DOI: https://doi.org/10.32782/2524-0072/2022-45-42

УДК 330.43:330.46

ПОПЕРЕДНІЙ АНАЛІЗ І ПІДГОТОВКА ДАНИХ ДЛЯ ПРОГНОЗУВАННЯ ТРЕНДІВ КІБЕРАТАК[1]

PRELIMINARY ANALYSIS AND PREPARATION OF DATA FOR CYBERATTACK TRENDS PREDICTION

Яровенко Ганна Миколаївна
докторка економічних наук, доцентка,
Сумський державний університет,
запрошена професорка,
Мадридський університет Карлоса III
ORCID: https://orcid.org/0000-0002-8760-6835

Кобзенко Вікторія Вікторівна
магістрантка,
Сумський державний університет
ORCID: https://orcid.org/0000-0002-7183-6687

Yarovenko Hanna
Sumy State University;
University Carlos III of Madrid

Kobzenko Viktoriia
Sumy State University

Дана стаття присвячена актуальному питанню протидії кібератакам шляхом застосування методів прогнозування. У дослідженні запропоновано концептуальну модель прогнозування трендів кібератак, яка передбачає реалізацію етапу попереднього аналізу та підготовки даних, та етапу розробки прогнозної моделі. Розрахунки проводилися на основі панельних даних, сформованих для 40 країн та 30-денного періоду. Проведений аналіз базових статистик виявив неоднорідність даних, обумовлених різним рівнем розвитку узятих для розрахунків країн. Реалізована декомпозиція трендів встановила відсутність трендової складової в рядах, наявність сезонної компоненти та адитивного зв'язку між складовими моделі. Перевірка на стаціонарність підтвердила стаціонарність досліджуваних рядів. Проведений тест Харка-Бера дозволив виявити невідповідність даних нормальному розподілу, в результаті чого було проведено їх трансформацію.

Ключові слова: кібератака, підготовка даних, попередній аналіз, прогнозування, тренд.

The article is devoted to the topical issue of combating cyberattacks through the use of forecasting methods. This issue is a consequence of the development of automation in various spheres of society and essential commercial and state companies. Cyber attacks can target multiple infrastructure facilities, which can cause power outages, disable equipment, and steal sensitive data that compromise a country's national security. The current situation related to cyber-attacks was analyzed, and the trends in studying this problem by scientists from various scientific schools and countries were investigated. The research proposed a conceptual model for predicting trends in cyberattacks, which involves the implementation of the preliminary analysis and data preparation stage and the stage of developing a predictive model. Calculations were made based on panel data generated for 40 countries and 30 days. Three types of time trends of cyber-attacks were used as a database of empirical data: the flow of data from malicious programs, suspicious and unwanted mail traffic, and data from detected network attacks. The analysis of the basic statistics revealed the heterogeneity of the data due to the different levels of the countries' development taken for the calculations. The implemented decomposition of trends established the absence of a trend component in the series, the presence of a seasonal element and an additive relationship between the model's parts. An extended Dickey-Fuller test was performed, which confirmed the stationarity of the studied series. The Jarque-Bera test made

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

it possible to reveal the inconsistency of the data with a normal distribution, resulting in the transformation of the variables "x" by logarithmization. The conducted data preparation made it possible to prepare the data for building predictive models of cyberattack trends. Combined regression and regressions with random and fixed effects were chosen as such models. In the future, it is planned to carry out appropriate calculations, build predictive models, assess their accuracy and adequacy, and make forecasts for short-term periods for various countries.

Keywords: cyberattack, data preparation, preliminary analysis, prediction, trend.

Постановка проблеми. Зростання рівня інформатизації та комп'ютеризації багатьох сфер життєдіяльності суспільства призвело до появи та розповсюдження такого явища як кіберзлочинність. Кіберзлочином вважається дія особи чи групи осіб, направлена на незаконне отримання персональних даних іншої фізичної особи, суб'єктів господарювання, державних органів, або порушення функціонування їх програмних та технічних засобів. Як правило, даний вид злочину здійснюються за допомогою комп'ютерних засобів та технологій.

