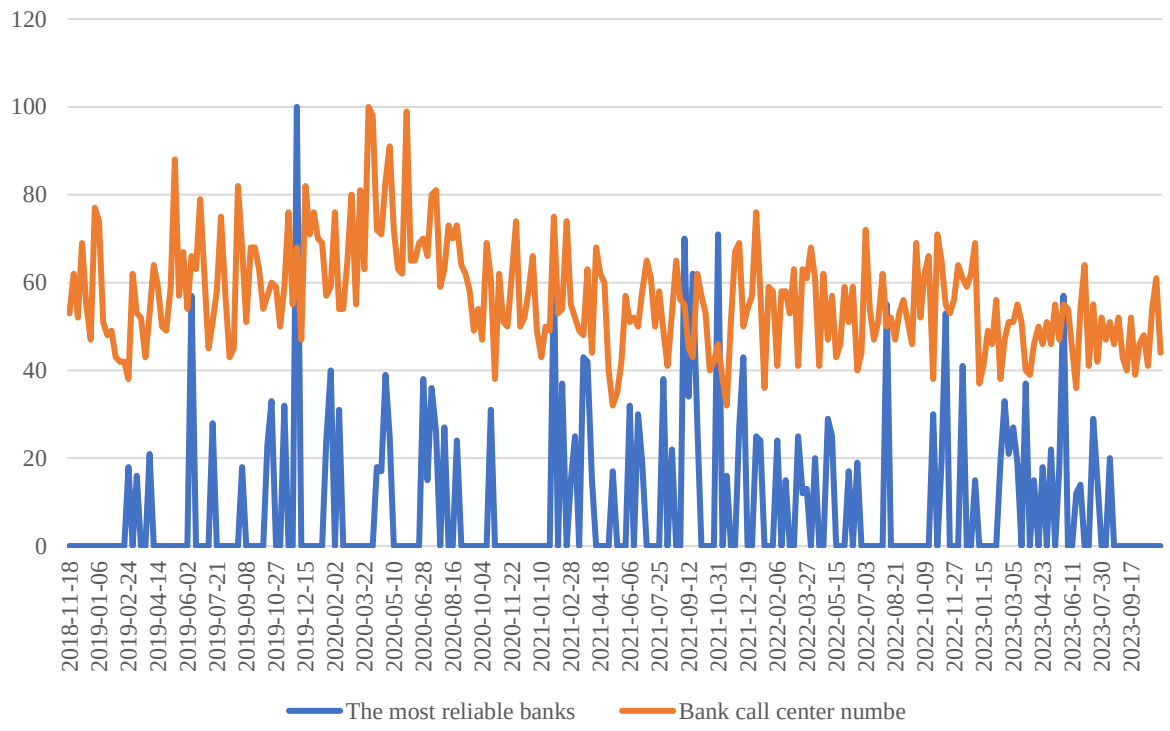


Рисунок 2.7 – Динаміка запитів «The most reliable banks» та «Bank call center number» протягом 2018-2023 рр.

Джерело: складено авторкою на основі [27]

Як бачимо із рисунку 2.7 частота пошукового запиту, який стосується номеру кол-центру банку, зменшувалась позначки 30 на тиждень протягом досліджуваного періоду. Пікові значення частоти використання запиту «Bank call center number» припадають на весну 2020 року. Після цього зацікавленість користувачів почала знижуватись. З осені 2020 по осінь 2022 року вона знаходилась приблизно на односу рівні (40-60 запитів на тиждень). Починаючи із кінця 2022 року кількість подібних заходів знизилась до рівня понад 40 запитів на тиждень. Питання визначення найбільш надійних банків також цікавило користувачів Google, однак говорити про

явно виражену тенденцію динаміки пошукового запиту «The most reliable banks» не можна, оскільки вона носить стрибкоподібний характер. Проте коливання частоти звернень за даним пошуковим запитом від 40 до 100 на тиждень свідчить про досить високий інтерес суспільства.

Остання пара пошукових запитів, які беруть участь у дослідженні, демонструє таку динаміку (рис. 2.8).

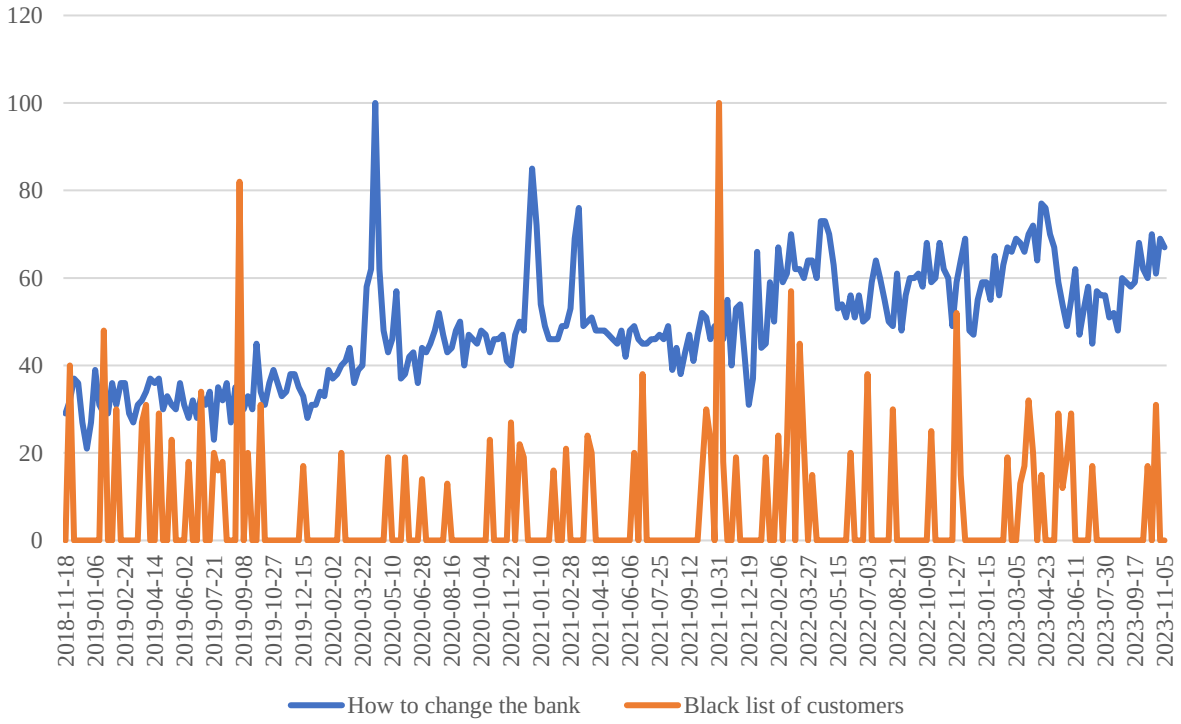


Рисунок 2.8 – Динаміка запитів «How to change the bank» та «Black list of customers» протягом 2018-2023 рр.

Джерело: складено авторкою на основі [27]

Синя лінія на графіку (рис. 2.8) позначає динаміку частоти запиту користувачів пошукової системи Google стосовно потреби зміни обслуговуючого банку. Як бачимо протягом 2018-2023 років частота запиту «How to change the bank» демонструє постійну тенденцію до збільшення. Крім того, із весни 2020 року до початку 2021 року спостерігались пікові значення (від 78 до 100 запитів на тиждень) за даним запитом. Щодо другого пошукового запиту, «Black list of customers», то можна сказати, що він не є особливо популярним на відміну від попереднього, оскільки

протягом останніх п’яти років користувачі Google досить нерегулярно здійснювали відповідний пошук. Причиною цього є стрибкоподібний характер динаміки даного пошукового запиту. Проте, варто також відзначити присутність на графіку пікових значень.

Таким чином, серед пошукових запитів зі списку запитів, що характеризують рівень зменшення довіри до фінансових установ, стабільну популярність протягом 2018-2023 рр. мають наступні пошукові запити: «How to block a trasaction», «How to block a bank card», «Bank call center number» та «How to change the bank».

2.2 Методологічне забезпечення моделювання ймовірної поведінки дій інсайдерів-кібершахраїв у банках

Моделювання ймовірної поведінки дій інсайдерів-кібершахраїв у банках здійснюватиметься у три етапи.

На першому етапі за допомогою методу головних компонент (*Principal Component Analysis*) буде сформовано масив найбільш релевантних для проведення подальшого дослідження змінних, отриманих зі списку 20 ключових запитів, що представлені у табл. 2.1 та 2.2.

Метод головних компонент – це статистичний метод, який використовується під час аналізу даних для зменшення розмірності даних, записаних у вигляді матриці (1) та виділення ключових компонент *Comp*.

$$X = \begin{matrix} x_{11} & x_{12} & \dots & x_{1j} & \dots & x_{1J} \\ x_{21} & x_{22} & \dots & x_{2j} & \dots & x_{2J} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ x_{i1} & x_{i2} & \dots & x_{ij} & \dots & x_{iJ} \end{matrix} \quad (1)$$

Основною метою даного методу є перетворення даних великої розмірності в представлення меншої розмірності, фіксуючи якомога більше відхилень у даних. Алгоритм методу головних компонент має наступну послідовність:

1. Центрування даних (віднімання середнього значення кожної змінної від кожного значення відповідного показника).

2. Обчислення коваріаційної матриці (коваріаційна матриця описує зв’язки між усіма парами змінних у даних).

3. Розкладання коваріаційної матриці на вектори власних значень, що представляють напрямки максимальної дисперсії в даних, а відповідні власні значення вказують на величину дисперсії вздовж цих напрямків.

4. Вибір основних компонентів супроводжується ранжуванням векторів власних значень компонент в порядку спадання. Власний вектор із найвищим власним значенням є першою головною компонентою, другий за величиною є другою головною компонентою і так далі.

5. Проектування даних на основні компоненти (початкові дані проектуються на вибрані основні компоненти, створюючи новий набір змінних (основних компонентів), які не корельовані та фіксують найважливішу інформацію в даних.

6. Оцінка факторних навантажень вхідних показників у межах виділених компонент.

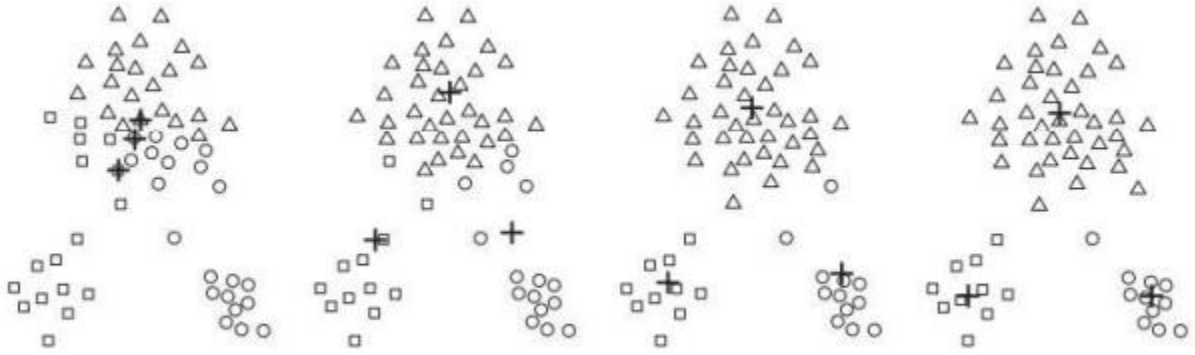
Визначившись із набором релевантних змінних на другому етапі моделювання необхідно провести кластеризацію методом *k*-середніх. Цей метод кластеризації був обраний для даного дослідження через свою популярність у використанні під час групування точок таким чином, щоб мінімізувати суму квадратів відстаней між точками даних і центроїдом кластера, до якого вони належать.

Алгоритм методу кластеризації *k*-середніх включає такі послідовні кроки:

1. Первинний вибір центрів попередніх *k* кластерів (вибір *k* змінних за умови визначення максимальної між ними відстані).

2. Первинний перерозподіл об’єктів між кластерами (принцип перерозподілу ґрунтується на визначенні мінімальної відстані між об’єктами).

3. Запуск ітераційного процесу, який триває до тих пір, доки не буде сформовано оптимальну структуру кластерів, а загальна кількість ітерацій дорівнюватиме максимальному числу (рис. 2.9).



Ітерація 1 Ітерація 2 Ітерація 3 Ітерація 4

Рисунок 2.9 – Схема кластеризації змінних за допомогою методу *k*-середніх

Джерело: складено авторкою на основі [15]

На третьому етапі загального дослідження передбачається побудова потенційних портретів інсайдерів-кібершахраїв у банках на основі відібраних змінних методом головних компонент та кластеризацією за допомогою методу асоціативного навчання [66].

Побудова асоціативних правил лежать в основі афінітивного аналізу (*affinity analysis*), суть якого полягає у виявленні взаємозв'язку між певними подіями, що можуть мати принципову обумовленість. Напрямки найчастішого використання методу асоціативних правил: формування кошику покупця в магазині за рахунок його особистих уподобань, оцінка рівня задоволеності клієнтів від використання тих чи інших послуг, формування профілю користувачів нового мобільного застосунку або веб-сайту, ідентифікація можливих побічних ефектів від вживання нового лікарського препарату тощо.

Загальний алгоритм моделювання за допомогою асоціативних правил включає наступні кроки:

1. Формування множини подій (транзакцій), які лежатимуть в основі моделювання.

2. Дослідження структури асоціативного правила, яке має включати умову (*antecedent*) та наслідок (*consequent*) (*X*=>*Y*).

3. Визначення основних характеристик асоціативного правила: підтримку (*support*), імовірність (*confidence*), ліфт (interest lift), левередж (leverage), доказ (*conviction*) та метрика Чжана (*zhangs_metric*).

Підтримка представляє собою набір транзакцій, які складаються із умови та наслідку (2).

$$S(X \to Y) = P(X \cap Y) = \frac{n(\{X;Y\} \in d_i)}{N}, \quad (2)$$

де N – загальний набір змінних.

d_i – конкретна транзакція із загальної кількості транзакцій D.

Імовірність у контексті асоціативного правила – це міра точності правила та дорівнює відношенню сукупної кількості транзакцій з умовою та наслідком до кількості транзакцій з умовою (3).

$$C(X \to Y) = P(X|Y) = \frac{n1(\{X;Y\} \in d_i)}{n1(\{X\} \in d_i)}. \quad (3)$$

Чим вищі значення підтримки та імовірності, тим вища імовірність того, що певна транзакція, яка містить умову, включатиме і наслідок.

Ліфт представляє собою відношення частоти умови та наслідку транзакції до частоти появи наслідку (чим більше значення, тим частіше умова обумовлює настання наслідку) (4).

$$L(X \to Y) = C(X \to Y)/P(Y). \quad (4)$$

У випадку, якщо ліфт рівний 1, то зв’язок між умовою та наслідком відсутній. Якщо значення близьке до 0, то присутній сильна зворотня залежність.

Левередж дорівнює різниці спостережуваної частоти, коли умова та наслідок ідентифікуються разом, і добутку частоти виявлення умови та наслідку (5).

$$T(X \to Y) = S(X \to Y) - P(X) * P(Y). \quad (5)$$

Доказ – це це міра, яка допомагає визначити чи випадково з'явилося правило (6). Високе значення доказу свідчить про те, що наслідок сильно залежить від умови. Якщо оцінка визначена ідеальною, то доказ визначається як «inf».

$$K(X \to Y) = \frac{1-S(Y)}{1-C(X \to Y)}. \quad (6)$$

Метрика Чжана (7) дозволяє визначити як асоціацію, так і дисоціацію. Значення коливається від -1 до 1. Позитивне значення вказує на асоціацію, а негативне значення вказує на дисоціацію.

$$Z(X \to Y) = \frac{C(X \to Y) - C(X` \to Y)}{Max[C(X \to Y), C(X` \to Y)]}. \quad (6)$$

4. Формулювання висновків на основі отриманих асоціативних правил.

Таким чином, в представленому підрозділі представлено комплексне методологічне забезпечення моделювання ймовірної поведінки дій інсайдерів-кібершахраїв у банках на основі поєднання трьох методів статистичного дослідження: методу головних компонент для ідентифікації релевантних змінних, метод кластеризації *k*-середніх для формування кластерів дослідження та метод асоціативних правил для побудови потенційних портретів інсайдерів-кібершахраїв у банках. Всі необхідні обчислення в роботі проводитимуться за допомогою програмного статистичного пакету Stata 18 та мови програмування Python 3.

3. ПРАКТИЧНА РЕАЛІЗАЦІЯ МОДЕЛІ ЙМОВІРНОЇ ПОВЕДІНКИ ДІЙ ІНСАЙДЕРІВ-КІБЕРШАХРАЇВ У БАНКАХ

3.1 Результати побудови комплексної моделі ймовірної поведінки дій інсайдерів-кібершахраїв у банках

Відповідно до визначеної послідовності етапів моделювання ймовірної поведінки дій інсайдерів-кібершахраїв у банках спочатку необхідно методом головних компонент відібрати найбільш релевантні змінні для проведення подальшого дослідження.

Проаналізуємо власні значення компонент, які отримані для 20 вхідних змінних (табл. 3.1) та графік кам’янистого осипу (рис. 3.1). Це дозволить виявити оптимальну кількість компонент для подальшого аналізу.

Таблиця 3.1 – Власні значення, дисперсія та кумулятивна дисперсія компонент

Компонента	Власне значення	Дисперсія	Кумулятивна дисперсія
Компонента 1	3,322	1,900	0,166
Компонента 2	1,423	0,082	0,237
Компонента 3	1,341	0,144	0,304
Компонента 4	1,197	0,066	0,364
Компонента 5	1,131	0,033	0,421
Компонента 6	1,098	0,021	0,476
Компонента 7	1,078	0,022	0,530
Компонента 8	1,055	0,047	0,582
Компонента 9	1,008	0,045	0,633
Компонента 10	0,964	0,056	0,681
Компонента 11	0,907	0,053	0,726
Компонента 12	0,854	0,079	0,769
Компонента 13	0,775	0,017	0,808
Компонента 14	0,757	0,030	0,846
Компонента 15	0,727	0,052	0,882
Компонента 16	0,676	0,097	0,916
Компонента 17	0,579	0,101	0,945
Компонента 18	0,478	0,135	0,969
Компонента 19	0,343	0,056	0,986
Компонента 20	0,287	,	1,000

Джерело: складено авторкою

Загальна кількість отриманих компонент відповідає загальній кількості вхідних змінних. З огляду на результати власних значень отриманих компонент, представлених у таблиці 3.1, то перші дев'ять компонент мають власне значення більше за 1. При цьому значення кумулятивної дисперсії для даних дев'яти компонент дорівнює 0,633, що означає, що більше ніж 63% досліджуваного явища пояснюється даними компонентами.

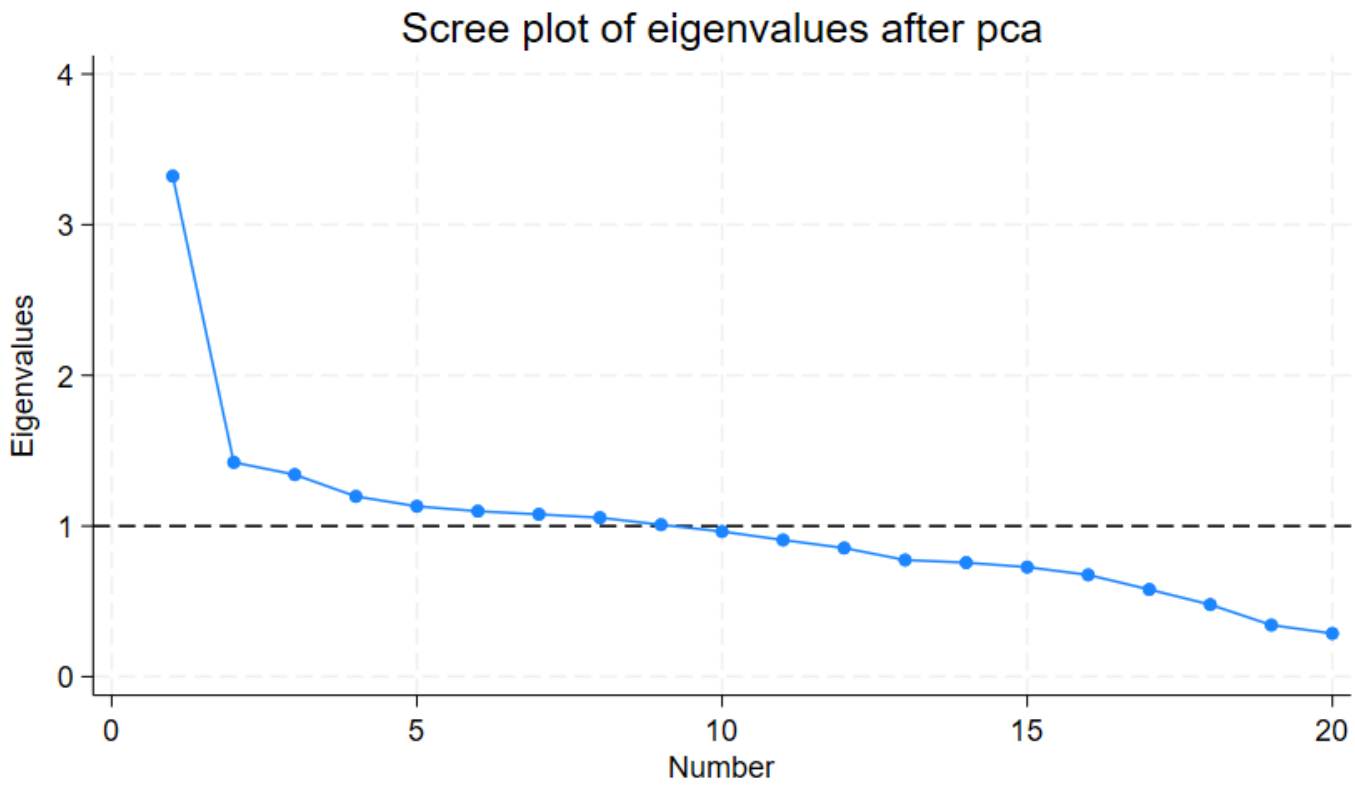


Рисунок 3.1 – Графік кам'янистого осипу

Джерело: складено авторкою

Графік кам'янистого осипу (рис. 3.1) дозволяє візуалізувати результати першого етапу методу головних компонент, оскільки демонструє власні значення кожної компоненти. Пунктирною лінією на графіку позначене місце, що відповідає оптимальній кількості компонент. У даному випадку – це 9.

Для того, щоб зрозуміти міру впливу кожної змінної в межах кожної компоненти, необхідно дослідити їх факторні навантаження (табл. 3.2). По суті

факторне навантаження представляє собою коефіцієнт кореляції відповідної змінної із компонентою, до якої вона потрапила. В контексті теми даного дослідження кожна компонента представляє собою певний портрет потенційного інсайдера-кібершахрая в банку, а найбільші значення факторних навантажень змінних свідчать якими саме ознаками обумовлюється даний портрет.

Таблиця 3.2 – Факторні навантаження показників

Змінна	Комп1	Комп2	Комп3	Комп4	Комп5	Комп6	Комп7	Комп8	Комп9	Комп10
var1	0,451	-0,019	-0,013	0,016	0,019	-0,098	-0,150	-0,091	-0,008	0,451
var2	0,271	-0,023	0,361	0,378	0,034	-0,130	-0,284	-0,122	0,076	0,271
var3	0,129	0,104	0,131	-0,168	-0,131	-0,135	0,422	0,030	0,473	0,129
var4	-0,046	0,195	-0,253	0,593	0,013	-0,017	0,082	0,048	-0,086	-0,046
var5	0,421	0,095	-0,152	0,020	0,058	0,029	0,119	0,032	-0,033	0,421
var6	0,052	-0,597	0,002	0,101	0,056	0,125	0,137	0,283	0,039	0,052
var7	0,213	0,236	-0,173	-0,070	-0,394	0,166	-0,041	-0,006	-0,165	0,213
var8	0,150	-0,091	-0,134	0,112	0,091	0,206	0,164	0,052	0,600	0,150
var9	-0,038	0,234	0,357	0,036	0,214	0,207	0,369	-0,118	0,129	-0,038
var10	-0,025	0,166	-0,309	0,175	0,057	-0,391	-0,158	0,307	0,196	-0,025
var11	0,378	0,117	0,107	0,015	-0,034	-0,113	-0,091	0,029	-0,073	0,378
var12	0,125	-0,085	0,044	0,037	0,173	-0,228	0,575	-0,094	-0,492	0,125
var13	-0,095	-0,171	-0,281	0,359	-0,017	0,239	0,144	-0,463	-0,057	-0,095
var14	0,130	-0,313	-0,241	-0,094	0,339	0,120	-0,232	-0,347	0,122	0,130
var15	0,161	-0,207	-0,057	0,037	-0,034	0,343	0,054	0,614	-0,187	0,161
var16	0,065	0,063	0,305	0,361	-0,397	0,363	-0,030	-0,031	0,038	0,065
var17	0,033	0,221	0,206	-0,176	0,417	0,434	-0,235	0,050	-0,126	0,033
var18	-0,170	-0,107	0,366	0,320	0,310	-0,245	-0,083	0,169	0,005	-0,170
var19	0,459	-0,050	0,015	-0,007	0,159	-0,097	0,055	-0,055	-0,034	0,459
var20	-0,012	0,425	-0,267	0,117	0,402	0,175	0,085	0,157	0,017	-0,012

Джерело: складено авторкою

Для кращого сприйняття отриманих результатів залишимо в даній таблиці лише ті значення факторних навантажень, які абсолютно перевищують значення 0,3 (табл. 3.3). Це дозволить ідентифікувати найбільш релевантні змінні в межах виділених компонент.

Як бачимо, кожна із представлених компонент обумовлюється різною комбінацією вхідних змінних. Це ще раз підтверджує можливість визначення різних потенційних портретів інсайдерів-кібершахраїв у банку.

Таблиця 3.3 – Факторні навантаження змінних, які перевищують 0,3 по модулю

Змінна	Комп1	Комп2	Комп3	Комп4	Комп5	Комп6	Комп7	Комп8	Комп9
var1	0,451								
var2			0,361	0,378					
var3							0,422		0,473
var4				0,593					
var5	0,421								
var6		-0,597							
var7					-0,394				
var8									0,590
var9			0,357				0,369		
var10			-0,309			-0,391		0,307	
var11	0,378								
var12							0,575		-0,491
var13				0,359				-0,463	
var14		-0,313			0,330			-0,346	
var15						0,343		0,614	
var16			0,305	0,361	-0,397	0,363			
var17					0,417	0,434			
var18			0,366	0,310	0,310				
var19	0,459								
var20		0,425			0,402				

Джерело: складено авторкою

В межах даного дослідження для проведення асоціативного аналізу та побудови наборів асоціативних правил зупинимось на більш детальному аналізу перших трьох компонент. На основі цих компонент та на підставі критерію Силует (Silhouette) (рис. 3.2), максимальне значення якого відповідає оптимальній кількості кластерів, які можуть сформуватись під час кластеризації методом *k*-середніх (додаток Б).

Найбільше значення критерію Силует (0,357) відповідає оптимальній кількості кластерів 2 або 3. Однак з урахуванням попереднього рішення щодо кількості відібраних компонент, для кластеризації методом *k*-середніх обрано 3 кластери. Візуальне представлення утворених кластерів зображено на рисунку 3.3.