Найбільш розповсюдженим видом кіберзлочину є кібератаки, які провадяться хакерами для досягнення економічних, політичних та соціальних цілей особи, груп осіб або держави. У 2020 році вони посідали п'яте місце у світі серед таких видів ризиків, як геополітичні, економічні, соціальні та навколишнього середовища, що робить їх досить серйозною проблемою для суспільства [1]. Серед кібератак виділяються такі види, як фішинг, DoS-атаки, розповсюдження шкідливого програмного забезпечення, Man-in-the-Middle, Zero-day exploit атаки, міжсайтовий скриптинг, логічні бомби, тощо. Їх головними характеристиками є непередбачуваність, стрімкість здійснення, масове охоплення об'єктів, висока ймовірність досягнення цілей, що робить їх швидкою та небезпечною зброєю в руках злочинців.

Результатом кібератак, як правило, є витік або втрата інформації. Так, у 2022 році найбільші втрати від кіберзлочинів відбулися у сфері охорони здоров'я (10,10 млн дол. США), фінансовій індустрії (5,97 млн дол. США), фармацевтичній галузі (5,01 млн дол. США), технологічній сфері (4,97 млн дол. США), енергетиці (4,72 млн дол. США) та інших [2]. Також прогнозується, що у 2025 році кіберзлочинність буде коштувати компаніям приблизно 10,5 трлн дол. США, що перевищуватиме втрати у 3,5 рази в порівнянні з 2015 роком [3]. Також слід зазначити, що кількість кібератак невпинно зростає. Наприклад, кількість їх випадків в результаті пандемії COVID-19 зросла на 600% [4].

Таким чином, проблема кіберзлочинів в цілому та кібератак зокрема є досить актуальною, потребує пошуку різних інструментів і методів її дослідження та протидії. Для цього ефективними є не тільки технічні та програмні засоби але й управлінські інструменти, такі як прогнозування трендів. Процес прогнозування є складним і включає різні етапи реалізації, одним з яких є підбір даних, здійснення їх попереднього аналізу та підготовки до розробки ефективних прогнозних моделей. Реалізації даного етапу й буде присвячене це дослідження.

Аналіз останніх досліджень і публікацій. Питання виявлення та протидії кібератак є актуальним перед усім для науковців, які займаються питаннями кібербезпеки. Але сьогодні дана проблема набуває міждисциплінарного значення, оскільки її наслідки спостерігаються в економіці, бізнесі, суспільстві, політиці, охороні здоров'я та інше. Тому вчені з різних наукових шкіл та напрямків намагаються вирішувати її з різних точок зору.

Стейсі П., Тейлор Р., Спанакі К. досліджували психологічні аспекти впливу кібератак, а саме емоційні реакції персоналу компаній [5]. Шендлер Р. та Гомес М. А. виявили, що кібератаки є джерелом суспільного ризику, що проявляється у зростанні рівня суспільної недовіри до уряду у випадку кіберзагроз [6]. Лонсдейл Д. Дж. перевіряв кібератаки на предмет їх благ для суспільства, що визначалося з точки зору поваги до людини, соціального благополуччя, безпеки та миру, а також солідарності [7]. Болпагні М. запропонував зведений індекс для вимірювання кіберризику та оцінив вплив соціо-економічних факторів на його зміни [8]. Сімонс Г., Даник Ю., Маляр-чук Т. намагалися вирішити дилему, породжену суперечністю правового регулювання із політичною та оперативною необхідністю управління ситуаціями, пов'язаними із кіберзагрозами [9].

Вівер Г. А., Феддерсен Б., Марла Л., Вей Д., Роуз А., Ван Моер М. вивчали економічні наслідки кібератак на прикладі морської транспортної системи та застосували оптимізаційний підхід для оцінки взаємодії між кібе-

ратаками та відповідними інформаційними технологіями компанії [10]. Лерой І. запропонувала застосовувати інструменти управління репутацією компанії для відновлення вартості її акцій після здійснення кібератак [11]. Акото У. дослідив позитивний вплив кібератак на торгівельні операції країни, що проявляється у використанні секретів, які добуваються в результаті кібершпигунства на користь держави [12]. Лаллі Г. С., Шеперд Л. А., Медсестра Дж. Р. К., Ерола А., Епіфаніу Г., Мейпл К., Беллекенс Х. проаналізували період пандемії COVID-19 з точки зору кібератак та виявили тенденцію їх щоденного зростання [13].