Таким чином, маємо три групи змінних (табл. 3.4).

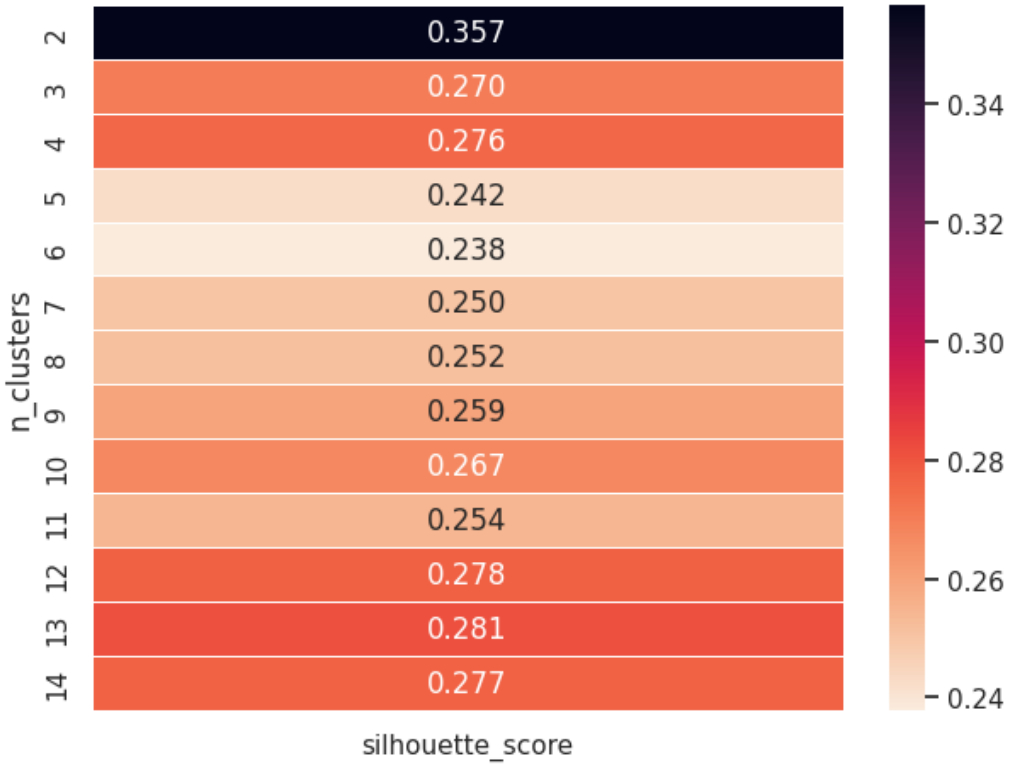


Рисунок 3.2 – Значення критерію Силует

Джерело: складено авторкою

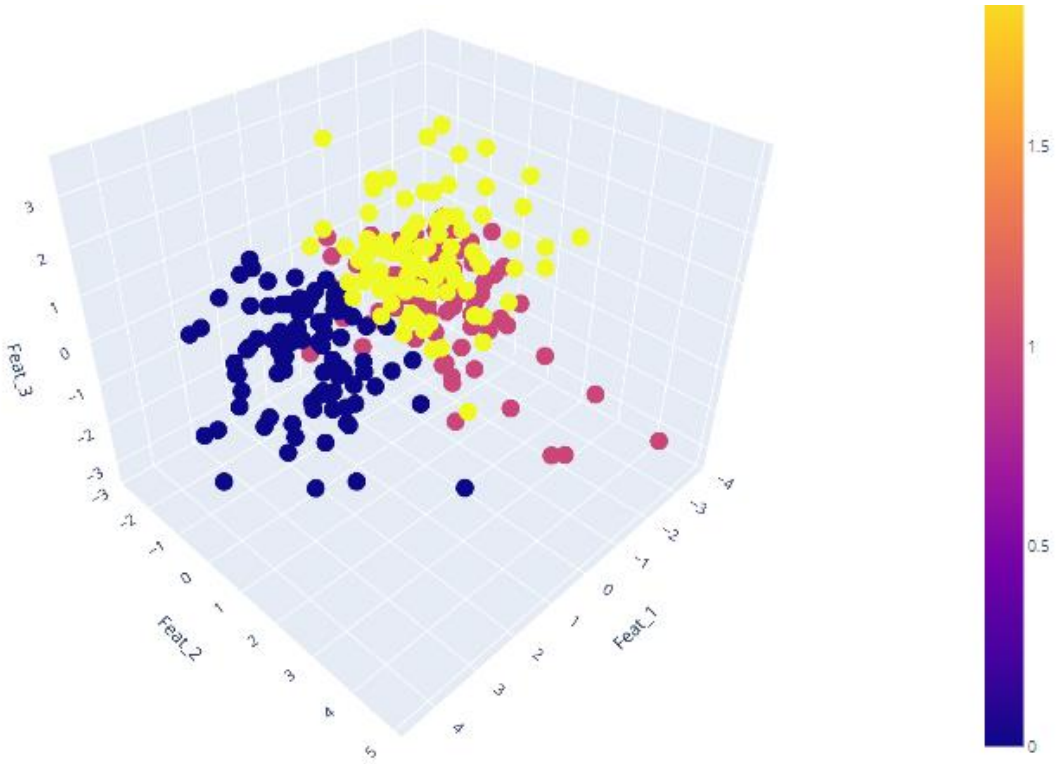


Рисунок 3.3 – Результати кластеризації методом *k*-середніх

Джерело: складено авторкою

Таблиця 3.4 – Відібрані групи змінних для проведення асоціативного аналізу

Група	Змінні
I	Номер кіберполіції
	Як посилити захист комп'ютера
	Як заблокувати транзакцію
	Як змінити обслуговуючий банк (як перевести виплату зарплати з одного банку на інший)
II	Як не допустити злому персональних даних (сайту, соціальних мереж)
	Як зменшити ліміт по банківській картці
	Чорний список користувачів
III	Номер поліції
	Як захистити себе від кібератак
	Як зрозуміти, що комп'ютер (телефон) зламали
	Який банк найбільш захищений (в Інтернеті)
	Номер підтримки банку (або номер кол-центру банку)

Джерело: складено авторкою

Таким чином, до першої групи потрапили змінні, які спрямовані на визначення політики безпеки від потенційних кібершахрайств, що з іншої сторони може бути можливістю для порушення даної безпеки інсайдерами-кібершахраями, банку зокрема.

Друга група об'єднує змінні, які мають безпосереднє відношення до захисту персональних даних клієнтів, що може бути основою для отримання необхідної інформації для інсайдерів-кібершахраїв.

До третьої групи увійшли змінні, які також мають відношення до забезпечення захищеності персональних даних користувачів, а також ідентифікації потенційних вразливостей банків.

Третій етап моделювання передбачає проведення асоціативного аналізу засобами Python 3. Для аналізу було використано бібліотеки «pandas» (під час роботи з даними) та «mlxtend» (безпосередньо під час проведення асоціативного аналізу). Також під час визначення асоціативних правил використовувався алгоритм «apriori».

Перш ніж починати визначення асоціативних правил за допомогою мови програмування Python необхідно вхідні дані перевести в бінарний вигляд (рис. 3.4).

```
[41] one_hot = pd.get_dummies(df[categorical_columns])

[42] one_hot
```

week	Cyber police number_0	Cyber police number_6	Cyber police number_7	Cyber police number_8	Cyber police number_9	Cyber police number_10	Cyber po number
2018-11-18	0	1	0	0	0	0	
2018-11-25	0	0	0	0	0	0	
2018-12-02	0	0	0	1	0	0	
2018-12-09	0	0	0	0	0	0	
2018-12-16	0	0	0	0	0	0	
...	...	...	...	...	...	...	
2023-10-08	0	0	0	0	0	0	
2023-10-15	0	0	0	0	0	0	
2023-10-22	0	0	0	0	0	0	
2023-10-29	0	0	0	0	0	0	
2023-11-05	0	0	0	0	0	0	

260 rows × 252 columns

Рисунок 3.4 – Перетворення вхідних даних в бінарні значення за допомогою методу «one hot encoding»

Джерело: складено авторкою

Представлений нижче фрагмент програмного коду написаний на Python (рис. 3.5) є прикладом використання апріорного алгоритму та функції «association_rules», які зазвичай використовуються для аналізу ринкового кошика в галузі інтелектуального аналізу даних.

```
# Find frequent itemsets
frequent_itemsets = apriori(one_hot, min_support=0.01, use_colnames=True)

# Generate association rules
rules = association_rules(frequent_itemsets, metric="confidence", min_threshold=0.2)

rules
[45]
```

Рисунок 3.5 – Фрагмент програмного коду написаний на Python, що представляє собою приклад використання апріорного алгоритму та функції «association_rules»

Джерело: складено авторкою

Представлений код використовує алгоритм «apriori» та функцію «association_rules» для аналізу запитів користувачів в області аналізу даних. Структура «apriori» алгоритму наступна (7).

frequent_itemsets = apriori(one_hot, min_support=0.01, use_colnames=True) (7)

де one_hot – вхідні дані, у форматі one-hot encoding;

min_support=0.01 – набори, що зустрічаються в 1% транзакцій;

use_colnames=True – використовує значення змінних.

Процес створення правил асоціації має наступний вигляд (8).

rules = association_rules(frequent_itemsets, metric="confidence", min_threshold=0,2) (8)

де metric="confidence" – міра надійності правила;

min_threshold=0.2 – правила з достовірністю не менше 20%.

У результаті проведення асоціативного аналізу для перерахованих груп змінних було отримано три моделі асоціативних правил із відповідними критеріями якості. Результати даного моделювання представлені в додатку Б (табл. Б1-Б3). Проаналізуємо отримані результати асоціативного аналізу за допомогою наступних харакетристик: підтримку (*support*), імовірність (*confidence*), ліфт (interest lift), левередж (leverage), доказ (*conviction*) та метрика Чжана (*zhangs_metric*).

З огляду на результати асоціативного аналізу для першої групи змінних, імовірність асоціативного правила коливається від 0,214 до 0,75. Тобто жодне правило не має 100% імовірності. Однак, зважаючи на цю обставину, проранжувавши отриману сукупність асоціативних правил за рівнем імовірності, що відповідає значенню в проміжку від 0,6 до 0,75, отримано наступні результати (табл. 3.5).

Таблиця 3.5 – Результати асоціативного аналізу для першої групи змінних, імовірність асоціативних правил яких знаходиться в діапазоні 0,6-0,75

Причина	Наслідок	Підтримка	Імовірність	Ліфт	Левередж	Доказ	Метрика Чжана
How to change the bank_40	Cyber police number_24	0,023	0,600	26,000	0,011	2,442	0,980
How to protect your computer_54	How to block a transaction_31	0,027	0,600	22,286	0,011	2,433	0,974

Джерело: складено авторкою

З огляду на представлені результати в таблиці Б1 додатку Б отримано всього 20 асоціативних правил, однак, провівши аналіз їх характеристик, спираючись в першу чергу на значення імовірності асоціативних правил, для підсумкового аналізу варто залишити лише два асоціативні правила (табл. 3.5). Як бачимо, із імовірністю 60% виконуються правила *How to change the bank => Cyber police number* та *How to protect your computer => How to block a transaction*. При цьому значення підтримки складає 2,3% і 2,7% відповідно, що означає те, що представлені правила зустрічаються в більше 2% усіх транзакцій. Відносно невисокий рівень значення підтримки в контексті виявлення потенційних шахрайських дій інсайдерів-кібершахраїв у банках є нормальним, оскільки із момент виявлення шахрайських дій є досить складним і може залежати від значного набору факторів. Високе значення ліфта для обох правил, 26 і 22,286 відповідно, свідчить про те, що представлені наслідки часто визначаються саме даними причинами, у порівнянні із ситуаціями, коли причини відсутні.

Значимість отриманих асоціацій, яка описується левереджем, є однаковою і становить 1,1%. Позитивне значення метрики Чжана для обох асоціативних правил є позитивним, 0,98 і 0,974 відповідно, що підтверджує факт присутності асоціації між причинами та наслідками.

Таким чином, якщо трансформувати отримані результати асоціативного аналізу для першої групи змінних на потенційного інсайдера-кібершахрая в банку, то можна зробити висновок, що причиною зміни обслуговуючого банку є саме кібершахрайство, оскільки імовірніше за все після цього є потреба в пошуку номеру

кіберполіції. Таким чином, інсайдер-кібершахрай банку може отримати доступ до персональної фінансової інформації клієнта, який постраждав. Друге асоціативне правило із табл. 3.5 надає інсайдеру-кібершахраю в банку по заблокованій транзакції зрозуміти потенційні уразливі моменти в захисті комп'ютера користувача-клієнта банку.

Результати асоціативного аналізу для другого набору змінних із табл. 3.4 представлені в таблиці Б2 додатку Б. Як бачимо, від попередніх результатів, отримані асоціативні правила мають значення імовірностей асоціативних правил на рівні 100%, однак потрібно зважати також на вид транзакції, для якої було отримано відповідне значення імовірності.

Аналогічно до попереднього аналізу результатів відберемо ті асоціативні правила, які мають найвище значення асоціативної імовірності (табл. Б4). Як бачимо, багато асоціативних правил мають значення імовірності 100%, однак, враховуючи невисоку кількість попередньо отриманих результатів за пошуковими запитами «How to reduce the credit limit» та «Black list of customers» усі наслідки утворених асоціативних правил відповідають нулевій кількості відповідних запитів, що не дає можливості коректно дослідити зв'язок між умовою та наслідком. Крім того, значення ліфту для всіх пар асоціативних правил наближається до одиниці, що також підтверджують відсутність зв'язку між умовою та наслідком.

Результати асоціативного аналізу для третього набору змінних із табл. 3.4 представлені в таблиці Б3 додатку Б. Як бачимо, кількість отриманих асоціативних правил є великою, тому необхідно проаналізувати їхню якість. Аналогічно до попередніх результатів для даної групи змінних є також значення асоціативних імовірностей на рівні 100%, однак не для всіх побудованих асоціативних правил вона дійсно підтверджує присутність причинно-наслідкового зв'язку між умовою та наслідком. Тому виникає потреба в аналізі нижчих значень асоціативних імовірностей, на основі яких можна довести присутність якісного зв'язку між умовою та наслідком. В наступній таблиці (табл. 3.6) представлені асоціативні правила для даного набору змінних, асоціативні імовірності для яких знаходяться в проміжку від 0,6 до 1, і пошукові запити при цьому не є нульовими.

Таблиця 3.6 – Результати асоціативного аналізу для третьої групи змінних, імовірність асоціативних правил яких знаходиться в діапазоні 0,6-1

Причина	Наслідок	Підтримка	Імовірність	Ліфт	Левередж	Доказ	Метрика Чжана
1	2	3	4	5	6	7	8
How to protect yourself from cyber attacks_13	Police number_63	0,065	1,000	15,294	0,011	inf	0,946
How to find that phone is hacked_28	Bank call center numbe_52	0,038	0,750	19,500	0,011	3,846	0,964
Which bank is the most secure online_0, How to protect yourself from cyber attacks_13	Police number_63	0,065	1,000	15,294	0,011	inf	0,946
How to protect yourself from cyber attacks_13	Which bank is the most secure online_0, Police number_63	0,042	1,000	23,636	0,011	inf	0,969
How to protect yourself from cyber attacks_0, How to find that phone is hacked_28	Bank call center numbe_52	0,038	0,750	19,500	0,011	3,846	0,964
How to find that phone is hacked_28	Bank call center numbe_52, How to protect yourself from cyber attacks_0	0,035	0,750	21,667	0,011	3,862	0,969
Which bank is the most secure online_0, How to find that phone is hacked_28	Bank call center numbe_52	0,038	0,750	19,500	0,011	3,846	0,964

Продовження таблиці 3.6

1	2	3	4	5	6	7	8
How to find that phone is hacked_28	Which bank is the most secure online_0, Bank call center numbe_52	0,035	0,750	21,667	0,011	3,862	0,969
Which bank is the most secure online_0, How to protect yourself from cyber attacks_0, How to find that phone is hacked_28	Bank call center numbe_52	0,038	0,750	19,500	0,011	3,846	0,964
Which bank is the most secure online_0, How to find that phone is hacked_28	Bank call center numbe_52, How to protect yourself from cyber attacks_0	0,035	0,750	21,667	0,011	3,862	0,969
How to protect yourself from cyber attacks_0, How to find that phone is hacked_28	Which bank is the most secure online_0, Bank call center numbe_52	0,035	0,750	21,667	0,011	3,862	0,969
How to find that phone is hacked_28	Which bank is the most secure online_0, Bank call center numbe_52, How to protect yourself from cyber attacks_0	0,031	0,750	24,375	0,011	3,877	0,974

Джерело: складено авторкою

Як бачимо, пошуковий запит «Police number» є наслідком для причини «How to protect yourself from cyber attacks» з імовірністю 100%. В межах інших асоціативних правил, де також зустрічається «Police number», як наслідок або частина наслідку разом із іншим пошуковим запитом, причина залишається незмінною.

Пошуковий запит «Bank call center number» присутній у семи отриманих асоціативних правилах і всі сім разів у вигляді наслідку. З імовірністю 75% даний пошуковий запит з'являється внаслідок іншого пошукового запиту – «How to find that phone is hacked». При чому варто зазначити, що даний причинно-наслідковий зв'язок присутній як безпосередньо між даною парою пошукових запитів, так і в сукупності із іншими пошуковими запитами.

Решта отриманих асоціативних правил містить пошукові запити, які мають нулеві значення частоти появи, тому інтерпретувати їх немає потреби.

При цьому значення підтримки для розглянутих асоціативних правил складає від 3,1% до 6,5%.Це означає, що представлені правила зустрічаються у від 3,1% до 6,5% усіх транзакцій. Даний результат є абсолютно нормальним, якщо мова йде про аналіз потенційних шахрайських схем. Високе значення ліфта для обох видів асоціативних правил, від 15,294 до 24,375 підтверджують, що представлені наслідки часто визначаються саме розглянутими причинами, у порівнянні із ситуаціями, коли причини відсутні.

Значимість отриманих асоціацій, яка описується левереджем, є однаковою і становить 1,1%. Позитивне значення метрики Чжана для обох асоціативних правил є позитивним, від 0,964 до 0,974, що підтверджує факт присутності асоціації між причинами та наслідками.

Отже, спираючись на результати третього асоціативного аналізу, потеційний інсайдер-кібершахрай у банку ще раз переконується у тому, що вразливість користувачів кібератаками супроводжується пошуком номеру поліції для усунення негативних наслідків, що ще раз підтверджує дієвість шахрайських дій за умови отримання доступу до персональних даних клієнтів банку. Друге асоціативне правило із табл. 3.6 надає інсайдеру-кібершахраю в банку розуміння, що більшість банківських транзакцій сучасним користувачем банківських послуг на сьогодні відбуваються за допомогою телефону, оскільки потреба у виявленні чи зламаний телефон кібершахраями імовірніше за все супроводжується дзвінком до кол-центру банку. Тому інсайдер-кібершахрай банку може, отримавши фізичний доступ до телефону клієнта банку, здійснити ряд шахрайських дій із його банківським акаунтом.

3.2 Розробка рекомендацій за результатами проведених розрахунків

Під час виконання даної роботи було сформовано два списки по десять змінних, які представляють собою пошукові запити, що характеризують кібератаки та рівень зменшення довіри до фінансових установ. Попередній аналіз частоти використання даних пошукових запитів користувачами пошукової системи Google підтвердив, що не всі вони є однаково популярними, проте позитивна динаміка протягом останніх років підтверджує актуалізацію поширення проблеми кібершахрайства у суспільстві. Асоціативний аналіз трьох наборів змінних, відібраних попередньо за допомогою методу головних, дозволив зрозуміти що саме є найбільш цікавим для потенційних інсайдерів-кібершахраїв у банках: персональна фінансова інформація клієнта, доступ до особистого кабінету банківського клієнта, а також заволодіння його телефоном.

Тому з метою мінімізації наслідків від дій інсайдерів-кібершахраїв у банку необхідно проводити профілактичні заходи та ніколи не втрачати пильності. До переліку основних профілактичних заходів можна віднести наступне:

– спілкуватись тільки із перевіреними працівниками банку, які можуть відповідно підтвердити той факт, що вони дійсно працюють в цьому банку, та не поширювати особисті паролі та іншу конфіденційну інформацію безпосередньо із працівниками банку;

– використовувати багатофакторну автентифікацію для онлайн-банківських операцій;

– регулярно оновлювати програмне забезпечення безпеки, включаючи антивірусні програми;

– слідкувати за активністю власного облікового запису в режимі реального часу для виявлення незвичної або підозрілої його активності (це може включати великі транзакції, невдалі спроби входу або транзакції з незнайомих місць;

– використовувати надійні паролі та безпечні застосунки для мобільного банкінгу;

– застрахувати себе від потенційного кібершахрайства (можливість інвестування в кіберстрахування, щоб зменшити фінансові втрати в разі кібератаки, що може забезпечити покриття судових витрат).

Поєднуючи ці заходи, клієнти банків можуть посилити власну кібербезпеку та мінімізувати наслідки від кібершахрайства.

ВИСНОВКИ

В межах представленої теми дослідження було сформульовану мету, яка полягала в розробці методики моделювання ймовірної поведінки дій інсайдерів-кібершахраїв у банках. Для її досягнення було сформульовано сім задач, кожна з яких була успішно досягнута.

Під час аналізу сучасних викликів фінансового сектору в контексті розвитку кібершахрайств та їх наслідків було розглянуто ключові тренди та інновації у банківській системі, представлено структуру найбільш популярних кібершахрайств у фінансовій сфері на сьогоднішній день та досліджено існуючу міжнародну нормативно-регулятивну базу, що сприяє підвищенню рівня кібербезпеки у фінансовій сфері.

Систематизація існуючих теоретичних підходів щодо розгляду кібершахрайств у банках дозволила виявити позитивну тенденцію в динаміці кількості опублікованих матеріалів конференцій та статей за ключовими словами «cyber» та «frauds» в міжнародній базі Scopus протягом 2000-2023 років, а також за допомогою програмного продукту VOSviewer систематизувати комбінації ключових слів,які використовуються в наукових публікаціях за обраною темою, що дозволило сформувати із них кластери, візуалізувати та систематизувати вектори наукових досліджень.

У межах сформульованих задач моделювання ймовірної поведінки дій інсайдерів-кібершахраїв у банках в якості масиву вхідних змінних, які дозволять оцінити дану поведінку, запропоновано використовувати можливі комбінації пошукових запитів в пошуковій системі Google. Загалом отримано два списки змінних: перший включає в себе десять змінних, які безпосередньо характеризують кібератаки, та другий – що характеризують рівень зменшення довіри до фінансових установ.

Запропонований методологічний підхід моделювання ймовірної поведінки дій інсайдерів-кібершахраїв у банках складався із трьох етапів. На першому та другому

етапах дослідження за допомогою методу головних компонент та кластеризації методом *k*-середніх сформовано масив найбільш релевантних для проведення подальшого дослідження змінних. У результаті до них увійшли дванадцять із двадцяти початкових змінних, які були згруповані у три списки. На наступному етапі моделювання за допомогою асоціативного аналізу було побудовано три моделі асоціативних правил, на основі яких було сформульовано наступний висновок – найбільш цікавим для потенційних інсайдерів-кібершахраїв у банках є персональна фінансова інформація клієнта, доступ до особистого кабінету банківського клієнта, а також заволодіння його телефоном. Тому з метою мінімізації наслідків від дій інсайдерів-кібершахраїв у банку необхідно проводити відповідні профілактичні заходи, а клієнтам пильно ставитись до персональних даних.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. 10 Emerging Banking Trends in 2024. StartUs Insights. URL: https://www.startus-insights.com/innovators-guide/banking-technology-trends/ (дата звернення 05.11.2023).

2. Al, A. W. E. Employee Behavioural Factors and Information Security Standard Compliance in Nigeria Banks. International Journal of Computing and Digital Systems. 2019. 8(4), 387–396. https://doi.org/10.12785/ijcds/080407.

3. Alharbi, A., Alshammari, M., Okon, O. D., Alabrah, A., Rauf, H. T., Alyami, H., & Meraj, T. A novel Text2IMG Mechanism of Credit Card Fraud Detection: A Deep Learning approach. Electronics. 2022. 11(5), 756. https://doi.org/10.3390/electronics11050756.

4. Almaiah, M. A., Al-Otaibi, S., Shishakly, R., Hassan, L. H., Lutfi, A., Alrawad, M., Qatawneh, M., & Alghanam, O. A. Investigating the role of perceived risk, perceived security and perceived trust on Smart M-Banking Application using SEM. Sustainability. 2023. 15(13), 9908. https://doi.org/10.3390/su15139908.

5. Alsolami, F. BioPay: Your Fingerprint is Your Credit Card. International Journal of Advanced Computer Science and Applications. 2019. https://doi.org/10.14569/ijacsa.2019.0100167.

6. Arner, D. W., Zetzsche, D. A., Buckley, R. P., & Barberis, J. The Identity Challenge in Finance: From analogue identity to digitized identification to digital KYC utilities. European Business Organization Law Review. 2019. 20(1), 55–80. https://doi.org/10.1007/s40804-019-00135-1.

7. Benjelloun, F. Z., Lahcen, A. A., & Belfkih, S. Outlier detection techniques for big data streams: focus on cyber security. International Journal of Internet Technology and Secured Transactions. 2019. 9(4), 446. https://doi.org/10.1504/ijitst.2019.102799.

8. Bera, D., Ogbanufe, O., & Kim, D. J. Towards a thematic dimensional framework of online fraud: An exploration of fraudulent email attack tactics and

intentions. Decision Support Systems. 2023. 171, 113977. https://doi.org/10.1016/j.dss.2023.113977.

9. Bharne, S., & Bhaladhare, P. An enhanced scammer detection model for online social network frauds using machine learning. International Journal on Recent and Innovation Trends in Computing and Communication. 2023. 11(5s), 239–249. https://doi.org/10.17762/ijritcc.v11i5s.6650.

10. Btoush, E. a. L. M., Zhou, X., Gururajan, R., Chan, K. C., Genrich, R., & Sankaran, P. A systematic review of literature on credit card cyber fraud detection using machine and deep learning. PeerJ. 2023. 9, e1278. https://doi.org/10.7717/peerj-cs.1278.

11. Carlos J., Pelegrini J., Prenio J. Banks' cyber security – a second generation of regulatory approaches. FSI Insights on policy implementation, No 50. 2023. URL: https://www.bis.org/fsi/publ/insights50.pdf. (дата звернення 05.11.2023).

12. Carvalho, S., Carvalho, J. V., Silva, J. C., Santos, G., & De Melo Bandeira, G. S. Concerns about Cybersecurity: The Implications of the use of ICT for Citizens and Companies. Journal of Information Systems Engineering and Management. 2023. 8(2), 20713. https://doi.org/10.55267/iadt.07.13226.

13. Chen, Z., & Omote, K. Preventing SNS Impersonation: a Blockchain-Based approach. IEICE Transactions on Information and Systems. 2023. E106.D(9), 1354–1363. https://doi.org/10.1587/transinf.2022icp0003.