Не дивлячись на те, що проблема кібератак є досить актуальною та практично значущою, існує потреба у розробці прогнозних моделей, які дозволять виявляти потенційні кіберзагрози для певних країн та застосовувати контрзаходи щодо їх попередження.

Формулювання цілей статті. Метою даного дослідження є здійснення попереднього аналізу даних та їх підготовка для подальшої розробки прогнозних моделей трендів кібератак.

Виклад основного матеріалу дослідження. Базою для розробки будь-якої прогнозної моделі є побудова її концептуальної моделі. Вона представляє собою зображення процесу моделювання, як сукупності етапів, починаючи з виявлення та аналізу вхідних даних, які відображають проблеми дійсності, та завершуючи розрахунком прогнозів за обраною моделлю та перевіркою їх якості. Для прогнозування інформаційних трендів кібератак пропонуємо наступну концептуальну модель (рис. 1).

Представлена на рисунку 1 концептуальна модель прогнозування трендів кібератак передбачає виконання двох процесів – попереднього аналізу і підготовки даних та прогнозування. Перший процес є необхідним для досліджень подібного характеру, оскільки він дозволяє сформувати такий набір даних, від якості якого залежатимуть подальші дії щодо створення прогнозної моделі та отримання адекватних та точних прогнозів. Другий процес передбачає вибір математичних моделей, які відповідатимуть результатам, отриманим після попереднього аналізу та підготовки даних. Дане дослідження буде охоплювати результати здійснення першого процесу, передбаченого концептуальною моделлю. Другий процес висвітлюватиметься у наступному дослідженні.

На першому етапі було сформовано набір змінних для розробки прогнозної моделі трендів кібератак. Вхідною інформацією було обрано статистичні дані 40 країн світу (по 10 країн з Європи, Азії, Африки та по 5 країн з Північної та Південної Америки) за період з 14 серпня 2022 року до 13 вересня

Рис. 1. Концептуальна модель прогнозування трендів кібератак

2022 року, узятих з відкритого доступу Лабораторії Касперського. Вони представляють собою щоденну статистику про кількість кібератак, виявлених за допомогою спеціальних інструментів їх протидії, а саме:

– MAV (Mail Anti Virus) – поштовий антивірус, який показує потік даних шкідливих програм, виявлених серед нових об'єктів у поштових додатках. Він перевіряє вхідні повідомлення та запускає автоматичну перевірку при збереженні вкладених файлів на диск;

– KAS (Kaspersky Anti-Spam) – Касперський Анти-Спам, який показує підозрілий та небажаний поштовий трафік, виявлений за допомогою технологій репутаційної фільтрації «Лабораторії Касперського»;

– IDS (Intrusion Detection Scan) – система виявлення вторгнень, яка показує потік даних з виявлених мережевих атак.

Обрані дані є панельними, оскільки містять інформацію про одну і ту ж множину об’єктів за ряд послідовних періодів часу. Тобто маємо одні й ті самі дані щодо трьох видів кібератак для сорока країн за 30 днів. Відповідно, для кожного спостереження будуть вимірюватися декілька параметрів (регресійні змінних або ефектів) за кожен період часу. Оскільки в даному випадку всі показники відстежуються протягом однакової кількості періодів часу, то така панель є збалансованою.

На наступному кроці необхідно провести первинний аналіз початкових даних та здійснити відповідні маніпуляції для його підготовки до безпосередньої побудови прогнозної моделі.

Розрахунки для даного дослідження проводилися із використанням мови програмування Python. Для цього було використано ряд стандартних бібліотек для аналізу, візуалізації і моделювання даних, таких як: Pandas, Numpy, Scipy.stats, Statsmodels, Matplotlib, Seaborn, Linearmodels та інші.

Спочатку була проведена перевірка набору даних щодо наявності пропущених значень за допомогою функції isna(). Дана процедура необхідна для виявлення відсутніх даних, що робить вибірку неоднорідною. Результат її проведення показав, що набір не має пропущених даних і не потребує додаткових маніпуляцій по їх відновленню чи заміні.