14. Cloud Based Intrusion Prevention System with Machine Learning Approach. International Journal of Pharmaceutical Research. 2020. 12(02). https://doi.org/10.31838/ijpr/2020.12.02.0133.

15. Cluster Analysis: Basic Concepts and Algorithms [Електронний ресурс]: Режим доступу: https://wwwusers.cs.umn.edu/~kumar/dmbook/ch8.pdf (дата звернення 05.11.2023).

16. Cyber risk and regulation in Europe. Deloitte. URL: https://www2.deloitte.com/content/dam/Deloitte/lu/Documents/risk/lu_deloitte-cyber-risk-regulation-europe.pdf. (дата звернення 05.11.2023).

17. Dahiya, P., & Srivastva, D. K. An efficient anomaly detection based on optimal deep belief network in big data. International Journal of Engineering and Advanced Technology. 2019. 9(1), 708–716. https://doi.org/10.35940/ijeat.f9178.109119.

18. Delroy A. Chevers The impact of cybercrime on e-banking: A proposed model. International conference on information resources management (conf-irm), 2019. URL: https://core.ac.uk/download/pdf/301381651.pdf (дата звернення 05.11.2023).

19. Dewi, Y., Suharman, H., Koeswayo, P. S., & Tanzil, N. D. Factors influencing the effectiveness of credit card fraud prevention in Indonesian issuing banks. Banks and Bank Systems. 2023. 18(4), 44–60. https://doi.org/10.21511/bbs.18(4).2023.05.

20. Didenko, Anton N., Cybersecurity Regulation in the Financial Sector: Prospects of Legal Harmonisation in the EU and Beyond. Uniform Law Review. 2020. 25(1), 125-167, UNSW Law Research Paper No. 20-9, Available at SSRN: https://ssrn.com/abstract=3533664 or http://dx.doi.org/10.2139/ssrn.3533664.

21. Distribution of cyber attacks on financial and insurance organizations worldwide from October 2021 to September 2022, by type. Statista. URL: https://www.statista.com/statistics/1323911/cyber-attacks-on-financial-organizations-worldwide-by-type/. (дата звернення 05.11.2023).

22. Dzomira, S. 2017. Internet banking fraud alertness in the banking sector: South Africa. *Banks and Bank Systems*, *12*(1), 143–151. https://doi.org/10.21511/bbs.12(1-1).2017.07.

23. Elmahalwy, A. M., Mousa, H. M., & Amin, K. M. New hybrid ensemble method for anomaly detection in data science. International Journal of Power Electronics and Drive Systems. 2023. 13(3), 3498. https://doi.org/10.11591/ijece.v13i3.pp3498-3508.

24. Eyo E. Impact of cyber -security on financial fraud in commercial banks in Nigeria: a case study of Zenith banks in Abuja, 2023. URL: https://repository.aust.edu.ng/xmlui/bitstream/handle/123456789/5117/Ekong%20Eyo%20Unwana.pdf?sequence=1&isAllowed=y (дата звернення 05.11.2023).

25. Financial crime and fraud in the age of cybersecurity. McKinsey&Company. URL: https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/Risk/Our%20Insig

hts/Financial%20crime%20and%20fraud%20in%20the%20age%20of%20cybersecurity/Financial-crime-and-fraud-in-the-age-of-cybersecurity.pdf (дата звернення 05.11.2023).

26. Godniuk, I., Shubenko, I., & Volska, A. FINANCIAL FRAUD IN COMMERCIAL BANKS OF UKRAINE. WAYS OF CONTROL IN THE FIELD OF CASHLESS OPERATIONS. Economic Scope. 2021. https://doi.org/10.32782/2224-6282/165-20.

27. Google Trends. URL: https://trends.google.com/trends/?hl=ru (дата звернення 05.11.2023).

28. Gritsenko, K. ANALYSIS OF METHODS OF FRAUD DETECTION OF BANK PERSONNEL. Ìnfrastruktura Rinku. 2019. *34*. https://doi.org/10.32843/infrastruct34-48.

29. Hafidi, M., & Lamia, M. A hybrid model to detect phishing-websites. International Journal of Internet Technology and Secured Transactions. 2022. 12(6), 483. https://doi.org/10.1504/ijitst.2022.126472.

30. Iancu, E., Tuşa, E., Iancu, N., Simion, E., & Moise, A. Preventing computer crime by knowing the legal regulations that ensure the protection of computer systems. Juridical Tribune. 2023.*13*(3). https://doi.org/10.24818/tbj/2023/13/3.03.

31. Jagan, S., Ashish, A., Mahdal, M., Isabels, K. R., Dhanke, J. A., Jain, P., & Elangovan, M. A Meta-Classification model for optimized ZBot malware prediction using learning algorithms. Mathematics. 2023. *11*(13), 2840. https://doi.org/10.3390/math11132840.

32. Jayanthi, E., Ramesh, T., Kharat, R., Veeramanickam, M. R. M., Bharathiraja, N., Venkatesan, R., & Marappan, R. Cybersecurity enhancement to detect credit card frauds in health care using new machine learning strategies. Soft Computing. 2023. 27(11), 7555–7565. https://doi.org/10.1007/s00500-023-07954-y.

33. Kalaichelvi, T., Mane, S., Dhanalakshmi, K., & Prasad, S. N. The detection of phishing attempts in communications systems. International Journal of Electronic Security and Digital Forensics. 2023. 15(5), 541–553. https://doi.org/10.1504/ijesdf.2023.133192.

34. Khan, H. U., Malik, M. Z., Nazir, S., & Khan, F. Utilizing Bio Metric System for Enhancing Cyber Security in Banking Sector: A Systematic Analysis. IEEE Access. 2023. 11, 80181–80198. https://doi.org/10.1109/access.2023.3298824.

35. Kuzmenko, O., Yarovenko, H., & Perkhun, L. Assessing the maturity of the current global system for combating financial and cyber fraud. Statistics in Transition New Series. 2023. 24(1), 229–258. https://doi.org/10.59170/stattrans-2023-013.

36. Malik, A. K., Gehlot, S., & Vyas, S. Proposed Framework for Implementation of Biometrics in Banking KYC. 2023. In Lecture notes in networks and systems (pp. 193–202). https://doi.org/10.1007/978-981-99-1479-1_15.

37. Mehrban, S., Khan, M. A., Nadeem, M. W., Hussain, M., Ahmed, M. M., Hakeem, O., Saqib, S., Kiah, L. M., Abbas, F., & Hassan, M. Towards Secure FinTech: A Survey, taxonomy, and open Research challenges. IEEE Access. 2020. 8, 23391–23406. https://doi.org/10.1109/access.2020.2970430.

38. Mondol, S. K., Tang, W., & Hasan, S. A. A case study of IoT-Based biometric cyber security systems focused on the banking sector. 2023. In Lecture notes in networks and systems (pp. 249–261). https://doi.org/10.1007/978-981-99-1745-7_18.

39. Nicholls, J., Kuppa, A., & Le-Khac, N. Financial Cybercrime: A comprehensive survey of deep learning approaches to tackle the evolving financial crime landscape. IEEE Access. 2021. 9, 163965–163986. https://doi.org/10.1109/access.2021.3134076.

40. Number of cyber incidents in the financial industry worldwide from 2013 to 2022. Statista. URL: https://www.statista.com/statistics/1310985/number-of-cyber-incidents-in-financial-industry-worldwide/#:~:text=Global%20number%20of%20cyber%20attacks%20in%20financial%20sector%202013%2D2022&text=In%202022%2C%20there%20were%201%2C829,2021%20to%20477%20in%202022. (дата звернення 05.11.2023).

41. Ramesh, K. P., Amudha, R., Prasob, K., & Kanna, K. S. Fintech innovations in E-payments: Privacy and security in cybercrime threats. Multidisciplinary Science Journal. 2023. 5, 2023ss0320. https://doi.org/10.31893/multiscience.2023ss0320.

42. Rawat, R., Oki, O., Chakrawarti, R. K., Adekunle, T. S., Gonzáles, J. L., & Ajagbe, S. A. Autonomous Artificial Intelligence Systems for Fraud Detection and Forensics in Dark Web Environments. 2023. Informatica, 47(9). https://doi.org/10.31449/inf.v46i9.4538.

43. Rawat, R., Oki, O., Sankaran, K. S., Flórez, H., & Ajagbe, S. A. Techniques for predicting dark web events focused on the delivery of illicit products and ordered crime. International Journal of Power Electronics and Drive Systems. 2023. 13(5), 5354. https://doi.org/10.11591/ijece.v13i5.pp5354-5365.

44. Rithani, M., Kumar, R. P., & Doss, S. A review on big data based on deep neural network approaches. Artificial Intelligence Review. 2023. 56(12), 14765–14801. https://doi.org/10.1007/s10462-023-10512-5.

45. Roy, N. C., & Prabhakaran, S. Internal-led cyber frauds in Indian banks: an effective machine learning–based defense system to fraud detection, prioritization and prevention. Aslib Proceedings. 2022. 75(2), 246–296. https://doi.org/10.1108/ajim-11-2021-0339.

46. Roy, N. C., & Prabhakaran, S. Sustainable response system building against insider-led cyber frauds in banking sector: a machine learning approach. Journal of Financial Crime. 2022. 30(1), 48–85. https://doi.org/10.1108/jfc-12-2021-0274.

47. Safi, A., & Singh, S. A systematic literature review on phishing website detection techniques. Journal of King Saud University - Computer and Information Sciences 2023. 35(2), 590–611. https://doi.org/10.1016/j.jksuci.2023.01.004.

48. Shabbir, A., Shabir, M., Javed, A. R., Chakraborty, C., & Rizwan, M. Suspicious transaction detection in banking cyber–physical systems. Computers & Electrical Engineering. 2022. 97, 107596. https://doi.org/10.1016/j.compeleceng.2021.107596.

49. Shamsi, M. A., Smith, D. D., & Gleason, K. C. Space transition and the vulnerabilities of the NFT market to financial crime. Journal of Financial Crime. 2023. 30(6), 1664–1673. https://doi.org/10.1108/jfc-09-2022-0218.

50. Sharma, R., Joshi, A. M., Sahu, C., & Nanda, S. J. Detection of false data injection in smart grid using PCA based unsupervised learning. Electrical Engineering. 2023. 105(4), 2383–2396. https://doi.org/10.1007/s00202-023-01809-3.

51. Siano, A., Raimi, L., Palazzo, M., & Panait, M. Mobile Banking: An Innovative Solution for Increasing Financial Inclusion in Sub-Saharan African Countries: Evidence from Nigeria. Sustainability. 2020. 12(23), 10130. https://doi.org/10.3390/su122310130.

52. Smikle, L. The impact of cybersecurity on the financial sector in Jamaica. Journal of Financial Crime. 2022. 30(1), 86–96. https://doi.org/10.1108/jfc-12-2021-0259.

53. Sood, P., & Bhushan, P. A structured review and theme analysis of financial frauds in the banking industry. Asian Journal of Business Ethics. 2020. 9(2), 305–321. https://doi.org/10.1007/s13520-020-00111-w.

54. Technology Innovations in Banking. FINCA. URL: https://finca.org/our-work/microfinance/innovations-and-technology (дата звернення 05.11.2023).

55. The future of banking is here. Deloitte. URL: https://www2.deloitte.com/content/dam/Deloitte/in/Documents/strategy/in-innovation-future-of-banking-noexp.pdf (дата звернення 05.11.2023).

56. Ugochukwu, N. A., Goyal, S. B., & Sampathkumar, A. Blockchain-Based IoT-Enabled system for secure and efficient logistics management in the era of IR 4.0. Journal of Nanomaterials. 2022. 1–10. https://doi.org/10.1155/2022/7295395.

57. Wahab, F., Khan, I., Kamontip, Hussain, T., & Abbas, A. An investigation of cyber attack impact on consumers' intention to purchase online. Decision Analytics Journal. 2023. *8*, 100297. https://doi.org/10.1016/j.dajour.2023.100297.

58. Wang, B., Dabbaghjamanesh, M., Kavousi-Fard, A., & Mehraeen, S. Cybersecurity Enhancement of power trading within the networked microgrids based on blockchain and directed acyclic graph approach. IEEE Transactions on Industry Applications. 2019. 55(6), 7300–7309. https://doi.org/10.1109/tia.2019.2919820.

59. Yoro, R. E., Malasowe, B. O., Akazue, M. I., Ibor, A. E., & Ojugo, A. A. Evidence of personality traits on phishing attack menace among selected university

undergraduates in Nigerian. International Journal of Power Electronics and Drive Systems. 2023. 13(2), 1943. https://doi.org/10.11591/ijece.v13i2.pp1943-1953.

60. Zhang, Y., & Dong, H. Criminal law regulation of cyber fraud crimes—from the perspective of citizens' personal information protection in the era of edge computing. Journal of Cloud Computing. 2023. 12(1). https://doi.org/10.1186/s13677-023-00437-3.

61. База даних Scopus. URL: https://www.scopus.com (дата звернення 05.11.2023).

62. Дубина М.В., Садчикова І.В., Середюк І.О. Концептуальні підходи до підвищення рівня безпечності банківського платіжного середовища України. URL: https://www.business-inform.net/export_pdf/business-inform-2020-3_0-pages-349_359.pdf (дата звернення 05.11.2023).

63. Коваленко І. О. Окремі питання визначення обставин, що підлягають встановленню при розслідуванні шахрайства у сфері використання банківських електронних платежів. Актуальні проблеми криміналістики та судової експертизи: матеріали наук.-практ. семінару (м. Дніпро, 28 трав. 2021 р.). Дніпро : ДДУВС, 2021. С. 145–147.

64. Коваленко І. О. Організаційно-практичне забезпечення проведення обшуку при розслідуванні шахрайства у сфері використання банківських електронних платежів. Науковий журнал «Visegrad Journal on Human Rights» («Пан'європейський університет» Словацької Республіки). 2019. № 6. С. 117–122.

65. Коваленко І. О. Типові слідчі ситуації під час розслідування шахрайства у сфері банківських електронних платежів. Науковий журнал «Visegrad Journal on Human Rights» («Пан'європейський університет» Словацької Республіки). 2020. № 1. С. 99–103.

66. Коваленко, І. І., Давиденко, Є. О., & Швед, А. В. МЕТОДИКА ПОШУКУ АСОЦІАТИВНИХ ПРАВИЛ. Вісник Черкаського державного технологічного університету. 2019. (3), 50–55. https://doi.org/10.24025/2306-4412.3.2019.176909.

67. Коваль Н. О., Борщ М. В. Особливості функціонування платіжних систем Україні на сучасному етапі їх розвитку. Електронний журнал «Ефективна економіка».

2012. № 10. URL: http://www.economy. nayka.com.ua/images/top_plashka.jpg (дата звернення 01.11.2022).

68. Кришевич О. В. Шахрайство у сфері обігу банківських платіжних карток: кримінально-правовий аспект. Актуальні проблеми кримінального права: матеріали X Всеукр. наук.-теоретичної конф. (Київ, 22 лист. 2019 р.). Присвячено пам'яті професора П. П. Михайленка. Київ : Нац. акад. внутр. справ, 2021. С. 81–84

69. Сигетова, К., Узікова, Л., Доценко, Т., & Boyko, A. ОСТАННІ ТЕНДЕНЦІЇ ФІНАНСОВОЇ ЗЛОЧИННОСТІ СВІТУ. Fìnansovo-kreditna Dìâl′nìst′: Problemi Teorìï Ta Praktiki. 2022. 5(46), 258–270. https://doi.org/10.55643/fcaptp.5.46.2022.3897.

70. Чучко С. В. Розслідування шахрайства при купівлі-продажу товарів через мережу Інтернет : дис. … д-а філософії за спеціальністю – 081 Право / Дніпропетровський державний університет внутрішніх справ. Дніпро, 2021. 276 с

71. Яровенко Г. М. Моделювання виявлення ознак кіберзагроз в банках із використанням інтелектуального аналізу [Електронний ресурс] / Г. М. Яровенко, А. І. Сковронська, М. М. Бояджян // Ефективна економіка. 2018. № 7. URL: http://www.economy.nayka.com.ua/?op=1&z=6453.

72. Яровенко Г. М., Ковач В. О. Моделювання портретів потенційних шахрая та жертви банківських шахрайств. Електронне наукове фахове видання «Ефективна економіка». 2018. URL : http://www.economy.nayka.com.ua/ pdf/10_2018/63.pdf (дата звернення – 17.11.2023).

73. Яровенко Г.М. Аналіз наслідків кібершахрайств в банківській системі України. URL: http://economyandsociety.in.ua/ journals/18_ukr/116.pdf. (дата звернення 05.11.2023).

ДОДАТКИ

ДОДАТОК А

SUMMARY

Raputa A.O. Modeling the Probable Behavior of Actions of Insiders – Cyber Fraudsters in Banks. – Masters-level Qualification Thesis. Sumy State University, Sumy, 2023

The master's thesis analyzes the modern challenges of the financial sector in the context of the development of cyber frauds and their consequences; existing theoretical approaches to the consideration of cyber fraud in banks are systematized; the problems of modeling the probable behavior of the actions of insiders-cyber fraudsters in banks were formed; the obtained results were analyzed, and recommendations were offered to commercial banks, bank clients and law enforcement agencies that regulate cyber fraud issues.

Keywords: insiders-cyber fraudsters, bank, financial sector, method of principal components, cluster analysis, associative analysis.

АНОТАЦІЯ

Рапута А.О. Моделювання ймовірної поведінки дій інсайдерів-кібершахраїв у банках – Кваліфікаційна магістерська робота. Сумський державний університет, Суми, 2023 р.

У роботі проведено аналіз сучасних викликів фінансового сектору в контексті розвитку кібершахрайств та їх наслідків; систематизовано існуючі теоретичні підходи щодо розгляду кібершахрайств у банках; сформовано задачі моделювання ймовірної поведінки дій інсайдерів-кібершахраїв у банках; проаналізовано отримані результати та запропоновано рекомендації комерційним банкам, клієнтам банків та правоохоронним органам, які регулюють питання кібершахрайств.

Ключові слова: інсайдери-кібершахраї, банк, фінансовий сектор, метод головних компонент, кластерний аналіз, асоціативний аналіз.

ДОДАТОК Б

```
from sklearn.cluster import KMeans
from sklearn.metrics import silhouette_samples, silhouette_score
clusters_range = range(2,15)
results=[]
for c in clusters_range:
  clusterer = KMeans(init='k-means++',n_clusters=c,n_init=100,random_state=0)
  cluster_labels = clusterer.fit_predict(df1)
  silhouette_avg=silhouette_score(df1, cluster_labels)
  results.append([c,silhouette_avg])
result = pd.DataFrame(results, columns=['n_clusters','silhouette_score'])
pivot_km=pd.pivot_table(result,index ='n_clusters',values='silhouette_score')
plt.figure()
sns.heatmap(pivot_km,annot=True,linewidths=.5,fmt='.3f', cmap=sns.cm.rocket_r)
plt.tight_layout()
```

Рисунок Б1 – Фрагмент програмного коду Python визначення критерія Силует

```
from yellowbrick.cluster import SilhouetteVisualizer

fig, ax = plt.subplots(7, 2, figsize=(15,30))
for i in [2,3,4,5]:
    km = KMeans(n_clusters=i, init='k-means++', n_init=10, max_iter=500,
random_state=42)
    q, mod = divmod(i, 2)
    visualizer = SilhouetteVisualizer(km, colors='yellowbrick', ax=ax[q-1][mod])
    visualizer.fit(df1)
```

Рисунок Б2 – Фрагмент програмного коду Python візуалізації критерія Силует

```
df2 = pd.DataFrame(X_scaled, columns=['Feat_1', 'Feat_2', 'Feat_3'])
kmeans = KMeans(n_clusters=3)

y = kmeans.fit_predict(df1)

df2['Cluster'] = y

print(df2)
```

Рисунок Б3 – Фрагмент програмного коду Python візуалізації реузльтатів кластеризації методом *k*-середніх

Таблиця Б1 – Результати асоціативного аналізу для першої групи пошукових запитів

№	antecedents	consequents	consequent support	confidence	lift	leverage	conviction	zhangs_metric
0	Cyber police number_17	How to block a transaction_0	0,131	0,444	3,399	0,011	1,565	0,731
1	Cyber police number_19	How to block a transaction_0	0,131	0,667	5,098	0,012	2,608	0,823
2	Cyber police number_21	How to block a transaction_0	0,131	0,500	3,824	0,011	1,738	0,762
3	How to change the bank_40	Cyber police number_24	0,023	0,600	26,000	0,011	2,442	0,980
4	Cyber police number_24	How to change the bank_40	0,019	0,500	26,000	0,011	1,962	0,984
5	Cyber police number_25	How to block a transaction_0	0,131	0,300	2,294	0,007	1,242	0,587
6	How to protect your computer_63	Cyber police number_49	0,023	0,500	21,667	0,011	1,954	0,976
7	Cyber police number_49	How to protect your computer_63	0,023	0,500	21,667	0,011	1,954	0,976
8	How to protect your computer_19	How to block a transaction_0	0,131	0,500	3,824	0,009	1,738	0,756
9	How to protect your computer_22	How to block a transaction_0	0,131	0,750	5,735	0,010	3,477	0,839
10	How to protect your computer_26	How to block a transaction_0	0,131	0,429	3,277	0,008	1,521	0,714
11	How to protect your computer_30	How to block a transaction_0	0,131	0,375	2,868	0,008	1,391	0,672
12	How to change the bank_55	How to protect your computer_48	0,023	0,600	26,000	0,011	2,442	0,980
13	How to protect your computer_48	How to change the bank_55	0,019	0,500	26,000	0,011	1,962	0,984
14	How to block a transaction_31	How to protect your computer_54	0,019	0,429	22,286	0,011	1,716	0,982
15	How to protect your computer_54	How to block a transaction_31	0,027	0,600	22,286	0,011	2,433	0,974
16	How to change the bank_31	How to block a transaction_0	0,131	0,273	2,086	0,006	1,195	0,544
17	How to change the bank_33	How to block a transaction_0	0,131	0,500	3,824	0,009	1,738	0,756
18	How to change the bank_36	How to block a transaction_0	0,131	0,364	2,781	0,010	1,366	0,669
19	How to change the bank_46	How to block a transaction_0	0,131	0,214	1,639	0,004	1,106	0,412

Таблиця Б2 – Результати асоціативного аналізу для другої групи пошукових запитів

№	antecedents	consequents	consequent support	confidence	lift	leverage	conviction	zhangs_metric
1	2	3	4	5	6	7	8	9
0	How to prevent hacking_18	How to reduce the credit limit_0	0,673	1,000	1,486	0,004	inf	0,331
1	How to prevent hacking_18	Black list of customers_0	0,758	1,000	1,320	0,003	inf	0,245
2	How to prevent hacking_22	Black list of customers_0	0,758	1,000	1,320	0,003	inf	0,245
3	How to prevent hacking_29	Black list of customers_0	0,758	1,000	1,320	0,004	inf	0,246
4	How to prevent hacking_30	How to reduce the credit limit_0	0,673	0,600	0,891	-0,001	0,817	-0,110
5	How to prevent hacking_30	Black list of customers_0	0,758	0,600	0,792	-0,003	0,606	-0,211
6	How to prevent hacking_34	How to reduce the credit limit_0	0,673	0,750	1,114	0,001	1,308	0,104
7	How to prevent hacking_35	How to reduce the credit limit_0	0,673	1,000	1,486	0,006	inf	0,333
8	How to prevent hacking_35	Black list of customers_0	0,758	0,800	1,056	0,001	1,212	0,054
9	How to prevent hacking_36	How to reduce the credit limit_0	0,673	0,857	1,273	0,005	2,288	0,221
10	How to prevent hacking_36	Black list of customers_0	0,758	1,000	1,320	0,007	inf	0,249
11	How to prevent hacking_37	How to reduce the credit limit_0	0,673	0,500	0,743	-0,004	0,654	-0,262
12	How to prevent hacking_37	Black list of customers_0	0,758	0,833	1,100	0,002	1,454	0,093
13	How to prevent hacking_38	How to reduce the credit limit_0	0,673	0,833	1,238	0,004	1,962	0,197
14	How to prevent hacking_38	Black list of customers_0	0,758	0,667	0,880	-0,002	0,727	-0,123
15	How to prevent hacking_39	How to reduce the credit limit_0	0,673	0,714	1,061	0,001	1,144	0,059
16	How to prevent hacking_39	Black list of customers_0	0,758	0,714	0,943	-0,001	0,848	-0,059
17	How to prevent hacking_40	How to reduce the credit limit_0	0,673	0,625	0,929	-0,001	0,872	-0,074
18	How to prevent hacking_40	Black list of customers_0	0,758	0,500	0,660	-0,008	0,485	-0,347
19	How to prevent hacking_41	How to reduce the credit limit_0	0,673	1,000	1,486	0,008	inf	0,335
20	How to prevent hacking_41	Black list of customers_0	0,758	0,833	1,100	0,002	1,454	0,093
21	How to prevent hacking_42	How to reduce the credit limit_0	0,673	0,556	0,825	-0,004	0,736	-0,180
22	How to prevent hacking_42	Black list of customers_0	0,758	1,000	1,320	0,008	inf	0,251
23	How to prevent hacking_43	How to reduce the credit limit_0	0,673	0,800	1,189	0,002	1,635	0,162
24	How to prevent hacking_43	Black list of customers_0	0,758	0,600	0,792	-0,003	0,606	-0,211
25	How to prevent hacking_44	How to reduce the credit limit_0	0,673	0,667	0,990	0,000	0,981	-0,010
26	How to prevent hacking_44	Black list of customers_0	0,758	1,000	1,320	0,006	inf	0,248
27	How to prevent hacking_46	How to reduce the credit limit_0	0,673	0,571	0,849	-0,003	0,763	-0,155
28	How to prevent hacking_46	Black list of customers_0	0,758	0,571	0,754	-0,005	0,565	-0,251