Далі була проведена оцінка базових статистик, результати якої представлені на рисунку.

На рисунку можна побачити, що набір даних складається з 1240 спостережень. Значення середньоквадратичного відхилення по всім трьом видам кібератак є дуже високим і значно перевищує середнє значення ряду, що говорить пре неоднорідність даних. Це пов’язано із тим, що деякі країни, які увійшли у вибірку, є більш атакованими, ніж інші. Також мінімальні та максимальні значення для всіх трьох видів кібератак мають суттєвий розкид – мінімальне є дуже маленьким числом, що свідчить про відсутність кібератак в даний момент часу для певної країни, а максимальне – дуже великим числом, що свідчить про значну активність кібератак в певному регіоні. У випадку MAV та IDS кібератак їх середні значення відповідають третьому квартилю, а у випадку KAS атаки – четвертому квартилю. Це свідчить про те, що кількість спостережень, відповідних найбільш активним фазам кібератак, складає приблизно 20–30% від загальної кількості. Тобто вони носять періодичний характер, який ймовірно залежить від часового періоду та від самої країни, на яку спрямована кібератака.

Оскільки панельні дані являються часовим рядом, необхідно дослідити їх декомпозицію та перевірити на відповідність нормаль-

index	MAV	KAS	IDS
count	1240.0	1240.0	1240.0
mean	4647.270967741935	7617245.080645162	152111.00161290323
std	7700.3844928245235	20092268.916028455	251532.5601747635
min	1.0	3500.0	2.0
25%	286.0	140375.0	8927.0
50%	1630.5	764000.0	46237.0
75%	5174.0	4785625.0	213360.75
max	77612.0	181005000.0	2643943.0

Рис. 2. Результати розрахунку базових статистик для початкових даних

ному розподілу. На рисунку 3 представлено декомпозицію інформаційних трендів кібератак, яка включає побудову графіків фактичних даних, трендової, сезонної та залишкової компонент.

Декомпозиції, представлені на рисунку 3, побудовано за адитивною моделлю, оскільки обрані тренди відповідають саме адитивному процесу. Це підтверджує випадковий розподіл їх залишків, які коливаються біля нуля. Візуальний аналіз трендової складової свідчить про її відсутність, але в даному випадку потрібні додаткові перевірки на стаціонарність, для чого використано тест Дикі-Фулера. Графіки, які відповідають сезонним складовим вказують на можливість наявності даної компоненти в досліджуваних часових рядах.

Результати перевірки досліджуваних рядів на стаціонарність представлені у таблиці 1.

Проведені тести перевірки рядів на стаціонарність показали, що вони є стаціонарними, тобто значення рядів не мають трендової складової. Для панельних даних у нашому випадку це означає, що у нас не буде виявлено ефекту хибної регресії, що дозволить будувати такі її різновиди, як об'єднана регресія, регресія з фіксованими та випадковими ефектами.

На наступному кроці проведемо перевірку часових рядів на нормальність, а саме їх відповідність нормальному розподілу. Для цього

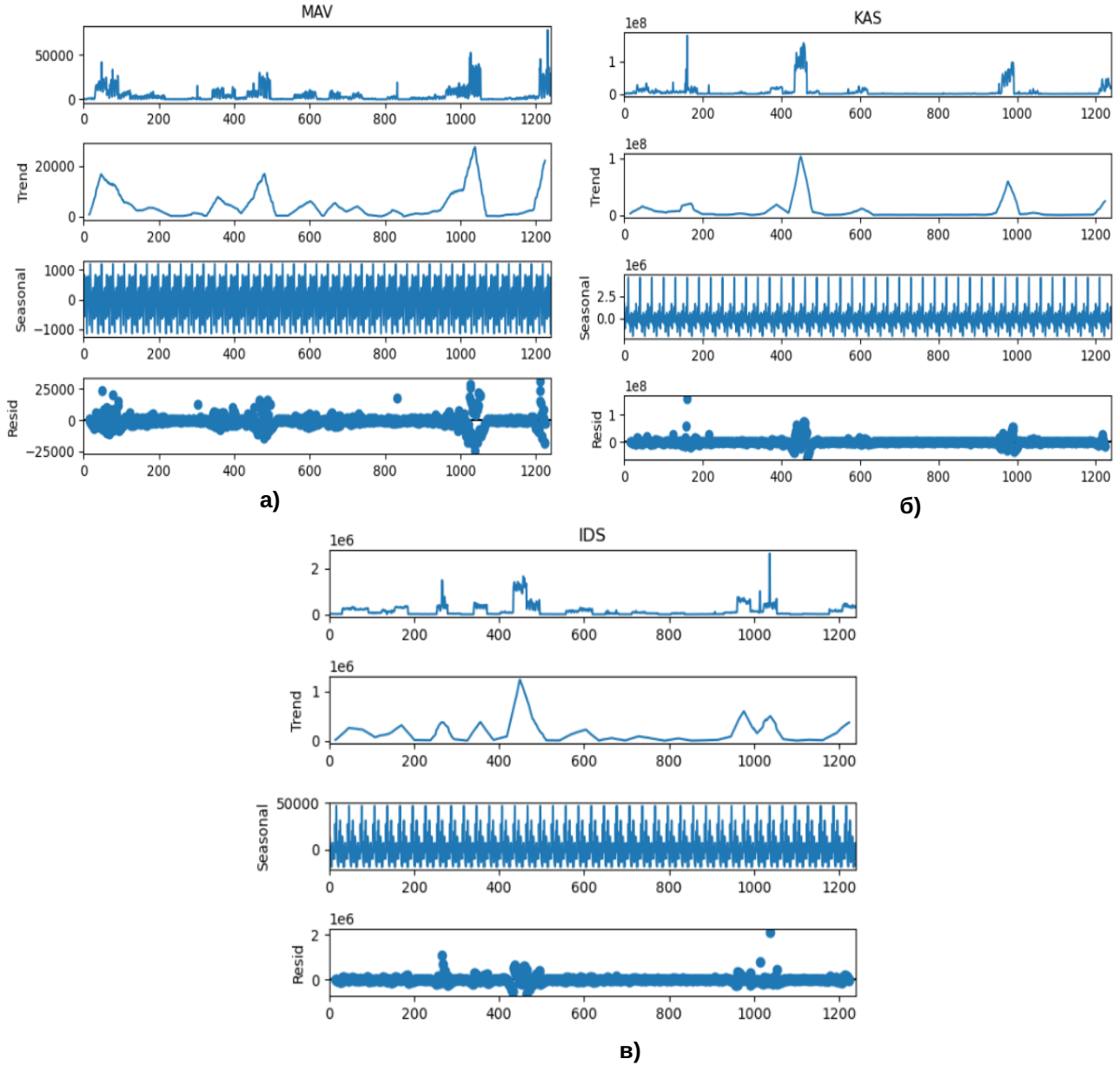

Рис. 3. Декомпозиція трендів для змінних: а) MAV; б) KAS; в) IDS

Таблиця 1

Результати тесту Дики-Фулера

Показники тесту	MAV	KAS	IDS
ADF	-7,1100	-36,6960	-36,0314
P-value	0,0000	0,0000	0,0000
Critical value 1%	-3,4357	-3,4356	-3,4356
Critical value 5%	-2,8639	-2,8639	-2,8639
Critical value 10%	2,5680	2,5680	2,5680
Висновок тесту	одиничних коренів немає, ряд є стаціонарним	одиничних коренів немає, ряд є стаціонарним	одиничних коренів немає, ряд є стаціонарним

застосуємо два методи: метод побудови гістограм та обчислення тесту Харке-Бера. Результати проведеної процедури представлено на рисунку 4. Обидва методи показали, що вхідні дані не відповідають нормальному розподілу. Статистика тесту Харка-Бера завжди є позитивним числом, і якщо вона далека від нуля, а значення p-value менше 0,05, то це вказує на те, що вибіркові дані не відповідають нормальному розподілу. Також й візуальний аналіз графіків підтверджує даний висновок. Якщо гістограма має приблизно «дзвіноподібну форму», то дані вважаються нормально розподіленими. В нашому випадку змінні не мають такої форми, що свідчить про наявність асиметрії в даних і їх не відповідність нормальному розподілу.