Продовження таблиці Б2

1	2	3	4	5	6	7	8	9
29	How to prevent hacking_47	How to reduce the credit limit_0	0,673	0,333	0,495	-0,012	0,490	-0,514
30	How to prevent hacking_47	Black list of customers_0	0,758	0,556	0,733	-0,007	0,545	-0,274
31	How to prevent hacking_48	How to reduce the credit limit_0	0,673	1,000	1,486	0,005	inf	0,332
32	How to prevent hacking_49	How to reduce the credit limit_0	0,673	0,833	1,238	0,004	1,962	0,197
33	How to prevent hacking_49	Black list of customers_0	0,758	0,833	1,100	0,002	1,454	0,093
34	How to prevent hacking_50	How to reduce the credit limit_0	0,673	0,667	0,990	0,000	0,981	-0,010
35	How to prevent hacking_50	Black list of customers_0	0,758	0,667	0,880	-0,002	0,727	-0,123
36	How to prevent hacking_51	How to reduce the credit limit_0	0,673	0,750	1,114	0,002	1,308	0,106
37	How to prevent hacking_51	Black list of customers_0	0,758	0,875	1,155	0,004	1,938	0,138
38	How to prevent hacking_52	How to reduce the credit limit_0	0,673	0,667	0,990	0,000	0,981	-0,010
39	How to prevent hacking_52	Black list of customers_0	0,758	0,667	0,880	-0,002	0,727	-0,123
40	How to prevent hacking_53	How to reduce the credit limit_0	0,673	0,500	0,743	-0,005	0,654	-0,263
41	How to prevent hacking_53	Black list of customers_0	0,758	0,625	0,825	-0,004	0,646	-0,180
42	How to prevent hacking_54	How to reduce the credit limit_0	0,673	1,000	1,486	0,010	inf	0,337
43	How to prevent hacking_54	Black list of customers_0	0,758	0,750	0,990	0,000	0,969	-0,010
44	How to prevent hacking_55	Black list of customers_0	0,758	0,750	0,990	0,000	0,969	-0,010
45	How to prevent hacking_56	How to reduce the credit limit_0	0,673	0,714	1,061	0,001	1,144	0,059
46	How to prevent hacking_56	Black list of customers_0	0,758	0,714	0,943	-0,001	0,848	-0,059
47	How to prevent hacking_57	How to reduce the credit limit_0	0,673	0,600	0,891	-0,001	0,817	-0,110
48	How to prevent hacking_57	Black list of customers_0	0,758	1,000	1,320	0,005	inf	0,247
49	How to prevent hacking_58	How to reduce the credit limit_0	0,673	0,600	0,891	-0,003	0,817	-0,112
50	How to prevent hacking_58	Black list of customers_0	0,758	0,800	1,056	0,002	1,212	0,055
51	How to prevent hacking_59	How to reduce the credit limit_0	0,673	0,800	1,189	0,002	1,635	0,162
52	How to prevent hacking_59	Black list of customers_0	0,758	0,600	0,792	-0,003	0,606	-0,211
53	How to prevent hacking_60	How to reduce the credit limit_0	0,673	0,571	0,849	-0,003	0,763	-0,155
54	How to prevent hacking_60	Black list of customers_0	0,758	1,000	1,320	0,007	inf	0,249
55	How to prevent hacking_61	How to reduce the credit limit_0	0,673	1,000	1,486	0,006	inf	0,333
56	How to prevent hacking_61	Black list of customers_0	0,758	0,600	0,792	-0,003	0,606	-0,211
57	How to prevent hacking_66	Black list of customers_0	0,758	1,000	1,320	0,004	inf	0,246
58	How to prevent hacking_68	How to reduce the credit limit_0	0,673	1,000	1,486	0,004	inf	0,331
59	How to prevent hacking_68	Black list of customers_0	0,758	1,000	1,320	0,003	inf	0,245

Продовження таблиці Б2

1	2	3	4	5	6	7	8	9
60	How to prevent hacking_69	Black list of customers_0	0,758	1,000	1,320	0,003	inf	0,245
61	How to prevent hacking_70	How to reduce the credit limit_0	0,673	0,667	0,990	0,000	0,981	-0,010
62	How to prevent hacking_70	Black list of customers_0	0,758	1,000	1,320	0,006	inf	0,248
63	How to prevent hacking_74	Black list of customers_0	0,758	1,000	1,320	0,003	inf	0,245
64	How to prevent hacking_77	Black list of customers_0	0,758	1,000	1,320	0,003	inf	0,245
65	How to reduce the credit limit_0	Black list of customers_0	0,758	0,766	1,011	0,005	1,034	0,032
66	Black list of customers_0	How to reduce the credit limit_0	0,673	0,680	1,011	0,005	1,022	0,043
67	Black list of customers_16	How to reduce the credit limit_0	0,673	1,000	1,486	0,004	inf	0,331
68	Black list of customers_17	How to reduce the credit limit_0	0,673	0,750	1,114	0,001	1,308	0,104
69	Black list of customers_18	How to reduce the credit limit_0	0,673	1,000	1,486	0,004	inf	0,331
70	Black list of customers_19	How to reduce the credit limit_0	0,673	0,857	1,273	0,005	2,288	0,221
71	Black list of customers_20	How to reduce the credit limit_0	0,673	0,714	1,061	0,001	1,144	0,059
72	Black list of customers_30	How to reduce the credit limit_0	0,673	1,000	1,486	0,004	inf	0,331
73	How to reduce the credit limit_18	Black list of customers_0	0,758	1,000	1,320	0,003	inf	0,245
74	How to reduce the credit limit_20	Black list of customers_0	0,758	1,000	1,320	0,003	inf	0,245
75	How to reduce the credit limit_23	Black list of customers_0	0,758	1,000	1,320	0,003	inf	0,245
76	How to reduce the credit limit_26	Black list of customers_0	0,758	1,000	1,320	0,006	inf	0,248
77	How to reduce the credit limit_27	Black list of customers_0	0,758	0,750	0,990	0,000	0,969	-0,010
78	How to reduce the credit limit_30	Black list of customers_0	0,758	0,667	0,880	-0,002	0,727	-0,123
79	How to reduce the credit limit_33	Black list of customers_0	0,758	1,000	1,320	0,004	inf	0,246
80	How to reduce the credit limit_0, How to prevent hacking_18	Black list of customers_0	0,758	1,000	1,320	0,003	inf	0,245
81	Black list of customers_0, How to prevent hacking_18	How to reduce the credit limit_0	0,673	1,000	1,486	0,004	inf	0,331
82	How to prevent hacking_18	How to reduce the credit limit_0, Black list of customers_0	0,515	1,000	1,940	0,006	inf	0,490
83	How to reduce the credit limit_0, How to prevent hacking_35	Black list of customers_0	0,758	0,800	1,056	0,001	1,212	0,054
84	Black list of customers_0, How to prevent hacking_35	How to reduce the credit limit_0	0,673	1,000	1,486	0,005	inf	0,332
85	How to prevent hacking_35	How to reduce the credit limit_0, Black list of customers_0	0,515	0,800	1,552	0,005	2,423	0,363
86	How to reduce the credit limit_0, How to prevent hacking_36	Black list of customers_0	0,758	1,000	1,320	0,006	inf	0,248
87	Black list of customers_0, How to prevent hacking_36	How to reduce the credit limit_0	0,673	0,857	1,273	0,005	2,288	0,221
88	How to prevent hacking_36	How to reduce the credit limit_0, Black list of customers_0	0,515	0,857	1,663	0,009	3,392	0,410

Продовження таблиці Б2

1	2	3	4	5	6	7	8	9
89	How to reduce the credit limit_0, How to prevent hacking_37	Black list of customers_0	0,758	1,000	1,320	0,003	inf	0,245
90	Black list of customers_0, How to prevent hacking_37	How to reduce the credit limit_0	0,673	0,600	0,891	-0,001	0,817	-0,110
91	How to prevent hacking_37	How to reduce the credit limit_0, Black list of customers_0	0,515	0,500	0,970	0,000	0,969	-0,031
92	How to reduce the credit limit_0, How to prevent hacking_38	Black list of customers_0	0,758	0,600	0,792	-0,003	0,606	-0,211
93	Black list of customers_0, How to prevent hacking_38	How to reduce the credit limit_0	0,673	0,750	1,114	0,001	1,308	0,104
94	How to prevent hacking_38	How to reduce the credit limit_0, Black list of customers_0	0,515	0,500	0,970	0,000	0,969	-0,031
95	How to reduce the credit limit_0, How to prevent hacking_39	Black list of customers_0	0,758	0,600	0,792	-0,003	0,606	-0,211
96	Black list of customers_0, How to prevent hacking_39	How to reduce the credit limit_0	0,673	0,600	0,891	-0,001	0,817	-0,110
97	How to prevent hacking_39	How to reduce the credit limit_0, Black list of customers_0	0,515	0,429	0,832	-0,002	0,848	-0,172
98	How to reduce the credit limit_0, How to prevent hacking_40	Black list of customers_0	0,758	0,600	0,792	-0,003	0,606	-0,211
99	Black list of customers_0, How to prevent hacking_40	How to reduce the credit limit_0	0,673	0,750	1,114	0,001	1,308	0,104
100	How to prevent hacking_40	How to reduce the credit limit_0, Black list of customers_0	0,515	0,375	0,728	-0,004	0,775	-0,279
101	How to reduce the credit limit_0, How to prevent hacking_41	Black list of customers_0	0,758	0,833	1,100	0,002	1,454	0,093
102	Black list of customers_0, How to prevent hacking_41	How to reduce the credit limit_0	0,673	1,000	1,486	0,006	inf	0,333
103	How to prevent hacking_41	How to reduce the credit limit_0, Black list of customers_0	0,515	0,833	1,617	0,007	2,908	0,391
104	How to reduce the credit limit_0, How to prevent hacking_42	Black list of customers_0	0,758	1,000	1,320	0,005	inf	0,247
105	Black list of customers_0, How to prevent hacking_42	How to reduce the credit limit_0	0,673	0,556	0,825	-0,004	0,736	-0,180
106	How to prevent hacking_42	How to reduce the credit limit_0, Black list of customers_0	0,515	0,556	1,078	0,001	1,090	0,075
107	How to reduce the credit limit_0, How to prevent hacking_44	Black list of customers_0	0,758	1,000	1,320	0,004	inf	0,246
108	Black list of customers_0, How to prevent hacking_44	How to reduce the credit limit_0	0,673	0,667	0,990	0,000	0,981	-0,010
109	How to prevent hacking_44	How to reduce the credit limit_0, Black list of customers_0	0,515	0,667	1,294	0,003	1,454	0,232
110	How to reduce the credit limit_0, How to prevent hacking_47	Black list of customers_0	0,758	1,000	1,320	0,003	inf	0,245
111	Black list of customers_0, How to prevent hacking_47	How to reduce the credit limit_0	0,673	0,600	0,891	-0,001	0,817	-0,110
112	How to prevent hacking_47	How to reduce the credit limit_0, Black list of customers_0	0,515	0,333	0,647	-0,006	0,727	-0,361
113	How to reduce the credit limit_0, How to prevent hacking_49	Black list of customers_0	0,758	0,800	1,056	0,001	1,212	0,054

Продовження таблиці Б2

1	2	3	4	5	6	7	8	9
114	Black list of customers_0, How to prevent hacking_49	How to reduce the credit limit_0	0,673	0,800	1,189	0,002	1,635	0,162
115	How to prevent hacking_49	How to reduce the credit limit_0, Black list of customers_0	0,515	0,667	1,294	0,003	1,454	0,232
116	How to reduce the credit limit_0, How to prevent hacking_50	Black list of customers_0	0,758	0,750	0,990	0,000	0,969	-0,010
117	Black list of customers_0, How to prevent hacking_50	How to reduce the credit limit_0	0,673	0,750	1,114	0,001	1,308	0,104
118	How to prevent hacking_50	How to reduce the credit limit_0, Black list of customers_0	0,515	0,500	0,970	0,000	0,969	-0,031
119	How to reduce the credit limit_0, How to prevent hacking_51	Black list of customers_0	0,758	0,833	1,100	0,002	1,454	0,093
120	Black list of customers_0, How to prevent hacking_51	How to reduce the credit limit_0	0,673	0,714	1,061	0,001	1,144	0,059
121	How to prevent hacking_51	How to reduce the credit limit_0, Black list of customers_0	0,515	0,625	1,213	0,003	1,292	0,181
122	How to reduce the credit limit_0, How to prevent hacking_54	Black list of customers_0	0,758	0,750	0,990	0,000	0,969	-0,010
123	Black list of customers_0, How to prevent hacking_54	How to reduce the credit limit_0	0,673	1,000	1,486	0,008	inf	0,335
124	How to prevent hacking_54	How to reduce the credit limit_0, Black list of customers_0	0,515	0,750	1,455	0,007	1,938	0,323
125	How to reduce the credit limit_0, How to prevent hacking_56	Black list of customers_0	0,758	0,800	1,056	0,001	1,212	0,054
126	Black list of customers_0, How to prevent hacking_56	How to reduce the credit limit_0	0,673	0,800	1,189	0,002	1,635	0,162
127	How to prevent hacking_56	How to reduce the credit limit_0, Black list of customers_0	0,515	0,571	1,109	0,002	1,131	0,101
128	How to reduce the credit limit_0, How to prevent hacking_57	Black list of customers_0	0,758	1,000	1,320	0,003	inf	0,245
129	Black list of customers_0, How to prevent hacking_57	How to reduce the credit limit_0	0,673	0,600	0,891	-0,001	0,817	-0,110
130	How to prevent hacking_57	How to reduce the credit limit_0, Black list of customers_0	0,515	0,600	1,164	0,002	1,212	0,144
131	How to reduce the credit limit_0, How to prevent hacking_58	Black list of customers_0	0,758	0,667	0,880	-0,002	0,727	-0,123
132	Black list of customers_0, How to prevent hacking_58	How to reduce the credit limit_0	0,673	0,500	0,743	-0,005	0,654	-0,263
133	How to prevent hacking_58	How to reduce the credit limit_0, Black list of customers_0	0,515	0,400	0,776	-0,004	0,808	-0,231
134	How to reduce the credit limit_0, How to prevent hacking_59	Black list of customers_0	0,758	0,750	0,990	0,000	0,969	-0,010
135	Black list of customers_0, How to prevent hacking_59	How to reduce the credit limit_0	0,673	1,000	1,486	0,004	inf	0,331
136	How to prevent hacking_59	How to reduce the credit limit_0, Black list of customers_0	0,515	0,600	1,164	0,002	1,212	0,144
137	How to reduce the credit limit_0, How to prevent hacking_60	Black list of customers_0	0,758	1,000	1,320	0,004	inf	0,246
138	Black list of customers_0, How to prevent hacking_60	How to reduce the credit limit_0	0,673	0,571	0,849	-0,003	0,763	-0,155
139	How to prevent hacking_60	How to reduce the credit limit_0, Black list of customers_0	0,515	0,571	1,109	0,002	1,131	0,101