Для наближення даних до нормального розподілу можна виконати процедуру їх логарифмування, тобто здійснити перетворення незалежних змінних “x” із використанням log(x). Отримані трансформовані дані візуалізовані на рисунку 5.

Хоча трансформація даних й не призвела до повній відповідності даних нормальному закону, але отримані розподіли, зображені на рисунку 5, є досить близькими, що, в принципі, дозволяє їх використання для побудови прогнозних моделей.

Висновки. Дане дослідження присвячене проблематиці кібератак, кількість випадків яких зросла за останні роки. Їх наслідки є катастрофічними для бізнесу, фізичних осіб та держав в цілому. Саме тому виникає потреба у використанні інструментів щодо їх попередження та протидії, в якості яких можуть виступати моделі прогнозування. Для їх реалізації важливим етапом є аналіз та підготовка вхідних даних, що було проведено у даному досліджені. В якості бази емпіричних даних виступили три види часових трендів кібератак, які відслідковувалися за допомогою поштового антивірусу, Касперського Анти-Спаму та системи виявлення вторгнень.

У статті було запропоновано концептуальну модель розробки прогнозних моделей кібератак, яка показує всі етапи процесу про-

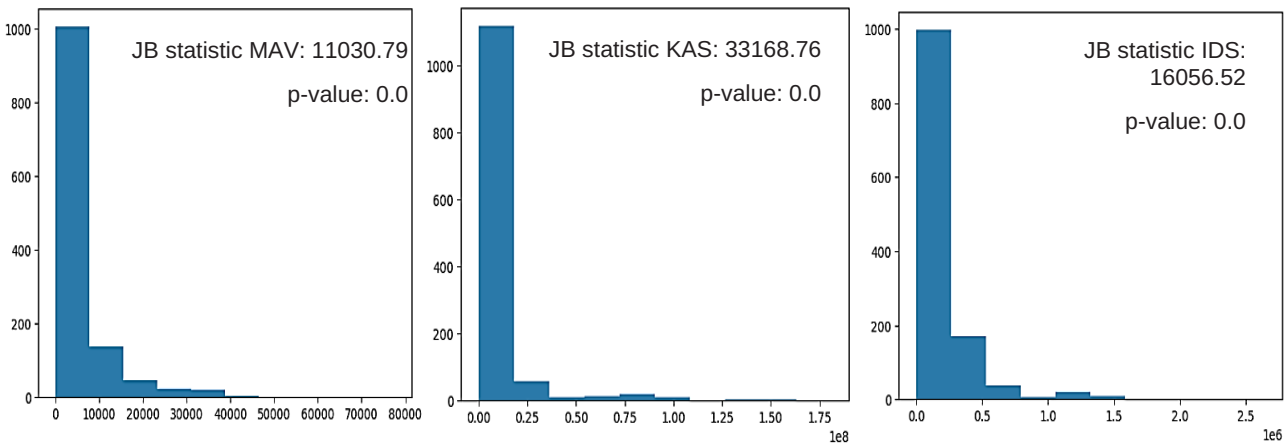

Рис. 4. Перевірка даних на відповідність закону нормального розподілу змінних

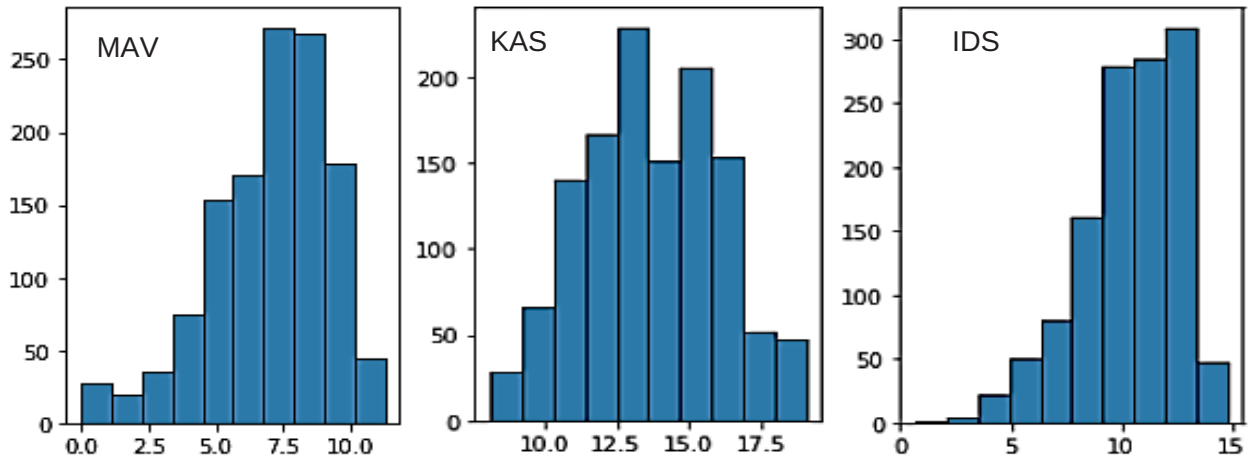

Рис. 5. Результат трансформування незалежних змінних “x”

гнозування. Розраховані базові статистики дозволили виявити неоднорідність даних. Встановлено, що це пов’язано із різним рівнем економічного розвитку країн, які було обрано для аналізу. Відповідно, деякі з них в більшій мірі ставали об’єктами кіберзагроз, інші – в меншій мірі. Проведена декомпозиція трендів дозволила виявити, що дані не містять трендової складової, мають сезонність та зв'язок між змінними є адитивним. Перевірка на стаціонарність за допомогою розширеного тесту Дики-Фулера встановила, що аналізовані тренди є стаціонарними, тобто був підтверджений попередній висновок щодо відсутності трендової складової. Оскільки дані характеризуються нерівномірністю, то проведена перевірка на відповідність нормальному розподілу за допомогою тесту Харка-Бера підтвердила, що їх невідповідність. Для їх наближення до умов нормального розподілу було проведено трансформацію змінних “x” шляхом логарифмування.

Таким чином, проведені в статті процедури підготовки даних дозволяють побудувати прогнозні моделі, такі як об’єднану регресію, регресію з випадковим та фіксованим ефектами. Дані побудові буде реалізовано у подальших дослідженнях.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. The Global Risk Report. *World Economic Forum.* URL: https://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf. (дата звернення: 10.12.2022).

2. Cost of a Data Breach Report 2022. *IBM Security.* URL: https://www.ibm.com/downloads/cas/3R8N1DZJ (дата звернення: 10.12.2022).

3. Mclean M. Must-Know Cyber Attack Statistics and Trendshttps. *Embroker.* 2022. URL: www.embroker.com/blog/cyber-attack-statistics/ (дата звернення: 10.12.2022).

4. Reports largest single day virus spike. URL: https://abcnews.go.com/Health/wireStory/latest-india-reports-largest-single-day-virus-spike-70826542 (дата звернення: 10.12.2022).

5. Stacey P., Taylor R., Spanaki K. Emotional reactions and coping responses of employees to a cyber-attack: A case study. *International Journal of Information Management.* 2021. Vol. 58, art. num. 102298. DOI: https://doi.org/10.1016/j.ijinfomgt.2020.102298.

6. Shandler R., Gomez M. A. The hidden threat of cyber-attacks–undermining public confidence in government. *Journal of Information Technology and Politics*. 2022. DOI: https://doi.org/10.1080/19331681.2022.2112796.

7. Lonsdale D. J. The Ethics of Cyber Attack: Pursuing Legitimate Security and the Common Good in Contemporary Conflict Scenarios. *Journal of Military Ethics*. 2020. Vol. 19. № 1. P. 20–39. DOI: https://doi.org/10.1080/15027570.2020.1764694.

8. Bolpagni M. Cyber risk index: a socio-technical composite index for assessing risk of cyber attacks with negative outcome. *Quality and Quantity.* 2022. Vol. 56. № 3. P. 1643–1659. DOI: https://doi.org/10.1007/s11135-021-01199-3.

9. Simons G., Danyk Y., Maliarchuk T. Hybrid war and cyber-attacks: creating legal and operational dilemmas. *Global Change, Peace and Security*. 2020. Vol. 32. № 3. P. 337–342. DOI: https://doi.org/10.1080/14781158.2020.1732899.