Продовження таблиці Б2

1	2	3	4	5	6	7	8	9
140	How to reduce the credit limit_0, How to prevent hacking_61	Black list of customers_0	0,758	0,600	0,792	-0,003	0,606	-0,211
141	Black list of customers_0, How to prevent hacking_61	How to reduce the credit limit_0	0,673	1,000	1,486	0,004	inf	0,331
142	How to prevent hacking_61	How to reduce the credit limit_0, Black list of customers_0	0,515	0,600	1,164	0,002	1,212	0,144
143	How to reduce the credit limit_0, How to prevent hacking_68	Black list of customers_0	0,758	1,000	1,320	0,003	inf	0,245
144	Black list of customers_0, How to prevent hacking_68	How to reduce the credit limit_0	0,673	1,000	1,486	0,004	inf	0,331
145	How to prevent hacking_68	How to reduce the credit limit_0, Black list of customers_0	0,515	1,000	1,940	0,006	inf	0,490
146	How to reduce the credit limit_0, How to prevent hacking_70	Black list of customers_0	0,758	1,000	1,320	0,004	inf	0,246
147	Black list of customers_0, How to prevent hacking_70	How to reduce the credit limit_0	0,673	0,667	0,990	0,000	0,981	-0,010
148	How to prevent hacking_70	How to reduce the credit limit_0, Black list of customers_0	0,515	0,667	1,294	0,003	1,454	0,232

Таблиця Б3 – Фрагмент результатів асоціативного аналізу для третьої групи пошукових запитів

	antecedents	consequents	consequent support	confidence	lift	leverage	conviction	zhangs_metric
1	2	3	4	5	6	7	8	9
0	Police number_47	How to protect yourself from cyber attacks_0	0,750	0,750	1,000	0,000	1,000	0,000
1	Police number_47	How to find that phone is hacked_0	0,685	0,750	1,096	0,001	1,262	0,089
2	Police number_47	Which bank is the most secure online_0	0,765	1,000	1,307	0,004	inf	0,238
3	Police number_48	How to protect yourself from cyber attacks_0	0,750	0,714	0,952	-0,001	0,875	-0,049
4	Police number_48	How to find that phone is hacked_0	0,685	0,857	1,252	0,005	2,208	0,207
5	Police number_48	Which bank is the most secure online_0	0,765	0,857	1,120	0,002	1,642	0,110
6	Police number_49	How to protect yourself from cyber attacks_0	0,750	1,000	1,333	0,007	inf	0,257
7	Police number_49	How to find that phone is hacked_0	0,685	0,429	0,626	-0,007	0,552	-0,380
8	Police number_49	Which bank is the most secure online_0	0,765	0,857	1,120	0,002	1,642	0,110
9	Police number_50	How to protect yourself from cyber attacks_0	0,750	0,833	1,111	0,002	1,500	0,102
10	Police number_50	How to find that phone is hacked_0	0,685	0,833	1,217	0,003	1,892	0,183
11	Police number_50	Which bank is the most secure online_0	0,765	0,500	0,653	-0,006	0,469	-0,352
12	Police number_51	How to protect yourself from cyber attacks_0	0,750	0,917	1,222	0,008	3,000	0,191
13	Police number_51	How to find that phone is hacked_0	0,685	0,833	1,217	0,007	1,892	0,187
14	Police number_51	Which bank is the most secure online_0	0,765	1,000	1,307	0,011	inf	0,246
15	Police number_52	How to protect yourself from cyber attacks_0	0,750	0,857	1,143	0,003	1,750	0,128
16	Police number_52	How to find that phone is hacked_0	0,685	0,714	1,043	0,001	1,104	0,043
17	Police number_52	Which bank is the most secure online_0	0,765	1,000	1,307	0,006	inf	0,241
18	Police number_53	How to protect yourself from cyber attacks_0	0,750	0,615	0,821	-0,007	0,650	-0,187
19	Police number_53	How to find that phone is hacked_0	0,685	0,615	0,899	-0,003	0,820	-0,106
20	Police number_53	Which bank is the most secure online_0	0,765	1,000	1,307	0,012	inf	0,247
21	Police number_54	How to protect yourself from cyber attacks_0	0,750	0,867	1,156	0,007	1,875	0,143
22	Police number_54	How to find that phone is hacked_0	0,685	0,467	0,682	-0,013	0,591	-0,331
23	Police number_54	Which bank is the most secure online_0	0,765	0,800	1,045	0,002	1,173	0,046
24	Police number_55	How to protect yourself from cyber attacks_0	0,750	0,600	0,800	-0,006	0,625	-0,206
25	Police number_55	How to find that phone is hacked_0	0,685	0,700	1,022	0,001	1,051	0,023
26	Police number_55	Which bank is the most secure online_0	0,765	0,900	1,176	0,005	2,346	0,156
27	Police number_56	How to protect yourself from cyber attacks_0	0,750	0,643	0,857	-0,006	0,700	-0,150
28	Police number_56	How to find that phone is hacked_0	0,685	0,786	1,148	0,005	1,472	0,136
29	Police number_56	Which bank is the most secure online_0	0,765	0,714	0,933	-0,003	0,821	-0,070
30	Bank call center numbe_68	Police number_56	0,054	0,500	9,286	0,010	1,892	0,913
31	Police number_56	Bank call center numbe_68	0,023	0,214	9,286	0,010	1,243	0,943
32	Police number_57	How to protect yourself from cyber attacks_0	0,750	0,667	0,889	-0,003	0,750	-0,115

Продовження таблиці Б3

1	2	3	4	5	6	7	8	9
33	Police number_57	How to find that phone is hacked_0	0,685	0,778	1,136	0,003	1,419	0,124
34	Police number_57	Which bank is the most secure online_0	0,765	0,778	1,016	0,000	1,056	0,017
35	Police number_58	How to protect yourself from cyber attacks_0	0,750	0,750	1,000	0,000	1,000	0,000
36	Police number_58	How to find that phone is hacked_0	0,685	0,875	1,278	0,012	2,523	0,232
37	Police number_58	Which bank is the most secure online_0	0,765	0,688	0,898	-0,005	0,751	-0,108
38	Bank call center numbe_50	Police number_58	0,062	0,300	4,875	0,009	1,341	0,827
39	Police number_59	How to protect yourself from cyber attacks_0	0,750	0,786	1,048	0,002	1,167	0,048
40	Police number_59	How to find that phone is hacked_0	0,685	0,500	0,730	-0,010	0,631	-0,281
41	Police number_59	Which bank is the most secure online_0	0,765	0,786	1,027	0,001	1,095	0,027
42	Police number_59	Bank call center numbe_58	0,035	0,214	6,190	0,010	1,229	0,886
43	Bank call center numbe_58	Police number_59	0,054	0,333	6,190	0,010	1,419	0,869
44	Police number_60	How to protect yourself from cyber attacks_0	0,750	0,850	1,133	0,008	1,667	0,127
45	Police number_60	How to find that phone is hacked_0	0,685	0,500	0,730	-0,014	0,631	-0,286
46	Police number_60	Which bank is the most secure online_0	0,765	0,750	0,980	-0,001	0,938	-0,022
47	Bank call center numbe_51	Police number_60	0,077	0,214	2,786	0,007	1,175	0,678
48	Police number_61	How to protect yourself from cyber attacks_0	0,750	0,857	1,143	0,006	1,750	0,132
49	Police number_61	How to find that phone is hacked_0	0,685	0,857	1,252	0,009	2,208	0,213
50	Police number_61	Which bank is the most secure online_0	0,765	0,714	0,933	-0,003	0,821	-0,070
51	Police number_62	How to protect yourself from cyber attacks_0	0,750	0,524	0,698	-0,018	0,525	-0,320
52	Police number_62	How to find that phone is hacked_0	0,685	0,762	1,113	0,006	1,325	0,110
53	Police number_62	Which bank is the most secure online_0	0,765	0,762	0,995	0,000	0,985	-0,005

Таблиця Б4 – Результати асоціативного аналізу для першої групи змінних, імовірність асоціативних правил яких дорівнює 1

Причина	Наслідок	Підтримка	Імовірність	Ліфт	Левередж	Доказ	Метрика Чжана
1	2	3	4	5	6	7	8
How to prevent hacking_18	How to reduce the credit limit_0	0,673	1,000	1,486	0,004	inf	0,331
How to prevent hacking_18	Black list of customers_0	0,758	1,000	1,320	0,003	inf	0,245
How to prevent hacking_22	Black list of customers_0	0,758	1,000	1,320	0,003	inf	0,245
How to prevent hacking_29	Black list of customers_0	0,758	1,000	1,320	0,004	inf	0,246
How to prevent hacking_35	How to reduce the credit limit_0	0,673	1,000	1,486	0,006	inf	0,333
How to prevent hacking_36	Black list of customers_0	0,758	1,000	1,320	0,007	inf	0,249
How to prevent hacking_41	How to reduce the credit limit_0	0,673	1,000	1,486	0,008	inf	0,335
How to prevent hacking_42	Black list of customers_0	0,758	1,000	1,320	0,008	inf	0,251
How to prevent hacking_44	Black list of customers_0	0,758	1,000	1,320	0,006	inf	0,248
How to prevent hacking_48	How to reduce the credit limit_0	0,673	1,000	1,486	0,005	inf	0,332
How to prevent hacking_54	How to reduce the credit limit_0	0,673	1,000	1,486	0,010	inf	0,337
How to prevent hacking_57	Black list of customers_0	0,758	1,000	1,320	0,005	inf	0,247
How to prevent hacking_60	Black list of customers_0	0,758	1,000	1,320	0,007	inf	0,249
How to prevent hacking_61	How to reduce the credit limit_0	0,673	1,000	1,486	0,006	inf	0,333
How to prevent hacking_66	Black list of customers_0	0,758	1,000	1,320	0,004	inf	0,246
How to prevent hacking_68	How to reduce the credit limit_0	0,673	1,000	1,486	0,004	inf	0,331
How to prevent hacking_68	Black list of customers_0	0,758	1,000	1,320	0,003	inf	0,245
How to prevent hacking_69	Black list of customers_0	0,758	1,000	1,320	0,003	inf	0,245
How to prevent hacking_70	Black list of customers_0	0,758	1,000	1,320	0,006	inf	0,248
How to prevent hacking_74	Black list of customers_0	0,758	1,000	1,320	0,003	inf	0,245
How to prevent hacking_77	Black list of customers_0	0,758	1,000	1,320	0,003	inf	0,245
Black list of customers_16	How to reduce the credit limit_0	0,673	1,000	1,486	0,004	inf	0,331
Black list of customers_18	How to reduce the credit limit_0	0,673	1,000	1,486	0,004	inf	0,331
Black list of customers_30	How to reduce the credit limit_0	0,673	1,000	1,486	0,004	inf	0,331
How to reduce the credit limit_18	Black list of customers_0	0,758	1,000	1,320	0,003	inf	0,245
How to reduce the credit limit_20	Black list of customers_0	0,758	1,000	1,320	0,003	inf	0,245

Продовження таблиці Б4

1	2	3	4	5	6	7	8
How to reduce the credit limit_23	Black list of customers_0	0,758	1,000	1,320	0,003	inf	0,245
How to reduce the credit limit_26	Black list of customers_0	0,758	1,000	1,320	0,006	inf	0,248
How to reduce the credit limit_33	Black list of customers_0	0,758	1,000	1,320	0,004	inf	0,246
How to reduce the credit limit_0, How to prevent hacking_18	Black list of customers_0	0,758	1,000	1,320	0,003	inf	0,245
Black list of customers_0, How to prevent hacking_18	How to reduce the credit limit_0	0,673	1,000	1,486	0,004	inf	0,331
How to prevent hacking_18	How to reduce the credit limit_0, Black list of customers_0	0,515	1,000	1,940	0,006	inf	0,490
Black list of customers_0, How to prevent hacking_35	How to reduce the credit limit_0	0,673	1,000	1,486	0,005	inf	0,332
How to reduce the credit limit_0, How to prevent hacking_36	Black list of customers_0	0,758	1,000	1,320	0,006	inf	0,248
How to reduce the credit limit_0, How to prevent hacking_37	Black list of customers_0	0,758	1,000	1,320	0,003	inf	0,245
Black list of customers_0, How to prevent hacking_41	How to reduce the credit limit_0	0,673	1,000	1,486	0,006	inf	0,333
How to reduce the credit limit_0, How to prevent hacking_42	Black list of customers_0	0,758	1,000	1,320	0,005	inf	0,247
How to reduce the credit limit_0, How to prevent hacking_44	Black list of customers_0	0,758	1,000	1,320	0,004	inf	0,246
How to reduce the credit limit_0, How to prevent hacking_47	Black list of customers_0	0,758	1,000	1,320	0,003	inf	0,245
Black list of customers_0, How to prevent hacking_54	How to reduce the credit limit_0	0,673	1,000	1,486	0,008	inf	0,335
How to reduce the credit limit_0, How to prevent hacking_57	Black list of customers_0	0,758	1,000	1,320	0,003	inf	0,245
Black list of customers_0, How to prevent hacking_59	How to reduce the credit limit_0	0,673	1,000	1,486	0,004	inf	0,331
How to reduce the credit limit_0, How to prevent hacking_60	Black list of customers_0	0,758	1,000	1,320	0,004	inf	0,246
Black list of customers_0, How to prevent hacking_61	How to reduce the credit limit_0	0,673	1,000	1,486	0,004	inf	0,331

Продовження таблиці Б4

1	2	3	4	5	6	7	8
How to reduce the credit limit_0, How to prevent hacking_68	Black list of customers_0	0,758	1,000	1,320	0,003	inf	0,245
Black list of customers_0, How to prevent hacking_68	How to reduce the credit limit_0	0,673	1,000	1,486	0,004	inf	0,331
How to prevent hacking_68	How to reduce the credit limit_0, Black list of customers_0	0,515	1,000	1,940	0,006	inf	0,490
How to reduce the credit limit_0, How to prevent hacking_70	Black list of customers_0	0,758	1,000	1,320	0,004	inf	0,246