10. Weaver G. A., Feddersen B., Marla L., Wei D., Rose A., Van Moer M. Estimating economic losses from cyber-attacks on shipping ports: An optimization-based approach. *Transportation Research Part C: Emerging Technologies.* 2022. Vol. 137, art. num. 103423. DOI: https://doi.org/10.1016/j.trc.2021.10342.

11. Leroy I. The relationship between cyber-attacks and dynamics of company stock: the role of reputation management. *International Journal of Electronic Security and Digital Forensics*. 2022. Vol. 14, №4. P. 309–317. DOI: https://doi.org/10.1504/IJESDF.2022.123891.

12. Akoto W. International trade and cyber conflict: Decomposing the effect of trade on state-sponsored cyber attacks. *Journal of Peace Research*. 2021. Vol. 58. № 5. P. 1083–1097. DOI: https://doi.org/10.1177/00223433 20964549.

13. Lallie H. S., Shepherd L. A., Nurse J. R.C., Erola A., Epiphaniou G., Maple C., Bellekens X. Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers and Security*. 2021. Vol. 105. Art. Num. 102248. DOI: https://doi.org/10.1016/j.cose.2021.102248.

REFERENCES:

1. World Economic Forum. (2020). *The Global Risk Report*. Retrieved from: https://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf (December 10, 2022).

2. IBM Security. (2022). *Cost of a Data Breach Report 2022*. Retrieved from: https://www.ibm.com/downloads/cas/3R8N1DZJ (December 10, 2022).

3. Mclean, M. (2022). *Must-Know Cyber Attack Statistics and Trendshttps*. Retrieved from: www.embroker.com/blog/cyber-attack-statistics/ (December 10, 2022).

4. Reports largest single day virus spike. Retrieved from: https://abcnews.go.com/Health/wireStory/latest-india-reports-largest-single-day-virus-spike-70826542 (December 10, 2022).

5. Stacey, P., Taylor, R., & Spanaki, K. (2021). Emotional reactions and coping responses of employees to a cyber-attack: A case study. *International Journal of Information Management, 58,* 102298. DOI: https://doi.org/10.1016/j.ijinfomgt.2020.102298.

6. Shandler, R. & Gomez, M. A. (2022). The hidden threat of cyber-attacks–undermining public confidence in government. *Journal of Information Technology and Politics*. DOI: https://doi.org/10.1080/19331681.2022.2112796.

7. Lonsdale, D. J. (2020). The Ethics of Cyber Attack: Pursuing Legitimate Security and the Common Good in Contemporary Conflict Scenarios. *Journal of Military Ethics*, *19*(1), 20–39. DOI: https://doi.org/10.1080/15027570.2020.1764694.

8. Bolpagni, M. (2022). Cyber risk index: a socio-technical composite index for assessing risk of cyber attacks with negative outcome. *Quality and Quantity, 56*(3), 1643–1659. DOI: https://doi.org/10.1007/s11135-021-01199-3.

9. Simons, G., Danyk, Y., & Maliarchuk, T. (2020). Hybrid war and cyber-attacks: creating legal and operational dilemmas. *Global Change, Peace and Security*, *32(*3), 337–342. DOI: https://doi.org/10.1080/14781158.2020.1732899.

10. Weaver, G. A., Feddersen, B., Marla, L., Wei, D., Rose, A. & Van Moer, M. (2022). Estimating economic losses from cyber-attacks on shipping ports: An optimization-based approach. *Transportation Research Part C: Emerging Technologies, 137,* 103423. DOI: https://doi.org/10.1016/j.trc.2021.10342.

11. Leroy, I. (2022). The relationship between cyber-attacks and dynamics of company stock: the role of reputation management. *International Journal of Electronic Security and Digital Forensics*, *14*(4), 309–317. DOI: https://doi.org/10.1504/IJESDF.2022.123891.

12. Akoto, W. (2021). International trade and cyber conflict: Decomposing the effect of trade on state-sponsored cyber attacks. *Journal of Peace Research*, *58*(5), 1083–1097. DOI: https://doi.org/10.1177/0022343320964549.

13. Lallie, H. S., Shepherd, L. A., Nurse, J. R.C., Erola, A., Epiphaniou, G., Maple, C., et al. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers and Security*, *105,* 102248. DOI: https://doi.org/10.1016/j.cose.2021.102248.